「個人資料保護法相關議題研析」委外服務案

結案報告

委託機關：國家發展委員會

受託單位：財團法人資訊工業策進會

中華民國 111 年 10 月

「個人資料保護法相關議題研析」委外服務案

結案報告

受委託單位：財團法人資訊工業策進會

研究主持人：顧振豪

研究期程：中華民國 110 年 9 月至 111 年 10 月

國家發展委員會 委託研究

中華民國 111 年 10 月

本研究報告內容僅供本會業務參考

摘要

我國《電腦處理個人資料保護法》自 84 年公布施行後，歷經 99 年全盤修正並更名為《個人資料保護法》（下稱個資法）及 104 年修法。隨著數位經濟與資訊科技之蓬勃發展，個人資料已成為新資源，各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討。為使我國個資法與時俱進並與國際接軌，本研究即以歐盟 GDPR、英國、德國、美國、日本、韓國、新加坡，及特定議題國家之瑞士及菲律賓、澳洲等國外立法例作為比較標的，並擇定外界關切之個資法相關議題，包括獨立專責機關監督權限行使、罰則、共通規定（豁免情形、域外效力、國際傳輸）、蒐集主體與受託處理者（蒐集、處理及利用之合法要件探討與受託處理者義務）、產業應用（科學研究、假名化及匿名化）與當事人權利（資料可攜權與被遺忘權）等，邀請學者專家及利害團體進行議題式討論，並就該等議題參考國外法制、會議討論，且蒐整重要實務議題與法規適用疑義，進行分析並比較我國現行個資法規定、行政函釋及司法實務判決。針對我國法制現況進行比較及評估對產業可能之影響後，具體呈現我國法制在前開討論之國別中，法令規範密度之程度。

在第三章結論與建議將本計畫所研析之議題依照優先性分別討論，國際傳輸、受託處理者義務等議題建議優先透過修法方式處理，且修法前得先以法規命令或指引加強規範；獨立專責機關之議題由於牽涉政府組織架構，宜透過修法整備組織設計；而去識別化規定、資料可攜權等議題涉及技術、標準等相關問題，建議先提供指引給予業界參考，修法可能性則須再研議；至於蒐集、處理或利用個資之合法性要件及特定目的解釋，目前各界尚未有明顯共識，宜待觀察各國實際應用情境作為後續法規調整。藉由本研究觀測國際個資法制重要議題，以針對我國國情提出適切之個資法修法政策規劃建議，俾利個資法後續研修作業之順利推行。

Abstract

In 1995, the Computer-processed Personal Data Protection Act in Taiwan has been promulgated by Presidential Decree. Undergoing a serial revision in 2010 and 2015. The Personal Data Protection Act (hereinafter, the "PDPA") is enacted to regulate the collection, processing and use of personal data, so as to empower the rights of data subject, and to facilitate the proper use of personal data. With the vigorous development of the digital economy and information technology, personal data has become a new asset. Hence, there are more and more countries adopted amendments in data protection laws to ameliorate data flow and protect personal data. Comparing data protection rules in the EU, the UK, Germany, the US, Japan, South Korea, Singapore, and other nations (Switzerland, the Philippines, and Australia), this study not only aims to keep pace with the times and align Taiwan's PDPA with international standards and best practices, but also provides analyses of independent supervisory authorities, penalties, common issues (exemptions, extraterritorial effects, and cross border transfers), data subject and data processor (including topics concerning data collection, data processing and utilization, as well as data processor's obligations), industrial application (scientific research, together with pseudonymization and anonymization), and rights of data subject (data portability and right to be forgotten). We have invited scholars, experts and other interest groups to conduct topic-based discussions, referring to the application of foreign laws regarding to the topics mentioned above. From these, we analyzed Taiwan's PDPA, administrative rules and adjudications, and evaluated the potential impacts and regulated intensity on the industries.

"Conclusions and Recommendations" in Chapter 3 is based on priority and importance to conclude issues: cross-border data transfers and the obligations of a data processor, which were suggested to be amended. Before the amendment, Guidelines may be published to strengthen regulatory norms. On the other hand, since the establishment of the independent supervisory agency involves in reorganizing the governmental structure, it is advisable to optimize the organizational structure through the revision of laws. Furthermore, this study suggested that the Taiwanese's government shall first published anonymisation, pseudonymisation and privacy enhancing technologies guidance. As for the legal requirements of collecting, processing or using personal data,

since there is no clear consensus among interest groups nor an urgent case, the regulatory adjustments and the dynamism of other countries shall be followed and tracked. In conclusion, comparing the important topics of the privacy laws that are widely discussed among the world, this study suggests several revisions of PDPA in different aspects, and to facilitate the smooth application of the follow-up research on PDPA.

目錄

第一章　前言 1
第一節　研究背景及目的 1
第二節　研究架構及方法 2
第三節　比較法國家之概述 3
第二章　個人資料保護法相關議題研析 6
第一節　獨立專責機關監督權限行使方式 6
壹、　比較法國家 6
一、　歐盟 6
二、　英國 8
三、　德國 9
四、　美國 10
（一）CCPA 及 CPRA 10
（二）UPDPA 12
五、　日本 12
六、　韓國 14
七、　新加坡 15
八、　瑞士 16
貳、　我國規定 17
參、　分析與小結 18
一、　比較法之分析 18
（一）調查權之行使方式 18
（二）處分權之行使方式 20
二、　小結 22
第二節　罰則 23
壹、　比較法國家 23
一、　歐盟 23
（一）有關刑事罰之規定 23

（二）有關行政罰之規定 24
二、 英國 26
（一）有關刑事罰之規定 26
（二）有關行政罰之規定 26
三、 德國 27
（一）有關刑事罰之規定 27
（二）有關行政罰之規定 27
四、 美國 28
（一）CCPA 及 CPRA 28
（二）UPDPA 29
五、 日本 29
（一）有關刑事罰之規定 29
（二）有關行政罰之規定 31
六、 韓國 31
（一）有關刑事罰之規定 31
（二）有關行政罰之規定 32
七、 新加坡.....33
（一）有關刑事罰之規定 33
（二）有關行政罰之規定 34
八、 菲律賓.....34
貳、 我國規定.....37
一、 有關刑事罰之規定.....37
二、 有關行政罰之規定.....37
參、 分析與小結.....38
一、 比較法之分析.....38
（一）刑事罰之規範 38
（二）行政罰之規範 41
二、 小結 44
第三節 共通規定.....45
第一項 豁免情形.....45
壹、 比較法國家.....45

一、 歐盟 45
二、 英國 46
三、 德國 47
四、 美國 48
（一）CCPA 及 CPRA 48
（二）UPDPA 49
五、 日本 50
六、 韓國 51
七、 新加坡 52
八、 菲律賓 52
九、 瑞士 53
貳、 我國規定 54
參、 分析與小結 55
一、 比較法之分析 55
二、 小結 60
第二項 域外效力 60
壹、 比較法國家 60
一、 歐盟 60
二、 英國 63
三、 德國 63
四、 美國 64
（一）CCPA 及 CPRA 64
（二）UPDPA 64
五、 日本 64
六、 韓國 65
七、 新加坡 65
八、 菲律賓 65
貳、 我國規定 66
參、 分析與小結 67
一、 比較法之分析 67
二、 小結 70

第三項　國際傳輸.....71
壹、　比較法國家.....71
一、　歐盟.....71
（一）國際傳輸之原則.....71
（二）國際傳輸之合法要件.....72
二、　英國.....77
（一）國際傳輸之原則.....77
（二）國際傳輸之合法要件.....77
三、　德國.....77
（一）國際傳輸之原則.....77
（二）國際傳輸之合法要件.....78
四、　美國.....78
五、　日本.....79
（一）國際傳輸之原則.....79
（二）國際傳輸之合法要件.....80
六、　韓國.....81
（一）國際傳輸之原則.....81
（二）國際傳輸之合法要件.....81
七、　新加坡.....82
（一）國際傳輸之原則.....82
（二）國際傳輸之合法要件.....82
八、　菲律賓.....83
（一）國際傳輸之原則.....83
（二）國際傳輸之合法要件.....84
九、　瑞士.....85
（一）國際傳輸之原則.....85
（二）國際傳輸之合法要件.....85
貳、　我國規定.....86
參、　分析與小結.....87
一、　比較法之分析.....87
（一）國際傳輸之限制.....87

（二）國際傳輸之合法要件.....88
二、 小結.....92
第四節 蒐集主體及受託處理者.....93
第一項 蒐集、處理及利用之合法要件探討（不含當事人同意）.....93
壹、 比較法國家.....93
一、 歐盟.....93
（一）一般及特種個人資料及處理之定義.....93
（二）一般個人資料之合法要件.....94
（三）特種個人資料之合法要件.....96
二、 英國.....99
（一）一般及特種個人資料之定義.....99
（二）處理一般個人資料之合法要件.....99
（三）處理特種個人資料之合法要件.....100
三、 德國.....101
（一）一般及特種個人資料及處理之定義.....101
（二）一般個人資料之合法要件.....102
（三）處理特種個人資料之合法要件.....103
四、 美國.....105
（一）一般及特種個人資料之定義.....105
（二）一般及特種個人資料之合法要件.....107
五、 日本.....110
（一）一般及特種個人資料之定義.....110
（二）一般個人資料之合法要件.....111
（三）特種個人資料之合法要件.....112
六、 韓國.....114
（一）一般及特種個人資料與處理之定義.....114
（二）一般個人資料之合法要件.....115
（三）特種個人資料之合法要件.....116
七、 新加坡.....117
（一）一般及特種個人資料之定義.....117

（二）一般個人資料之合法要件.....118
（三）特種個人資料之合法要件.....120
八、 瑞士 122
（一）一般及特種個人資料之定義.....122
（二）一般個人資料之合法要件.....123
（三）處理特種個人資料之合法要件.....125
貳、 我國規定及比較法分析.....125
一、 我國有關合法要件之相關規定.....125
（一）一般個人資料合法要件.....126
（二）特種個人資料合法要件.....128
二、 一般個人資料之比較法分析.....130
（一）公共利益要件之類型化討論.....130
（二）避免當事人及他人生命身體危險要件之討論.....134
（三）正當利益要件之討論.....136
（四）對當事人影響、取自公開資料或一般可得來源要件之討論 136
三、 特種個人資料之比較法分析.....137
（一）特種個人資料之定義及立法例之討論.....138
（二）履行法定義務要件之討論.....140
（三）公共利益及保護個人利益要件之討論.....140
（四）取自公開資料或一般可得來源要件之討論.....143
參、 分析與小結.....144
第二項 受託處理者義務.....145
壹、 比較法國家.....145
一、 歐盟 145
（一）資料控管者與受託處理者之概念.....145
（二）受託處理者之相關義務.....145
二、 英國 149
三、 德國 150
四、 美國 152
（一）CCPA 及 CPRA 相關規定.....152

（二）UPDPA 相關規定 155
五、 日本 156
（一）個人資料處理事業者及受委託人之相關概念.....156
（二）個人資料處理事業者應監督之內容.....156
六、 韓國 158
（一）委託者及受託者之相關概念.....158
（二）受託者之相關義務 158
（三）針對影像處理之特殊規範.....160
七、 新加坡.....161
（一）組織與資料中介者之概念說明.....161
（二）資料中介者之相關義務.....161
貳、 我國規定.....162
一、 個資法上委託關係之規範及概念.....162
二、 受託者視為委託機關.....163
三、 受託者依委託機關應適用之規定.....163
四、 委託機關之監督義務.....164
參、 分析與小結.....164
一、 比較法之分析.....164
（一）委託、委託機關與受託者之相關定義.....164
（二）個資法上的責任義務.....166
（三）個資法上的法律效果歸屬.....169
二、 小結 170
第五節 產業應用.....172
第一項 科學研究.....172
壹、 比較法國家.....172
一、 歐盟 172
（一）科學研究之定義及適用範圍.....172
（二）科學研究之適用條件.....173
（三）科學研究之特殊彈性規範.....173
二、 英國 175
三、 德國 176

（一）科學研究之定義及特殊規定.....176
（二）科學研究之特殊放寬規定.....177
四、 美國 178
（一）HIPAA 之相關規定.....178
（二）CCPA 之相關規定 179
（三）UPDPA 之相關規定.....180
五、 日本 181
（一）學術研究之定義及適用對象.....181
（二）學術研究之相關放寬規定.....182
（三）學術研究機關等應遵守之義務.....183
六、 韓國 184
（一）科學研究之背景與定義.....184
（二）科學研究之適用條件與限制.....184
七、 新加坡.....185
（一）產業應用之相關合法事由.....185
（二）資料共享政策之特殊規定.....187
八、 菲律賓.....190
貳、 我國規定.....191
參、 分析與小結.....192
一、 比較法之分析.....192
（一）有關學術研究條款之相關定義討論.....192
（二）因學術研究條款而蒐集、處理或利用個資合法要件之探討 193
（三）有關學術研究而蒐集、處理或利用個資之特殊彈性規範 196
二、 小結 198
第二項 假名化及匿名化.....200
壹、 比較法國家.....200
一、 歐盟 200
（一）假名化之規範 200
（二）匿名化之規範 201

二、 英國 202
（一）假名化之規範 202
（二）匿名化之規範 203
三、 德國 204
（一）假名化之規範 204
（二）匿名化之規範 205
四、 美國 205
（一）UPDPA 205
（二）CCPA 206
（三）HIPAA 206
五、 日本 207
（一）假名化之規範 207
（二）匿名化之規範 209
六、 韓國 213
（一）定義及效果 213
（二）管理規範 213
七、 新加坡.....214
（一）定義及效果 214
（二）管理規範 215
八、 菲律賓.....216
（一）定義及效果 216
（二）管理規範 217
貳、 我國規定.....218
參、 分析與小結.....219
一、 比較法之分析.....219
（一）有關匿名化之相關規範探討.....219
（二）有關假名化之相關規範探討.....222
二、 小結 225
第六節 當事人權利.....226
第一項 資料可攜權.....226
壹、 比較法國家.....226

一、 歐盟 226
（一）有關資料可攜權之規範 226
（二）產業應用 227
二、 英國 228
（一）有關資料可攜權之規範 228
（二）產業應用 228
三、 德國 229
（一）有關資料可攜權之規範 229
（二）產業應用 230
四、 美國 231
（一）有關資料可攜權之規範 231
（二）產業應用 232
五、 日本 232
（一）有關資料可攜權之規範 232
（二）產業應用 233
六、 韓國 233
（一）有關資料可攜權之規範 233
（二）產業應用 234
七、 新加坡 235
（一）有關資料可攜權之規範 235
（二）產業應用 235
八、 澳洲 236
（一）有關資料可攜權之規範 236
（二）產業應用 237
貳、 我國規定 238
參、 分析與小結 239
一、 比較法之分析 239
（一）資料可攜權之形式 239
（二）資料可攜權之規範 240
二、 小結 241
第二項 被遺忘權 242

壹、　比較法國家.....242
一、　歐盟.....242
（一）背景與定義.....242
（二）相關規範.....242
二、　英國.....245
（一）有關被遺忘權之規範.....245
（二）實務案例.....245
三、　德國.....245
（一）有關被遺忘權之規定.....245
（二）實務案例.....246
四、　美國.....247
（一）CCPA 及 CPRA.....247
（二）UPDPA.....248
五、　日本.....248
（一）有關被遺忘權之規範.....248
（二）實務案例.....249
六、　韓國.....250
七、　新加坡.....250
貳、　我國規定及分析.....250
參、　分析與小結.....252
一、　比較法之分析.....252
（一）被遺忘權之內涵.....252
（二）被遺忘權之規範.....252
二、　小結.....253
第三項　權利限制規定.....254
壹、　比較法國家.....254
一、　歐盟.....254
（一）權利行使限制事由.....254
（二）權利行使限制規範.....255
二、　英國.....256
（一）UK GDPR.....256

（二）DPA 2018 257
三、 德國 257
四、 美國 258
（一）CCPA 及 CPRA 258
（二）UPDPA 259
五、 日本 260
（一）非公務機關 260
（二）公務機關 260
六、 韓國 262
七、 新加坡 262
八、 瑞士 263
貳、 我國規定 264
一、 近用權之限制 264
二、 更正權之限制 264
三、 刪除權及停止蒐集、處理或利用權之限制 265
參、 分析與小結 265
一、 比較法之分析 265
（一）近用權之限制 265
（二）更正權之限制 268
（三）刪除及停止蒐集、處理或利用權之限制 269
二、 小結 275
第三章 結論與建議 277
一、 獨立專責機關監督權限行使方式 277
（一）獨立專責機關之設置 277
（二）監督權限行使方式 279
二、 罰則 281
三、 共通規定 283
（一）豁免情形 283
（二）域外效力 285
（三）國際傳輸 285
四、 蒐集主體及受託處理者 287

（一）蒐集、處理及利用之合法要件探討.....287
（二）受託處理者義務 289
五、 產業應用.....290
（一）科學研究 290
（二）假名化及匿名化 292
六、 當事人權利.....294
（一）資料可攜權 294
（二）被遺忘權 295
（三）權利限制規定 297
參考資料 300
附件一、諮詢會議之會議記錄.....313
附件二、專家學者訪談相關記錄.....451
附件三、國際觀測相關彙整之簡報內容.....478
附件四、諮詢會議之會議資料.....517

表目錄

表 1 各國獨立專責機關有關調查權限之規範 19
表 2 各國獨立專責機關有關處分權限之規範 21
表 3 各國針對刑事罰之規範 40
表 4 各國針對行政罰之規範 43
表 5 各國針對豁免情形之規範 56
表 6 我國個資法域外效力 67
表 7 各國針對域外效力之規範 69
表 8 各國承認企業採行適當保護措施之類型 90
表 9 各國承認特定情形之類型 91
表 10 我國有關一般個人資料蒐集、處理或利用之合法要件 128
表 11 我國有關特種個人資料蒐集、處理或利用之合法要件 130
表 12 一般個人資料基於公共利益之合法要件比較表 131
表 13 一般個人資料基於公共利益目的外利用之比較表 133
表 14 一般個人資料有關避免當事人及他人生命身體危險要件之比較表 135
表 15 我國與各國有關特種個人資料立法例之比較 139
表 16 特種個人資料基於公共利益要件之比較表 141
表 17 特種個人資料基於保護個人利益要件之比較表 142
表 18 特種個人資料基於公開資料或一般可得來源要件之比較表 143
表 19 個資法上委託關係之法律定義與適用主體 165
表 20 個資法上委託關係之責任義務規範 168
表 21 個資法上委託關係之效果歸屬 170
表 22 我國個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之整理 191
表 23 我國與各國有關研究/科學研究/學術研究合法要件之比較 ..194
表 24 我國與各國針對研究/科學研究/學術研究彈性措施之比較 ..198
表 25 各國有關匿名化之要件 220
表 26 各國有關匿名化之管理措施 221
表 27 各國有關匿名化之義務要求 222

表 28 各國有關假名化之要件 223
表 29 各國有關假名化之管理措施 224
表 30 各國有關假名化之義務要求 225
表 31 各國有關資料可攜權之形式要件 239
表 32 有關近用權之主要類型限制要件比較 266
表 33 有關近用權之其他類型限制要件比較 267
表 34 有關更正權之限制要件比較 269
表 35 針對特定個資利用方式之刪除/停止蒐集、處理或利用權限制比較 271
表 36 針對特定蒐集、處理或利用合法要件之刪除/停止蒐集、處理或利用權限制比較 273
表 37 針對一般性請求刪除/停止蒐集、處理或利用權之限制比較 274

第一章　前言

第一節 研究背景及目的

我國自電子科技進步以來，便運用電腦大量快速地處理各類資料，隨著電腦對於國民經濟佔有重要貢獻且日益普及後，為避免電腦被濫用或不當利用之情形，對於人民隱私等權益產生重大危害；因此，參考經濟合作暨發展組織（Organisation for Economic Cooperation and Development, OECD）及歐盟執委會於 1981 年提出之保護個人資料自動化處理公約，遂於 1995 年公布施行《電腦處理個人資料保護法》[1]，該法雖曾於 2010 年全盤修正並更名為《個人資料保護法》（以下簡稱個資法），並嗣經 2015 年部分修正。

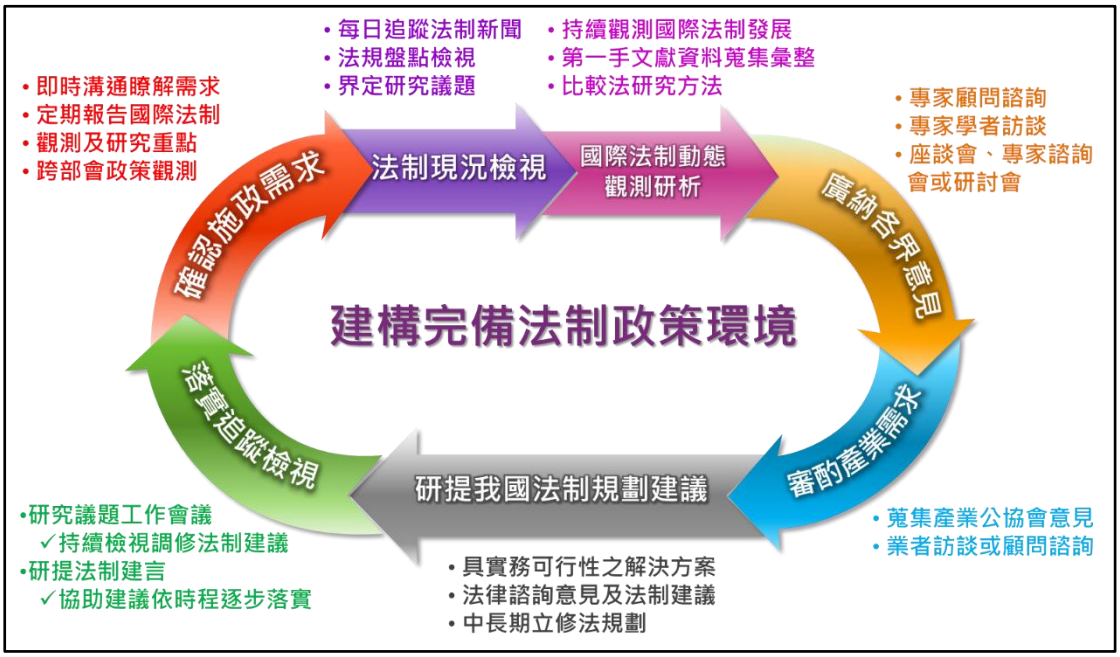
然而，隨著數位經濟與資訊科技之迅速發展，包含大數據、雲端運算、邊緣運算、物聯網及人工智慧等科技的日趨成熟，以及 5G 世代的來臨，使全球經濟發展進入嶄新的紀元，對於傳統的經濟與產業發展模式產生巨大改變。我國憲法法庭於 2022 年 8 月 12 日做出 111 年憲判字第 13 號判決，針對健保資料庫案認為由個人資料保護法或其他相關法律規定整體觀察，欠缺個人資料保護之獨立監督機制。而個人資料已成為數位經濟發展之重要基石，各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，在資料經濟流通運用過程內，同時兼顧個人資料的保護，以維護當事人隱私權利。對此，針對個資法上重要修法討論之議題，包括：獨立專責機關監督權限行使方式、罰則、豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含當事人同意要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）等議題進行研析，並參考國際立法例歐盟、德國、英國、美國、日本、韓國及新

[1] 立法院第 2 屆第 1 會期第 4 次會議議案關係文書（行政院院總第 1570 號政府提案第 4544 號），頁 71-75。

加坡等國家之個資法規範，以提出符合國際趨勢之修法意見。

第二節　研究架構及方法

考量個資法修正為外界所關注，本計畫擇定外界關切之個資法相關議題，進行蒐集、比較與分析國外立法例（包括但不限於歐盟GDPR、英國、德國、美國、日本、韓國、新加坡）等實務適用情形。另為廣納各界修法意見，就獨立專責機關、罰則、共通規定、蒐集主體與受託處理者、產業應用與當事人權利等議題召開會議，邀請學者專家及利害團體進行議題式討論，並就該等議題參考國外法制、會議討論，且蒐整重要實務議題與法規適用疑義，進行分析並比較我國現行個資法規定、行政函釋及司法實務判決。並我國法制現況比較及評估對產業可能之影響後，具體呈現我國法制在前開討論之國別中，法令規範密度之程度。就此針對我國國情提出適切之個資法修法政策規劃建議，俾利個資法後續研修作業之順利推行。



資料來源：本研究自行繪製

第三節　比較法國家之概述

為接軌國際個人資料保護法制，本計畫將蒐集與分析先進國家之個資法規，包含歐盟、英國、德國、美國、日本、韓國及新加坡，另就特定議題擇定瑞士、菲律賓與澳洲等國家，以資豐富本研究計畫之深度。由於本計畫比較與分析之國家較多，因此先就比較法國家之個資法概略介紹：

- 歐盟：歐盟於 2016 年 4 月通過《一般資料保護規則》(General Data Protection Regulation, 以下簡稱 GDPR)，並於 2018 年 5 月 25 日全面實施，凡有蒐集、處理或利用歐洲人民個人資料之組織，皆應遵守 GDPR 之相關規定。

- 英國：雖於 2021 年 1 月 1 日正式脫歐，惟其內閣為使日後資料可以無阻礙的傳輸於歐盟地區，除內國法之《資料保護法》（Data Protection Act 2018, 以下簡稱 DPA）作為隱私保護法規外，另依據 2018 年《歐盟（退出）法》(European Union (Withdrawal) Act 2018）之授權，訂定《2019 年資料保護、隱私與電子通訊（修正等）(脫歐）規則》(The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019)，並修正為 UK GDPR 以因應脫歐後的規範變遷。

- 德國：德國自 1990 年 12 年 20 日公布《聯邦個人資料保護法》(Bundesdatenschutzgesetz, 以下簡稱 BDSG)，後於 2017 年因應 GDPR 之實施而重新修正並公布，最近一次修正為 2021 年 6 月 23 日。此外，由於德國屬於歐盟成員國之一，而 GDPR 屬於「規則」之法律位階，依據《歐盟運作條約》（Treaty on the Functioning of the European Union）第 288 條第 2 項規定，對於成員國發生普遍的拘束力，成員國應普遍適用，且無須成員國依其國內立法程序轉換為內國法，而得直接適用於成員國。

- 美國：美國目前針對個人資料保護，有美國統一法律委員會（Uniform Law Commission, ULC）於 2021 年 7 月 14 日通過之《統一個人資料保護法》（Uniform Personal Data Protection Act, 以下簡稱 UPDPA），為統一州法法律委員全國會議為協助統一各州規定而訂定之非實定法律；2018 年 6 月 28 日通過之《加州消費者隱私法》（California Consumer Privacy Act 2018，以下簡稱 CCPA），以及 2020 年 11 月 3 日通過之《加州隱私權法》（California Privacy Rights Acts, 以下簡稱 CPRA）規定。另就特定議題討論《健康保險可攜與責任保險法》（Health Insurance Portability and Accountability Act, 以下簡稱 HIPAA）予以補充說明。

- 日本：日本於 2022 年 5 月通過修正《個人資料保護法》（個人情報の保護に関する法律，令和四年法律第四号による改正），並預計於 2023 年 4 月起正式施行，故以下針對日本新修正之個資法，作為主要闡述及討論規範。另就特定議題討論《行政機關個人資料保護法》（行政機関の保有する個人情報の保護に関する法律）及《次世代醫療基盤法》（医療分野の研究開発に資するための匿名加工医療情報に関する法律）。另應注意，日本於 2019 年 1 月取得歐盟 GDPR 適足性認定。

- 韓國：韓國於 2020 年 2 月修正並於同年 8 月 5 日實施「個人資料保護法」（개인정보보호법；Personal Information Protection Act, 以下簡稱 PIPA）。另韓國於 2021 年 12 月 17 日取得歐盟 GDPR 之適足性認定。

- 新加坡：新加坡於 2012 年 10 月 15 日通過《個人資料保護法》（Personal Data Protection Act 2012，以下簡稱 PDPA），並於 2020 年 11 月 2 日通過 PDPA 之修正案，本文以 2020 年版本之 PDPA，作為比較法分析。

- 瑞士：瑞士於 1992 年通過《聯邦個人資料保護法》

（Bundesgesetzüber den Datenschutz, 以下簡稱 DSG），最近一次修正時間為 2019 年。為促進個資處理透明化並強化個資主體權利，使國內個資法得盡量與 GDPR 一致，同時也為符合歐盟跨國資料傳輸的適足性要求。並於 2020 年 9 月 25 日通過新修正之個資法，預計 2022 年夏季正式生效[2]，故以下將以 2020 年新修正之 DSG 作為比較法分析。

— 菲律賓：菲律賓自 2012 年 8 月 15 日公布《資料隱私法》（Data Privacy Act of 2012, DPA）後，最近一次的修正為 2021 年 8 月 24 日順利通過聯邦眾議院三讀程序，並於 2021 年 8 月 26 日送至菲律賓參議院審議階段[3]。因該修正新法尚未公布，故本文以 2012 年版本之 DPA，作為討論基礎。

— 澳洲：澳洲於 2019 年 8 月 1 日通過《2019 年消費者資料權法》（Treasury Laws Amendment（Consumer Data Right）Act 2019），針對《2010 年競爭及消費者法》（Competition and Consumer Act 2010）、《2010 年澳洲資訊委員法》（Australian Information Commissioner Act 2010）及《1988 年隱私法》（Privacy Act 1988）增訂「消費者資料權」（Consumer Data Right, CDR）相關規定。

---

2 ALAN CHARLES RAUL, THE PIVACY ,DATA PROTECTION AND CYBERSECURITY LAW REVIEW, 6th ed, 339-340 (2019).

3 18th Congress House Bill NO. HB01188, July 2, 2019, REPUBLIC OF THE PHILIPPINES HOUSE OF REPRESENTITIVES, https://www.congress.gov.ph/legisdocs/basic_18/HB01188.pdf (last visited Nov. 3, 2021).

第二章　個人資料保護法相關議題研析

第一節 獨立專責機關監督權限行使方式

壹、比較法國家

一、歐盟

GDPR 第 51 條要求各成員國必須成立至少一個獨立專責機關（supervisory authority）以獨立監督該國實施 GDPR 之情形，又第 52 條強調專責機關之獨立性。於 GDPR 架構下規定，當組織於多個歐盟成員國境內設有據點並於成員國之間傳輸資料時，監督權限行使方式採一站式制度（one stop shop mechanism），意指 GDPR 要求由單一獨立領導專責機關（lead supervisory authority）處理 GDPR 事務，讓資料當事人有單一窗口申訴。第 56 條第 1 項明定，當組織於多個成員國內設有據點時，位於主要據點的獨立專責機關即成為獨立領導專責機關，其他獨立專責機關應依 GDPR 第 60 條，與獨立領導專責機關合作，包含資訊交換、相互協作及即時回覆等。

有關獨立專責機關之監督權限行使方式，依第 57 條第 1 項明定包括：（1）監督 GDPR 之實施狀況及進行 GDPR 執法作業。（2）推廣公眾對 GDPR 的認知，以及對資料處理之風險、規定、安全措施、當事人權利的理解，並應特別重視對未成年者之推廣活動。（3）成員國內之立法機關、行政機關與其他相關機構及組織處理資料時，應基於保護自然人權利及自由原則採取行政、法律措施，獨立專責機關可依國內法針對所採取措施提出建議。（4）提倡資料控管者及受託處理者之義務。（5）依當事人請求履行當事人權利，視情況與其他成員國之專責機關合作。（6）處理當事人、機關、組織、團體提起之訴訟，針對訴訟內容進行調查，並於適當合理時間內通知調查進度及結果，尤其當調查時間需延長或有其他專責機關加入調查時應另行通知。又同條第 2 項明定專責機關應建立申訴表單。（7）與其他專責機關合作，為確保 GDPR 在實施及執法層面維持一致性，包

含資訊共享及互相協助。（8）主動對企業針對 GDPR 之實施展開調查，無論是經其他專責機關通報或是公務機關通報。（9）監督與個人資料保護相關事宜之發展，特別是科技發展及商業實務見解之發展。（10）採用認可標準契約條款。（11）建立並維持應進行資料保護影響評估之資料處理種類清單。（12）針對資料保護影響評估結果為高風險之資料控管者提出資料處理之建議。（13）鼓勵行為守則之擬定及核可所提出申請之行為守則，並提出建議。（14）鼓勵驗證制度之建立並核可驗證規則。（15）依情況而定，定期對受證組織進行檢查。（16）擬定及公布監督行為守則之認證機構（accreditation body）和驗證機構（certification body）的相關要求。（17）核准監督行為守則之認證機構（accreditation body）和驗證機構（certification body）。（18）國際傳輸情境下，核可資料控管者或受託處理者自行制定的契約條款，或是公務機關自行制定之行政條款。（19）核可企業自我拘束規則。（20）參加歐盟資料保護委員會（European Data Protection Board, EDPB）之活動。（21）紀錄 GDPR 違規案件及矯正措施。（22）其他基於個人資料保護應盡事項。

此外，依第 57 條第 3、4 項強調上述事務應免費提供，但當要求過分或明顯無依據、提出次數過於頻繁等情形得酌收合理費用。而第 58 條規範獨立專責機關具有調查權（investigative powers）、糾正權（corrective powers）、授權及建議權（authorisation and advisory powers）以協助其完成上述事務。

首先，調查權依第 58 條第 1 項明定包含：（1）命令資料控管者、受託處理者及其代表人提供有助於專責機關執行任務之所有資訊。（2）進行資料保護稽核。（3）針對受證單位進行審查。（4）對違法事項之指控，通知資料控管者及受託處理者。（5）從資料控管者及受託處理者端取得所有必要資訊之存取，以執行其任務。（6）依歐盟法或成員國國內程序法，專責機關得進入資料控管者及受託處理者之實體場域，包含使用設備。其次，糾正權依第 58 條第 2 項明定包含：（1）對疑似違反 GDPR 之資料控管者或受託處理者提出警告。（2）對已違反 GDPR 之資料控管者或受託處理者作出譴責（reprimand）。

（3）命令資料控管者及受託處理者履行當事人權利。（4）命令資料控管者及受託處理者於期限內依指定方式改善，使資料處理之方式符合 GDPR 要求。（5）發生個人資料事故時，命令資料控管者通知當事人。（6）發布暫時或終局限制，如對資料處理發布禁止令。（7）命令確實履行更正權、刪除權、限制處理權，以及進行通知。（8）撤銷受證組織之驗證標章，或命令驗證機構撤回受證組織之驗證標章，或於因未達到或不再達到驗證規則要求時，命令驗證機構不得授證。（9）處以行政罰鍰，依個案情形而定，專責機關可僅處以行政罰鍰，或與本項其他措施併同為之。（10）涉及國際傳輸時，得命令停止傳輸資料至他國或組織。最後，依第 58 條第 3 項具有之授權及建議權力包含：（1）針對資料保護影響評估結果為高風險之資料控管者進行事前諮詢並提出相關建議。（2）主動或依要求對成員國立法機關、行政機關、組織或公眾發布個人資料保護相關意見書。（3）依成員國國內法規定，核准符合公共利益之資料處理行為，雖然資料保護影響評估結果為高風險，包含與社會安全及公共衛生相關之資料處理。（4）核准行為守則及對其發布意見書。（5）審核核可驗證機構。（6）授證及核可驗證規則。（7）採用認可標準契約條款。（8）國際傳輸下核可資料控管者或受託處理者自行制定的契約條款。（9）國際傳輸下核可公務機關自行制定之行政條款。（10）核可企業自我拘束規則。

另外第 58 條第 4 項規定機關權限行使受司法救濟及正當程序保障，及第 58 條第 5 項規定機關得將違反 GDPR 規定事宜進行訴訟交由司法處理，且第 58 條第 6 項規定成員國得賦予機關除第 58 條以外的權限，惟第 58 條第 4 項至第 6 項均須具有法源。

二、英國

UK GDPR 第六章以下（第 51 條至第 59 條）該章節名稱為「委員[4]（The Commissioner）」，與 GDPR 規範大抵相同。又 DPA 2018 在

[4] The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019, LEGISLATION.GOV.UK, https://www.legislation.gov.uk/uksi/2019/419/contents (last visited June. 29,

第 114 條把「委員」與「英國資訊委員（The Information Commissioner）」作相同解釋，並在第五部分（Part 5）就英國資訊委員之功能、角色、實務守則等進行規範。因此由委員及其辦公室所組成之「英國資訊委員辦公室」（Information Commissioner's Office, ICO），為英國個人資料與隱私保護的獨立專責機構。

UK GDPR 第 58 條所賦予之調查權同 GDPR 規定，惟依 DPA 2018 第 115 條第 5 項之規定，當機關依 UK GDPR 第 58 條第 1 項第 a 款「命提供資訊」時，應先依 DPA 2018 第 142 條進行「資訊通知」（information notice），通知內容應包括命提供資訊之理由、不配合之後果、受命令之單位有申訴權等。又依 DPA 2018 第 115 條第 6 項之規定，機關依 UK GDPR 第 58 條第 1 項第 b 款「進行調查」時，應先依 DPA 2018 第 146 條進行評估通知（assessment notice），亦即要求控管者或處理者允許委員對其資料處理適法性進行評估，通知內容應包含不配合之後果、受命令之單位有申訴權及通知所施加之各項要求，並說明必須遵守該要求的期間等。另依 DPA 2018 第 115 條第 7 項之規定，機關依 UK GDPR 第 58 條第 1 項第 e 款及 f 款「獲取資訊」與「實地調查」時，應依 DPA 2018 第 154 條及附錄 15 之程序性規定進行（如應於 7 日前以書面通知將進入相關場所）。

而關於機關之糾正權，UK GDPR 沿用 GDPR 相同規定。惟依 DPA 2018 第 115 條第 8 項及第 9 項針對糾正權有所限制。首先，UK GDPR 第 58 條第 2 項第 c 款至第 h 款、第 j 款須先依第 149 條發出強制執行通知（enforcement notice），始得行使。又第 i 款則僅得透過第 155 條發出處罰通知（penalty notice），方得行使。意即在委員行使糾正權時，應預先通知受糾正對象，但受糾正對象得依第 162 條向法院提出救濟。

三、德國

依 BDSG 第 2 條第 1 項及第 2 項規定，包含聯邦個人資料保護

2022).

暨資訊自由監察官（Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI）及各邦設置之資料保護監察官（Der Landesbeauftragte für den Datenschutz, LfD）。

有關聯邦個人資料保護暨資訊自由監察官之職務權責，主要規定在 BDSG 第 8 條至第 16 條，分別為組織設立、監察官之獨立性、監察官之任用及任期、權利及義務以及相關職務權限。有關職務權限行使當監察官認為非公務機關或個人違反個資法或有相關瑕疵時，應通知主管機關，並在行使 GDPR 第 58 條第 2 項第 b 款至第 g 款、第 i 款及第 j 款前，除有立即危險或為公共利益須立即作出決定，且提供建議將與公共利益相衝突之外，應給予主管機關在合理期限內對資料控管者提供建議的機會；若屬聯邦公務機關違反個資法之情況，除所涉及的問題微不足道或在此期間已得到補救外，監察官應向聯邦最高主管機關提出投訴，並應要求該機關在一定期限內作出回應。而當預期的資料處理操作可能違反本法及其他資料保護規定，監察官亦得警告資料控管者改正。

另 BDSG 第 39 條同 GDPR 第 43 條第 1 項規定，允許在個人資料保護方面具有適當專業知識水準的認證機構於必要時行使權力，頒發及更新認證。故本條對認證機構之權力來源，明定應由聯邦或各州的監管機構授予，並另定專法《認證機構法》進行相關規範。

四、美國

（一）　CCPA 及 CPRA

CPRA 第 1798.199.10 條設立「加州隱私保護機關」（California Privacy Protection Agency, CPPA），將原 CCPA 下由加州檢察長獨立執行之權責，部分交由 CPPA 負擔。CPPA 為加州政府下的州級機構，掌管加州隱私保護相關執行事項，包括更新 CCPA、CPRA 現有規範、訂立施行規範、解釋、受理申訴、進行調查及違規案件執法、應立法機關要求提供意見諮詢、監測個人資料保護相關發展、與其他機關合作，並且在「消費者隱私基金」（consumer privacy fund）可贈予資金

的範圍內處理請求、審查及批准該贈款之申請[5]。

有關 CPPA 之調查權依第 1798.199.45 條規定，基於個人投訴或 CPPA 主動發起調查，CPPA 得調查與任何營利事業、服務提供者、承包商或個人相關可能違反本法之行為。CPPA 得決定不調查投訴，或命令營利事業限期改正其違規行為。針對不進行調查或提供更長寬限期間之決定，CPPA 得考慮事項包括是否故意違反本法、接獲投訴通知前，營利事業、服務提供者、承包商或人員為解決投訴的違規行為所付出之自願努力。而 CPPA 應以書面通知申訴人關於 CPPA 已採取或計畫受理投訴，並說明採取行動或不採取行動的原因。另外 CPPA 得傳喚證人、強制出席與作證、主持宣誓及陳述事實、取證，並透過傳喚要求出示任何書籍、紙本、記錄或其他對 CPPA 履行職責具重要性的文件或權限行使，包括但不限於稽核企業對本法的法遵性。

而 CPPA 處理違規案件之程序，首先係合理依據認定，依第 1798.199.50 條由 CCPA 認定違規指控的合理依據成立與否應符合正當程序，CPPA 應於考量違規行為前至少 30 天，告知營利事業、服務提供者、承包商、或遭到指控違反本法規定的人其違法行為。通知方式為傳票送達或掛號信以提供證據摘要，並告知被投訴者於 CPPA 考量有無合理依據認定被投訴者違法的所有相關程序中有權親自出席並委任律師代表。除非被投訴者向 CPPA 提交要求公開程序之書面請求，否則合理依據的考量程序不公開。其次係違規行為認定與處分，依第 1798.199.55 條第 a 項違規案件的認定應符合正當程序，當 CPPA 確定有合理依據相信有違反本法之行為時，CPPA 應舉行聽證會加以確定是否發生違規行為。CPPA 應根據《行政程序法》（Administrative Procedure Act, APA）規定發出通知並舉行聽證會，若確定有違規行為，則應發布命令要求違規者停止、中止行為，或處

[5] 依據 CPRA§1798.160(a), (b) (2)規定，加州州庫成立消費者隱私基金（Consumer privacy fund），CPPA 每年可就 9%基金就隱私保護事項分配與符合條件的非營利組織、公務機關、校區、執法單位等。

以罰鍰。

關於救濟程序，利害關係人得對 CPPA 之行政處分提起司法審查[6]，該行政處分則須受裁量濫用標準[7]之判斷。又第 1798.199.90 條第 c 項賦予州檢察長有權介入並接手案件，如州檢察長為進行調查或提起民事訴訟向 CPPA 請求暫停行政行為或行政調查，則 CPPA 應停止其行為或調查。

（二）　UPDPA

UPDPA 未明文設置獨立專責機關，依 UPDPA 第 16 條第 a 項規定違反 UPDPA 之執法機關、救濟、處罰依該州消費者保護法規定；另依同條第 b 項，賦予州檢察長得依該州行政程序法實施本法、訂定規則之權力。

此外，州檢察長依 UPDPA 第 11 條得承認遵守類似的資料保護法如 GDPR 或 CCPA 者，可視為符合 UPDPA；州檢察長亦得依 UPDPA 第 12 至 15 條承認自願共識標準（voluntary consensus standards），納入利害關係人所訂的行業守則作為資料保護規範。

五、日本

日本個資法第 130 條第 1 項設置之個資專責機關為個人資料保護委員會（個人情報保護委員会），隸屬於內閣總理大臣管轄，並依第 133 條獨立行使職權。個人資料保護委員會主要任務在於專責監督與管理政府各機關以及民間個人資料處理事業對於個人資料之傳輸、處理，並適時提出指導意見或建議。依本法第 132 條賦予委員會之職務包括，（1）制定及推行基本方針之相關事務；（2）監督組織就個人資料之處理情形，並協助對當事人提出申訴進行必要之調解；（3）個人資料保護團體之認證；（4）監督組織處理特定個人資料之

6　美國司法系統為一元制，行政訴訟亦由普通法院管轄，不另設行政法院。

7　裁量濫用標準（abuse of discretion standard）是美國行政法上對行政行為是否違法、可被撤銷之判斷標準；*See* also Administrative Procedure Act §706。

情形，並協助對當事人提出申訴進行必要之調解；(5)特定個人資料保護評價之相關事務；(6) 宣導及教育個人資料保護之相關事務；(7) 為執行以上事務所需之調查及研究；(8) 國際間合作之相關事務；(9) 除前揭事項以外之其他依法屬於委員會之事務。

關於其監督權限行使方式，首先係針對非公務機關之部分，個人資料保護委員會得對個人資料處理事業者等進行必要之指導、建議、命其報告、進入檢查，如有違反法令，則進行勸告、命令等。依第 146 條「報告及進入檢查」之規定，委員會得要求個人資料處理事業者提出必要之報告或資料，或得使其職員進入該當個人資料處理事業之事務所或其他必要場所，命其說明有關個資處理或檢查其他相關文件。又依第 147 條「指導及建議」之規定，委員會得對個人資料處理事業者提供處理資料之必要指導及建議，惟此指導及建議並非行政處分，亦無法律拘束力，旨在助於業者自主改善不當處理個人資料之行為。復依第 148 條「勸告及命令」之規定，委員會對於違反本法義務之個人資料處理事業者，得勸告其中止違反行為或為改正所應採取之其他必要措施。至於第 149 條「委員會權限行使之限制」，規定委員會行使上述權限均應不得妨礙表現自由、學問自由、信仰自由及政治活動自由，又對於個人資料處理事業者向第 57 條第 1 項豁免情形所列人員提供個人資料的行爲亦不得行使其權限。惟第 150 條「權限委任」之規定，委員會得將上述權限委任由事業所管大臣、金融廳長官或證券交易等監事委員會及財務局長、財務支局長行使。

其次，針對公務機關之部分，委員會在認爲有必要確保法令規定順暢運作時，亦得對行政機關等進行指導、建議、命其報告、實地調查或勸告。依第 156 條「要求提出資料及實地調查」之規定，委員會得要求行政機關首長對行政機關就個人資料處理相關事務的實施狀況，提出資料並進行說明或得使其職員進行實地調查。又依第 157 條「指導及建議」之規定，委員會得對行政機關首長就個人資料處理進行必要之指導或給予建議。復依第 158 條「勸告」之規定，委員會得對行政機關首長就個人資料處理進行勸告。另依第 159 條「基於建議所採取措施之報告要求」之規定，委員會對行政機關首長提出勸告

時，得要求該行政機關首長報告其根據該勸告所採取的措施。至於第160條「委員會權限行使之限制」，委員會就行政機關首長對第57條第1項各款規定者（限於以個別規定目的處理個人資料之情形）進行提供個人資料之行為時，不得行使其職權。

六、韓國

韓國在制定PIPA後設置個人資料保護委員會（개인정보보호위원회）掌管個人資料保護相關業務。此外，韓國訊息安全局（한국인터넷진흥원, KISA）轄下亦成立個人資料紛爭調解委員會（개인정보분쟁조정위원회）負責調解個人資料相關爭議，以作為替代性紛爭解決機制（Alternative Dispute Resolution, ADR），達成有效解決個人資料紛爭及減少訟源之目的。

關於個人資料保護委員會之權限，依PIPA第7條之8規定，包含：（1）檢視個人資料保護相關法令。（2）建立並執行個人資料保護政策、制度及計畫。（3）對當事人權利侵害進行調查及處分事宜。（4）個人資料權利救濟及相關爭議之調解。（5）與國際機構就個人資料保護之交流與合作。（6）調查、研究與教育、宣傳個人資料保護法令、政策、制度與實務相關事宜。（7）支援個人資料保護技術發展及專門人才培育。（8）依本法及其他法定所訂之規定。

至於委員會之調查權限，依PIPA第63條規定當資料控管者有下列情形之一，委員會得發動調查權要求資料控管者提出相關資料，包括：（1）有違反本法所定之事項或得知有嫌疑。（2）接獲通報或申訴時。（3）當發生個人資料事故時，為保護當事人所必要之事項。（4）稽核與行政檢查。而若資料控管者未依規定提出資料或確有違法時，委員會應進行實地查核，並得要求業者提示書面文件等相關證據。另當委員會發覺有違法之虞時，得向相關中央行政機關首長請求共同調查，如預防個人資料事故發生，委員會得會同相關中央行政機關首長為行政檢查。若委員會認定有侵害個人資料之行為，得要求中止、暫停該行為及其他必要措施，並向有搜查權之機關告發或自為懲戒、

勸告。另依 PIPA 第 64 至 66 條規定，委員會應參酌調查結果提出糾正或處罰意見，並將結果公告之。若組織不服公告結果，得依委員會書面裁罰通知書記載之救濟程序，於期限內提出異議。此外，委員會亦有行政罰鍰之裁處權，以提升執行力道。

七、新加坡

新加坡依據 PDPA 設置之專責機關為個人資料保護委員會（Personal Data Protection Commission, PDPC），隸屬於通訊及新聞部（Ministry of Communications and Information, MCI）下的資訊通信媒體發展管理局（Info-communications Media Development Authority, IMDA），而 PDPC 轄下另設有資料保護諮詢委員會（Data Protection Advisory Committee）。PDPC 成立目的在於確保企業遵守 PDPA、徵集公眾對於資料保護之意見、制定相關個人資料保護之政策與發布準則或指引、協助組織在資料利用與共享時遵守其責任，以及舉辦特定領域或公共事務之宣傳活動。

關於 PDPC 之審查權限，依 PDPA 第 48H 條規定，針對組織拒絕當事人請求提供或更正等情事，PDPC 得確認後另行決定；另針對組織向申訴人提供或更正所收取之費用，PDPC 亦得進行審核為減少或禁止該等費用。至於 PDPC 之調查權限，依第 48L 條規定，PDPC 及其內部調查員得依據申訴案或主動調查組織是否確實遵守 PDPA，接受組織的書面自願承諾書（Voluntary undertakings）以改正並防止其再次發生違法行為。又依第 50 條規定 PDPC 得裁量申訴案是否為惡意申訴或濫訴，決定受理或暫停、終止調查。

而關於 PDPC 之裁罰權限，依第 48L 條規定當組織有違法行為時，PDPC 得命令組織停止行為、銷毀違法蒐集之個人資料或對其裁罰等。惟 PDPC 考量個人申訴組織以調解方式解決更為適當，依第 48G 條得未經申訴人與該組織同意下，根據紛爭解決機制將該事宜提交調解。另依第 48N 條規定，有關第 48G 條第 2 項替代性紛爭解決、第 48I 條第 1 及 2 項之違規指示或第 48L 條第 4 項自願承諾、

或依第 48H 條第 2 項審查所作出之任何指示或決定，得依書面申請由 PDPC 重新再議（reconsideration）。而上述 PDPC 所做決定或再議，依第 48Q 條第 1 及 2 項得於法定期間向上訴小組主席（the Chairperson of the Appeal Panel）提起上訴。

八、瑞士

瑞士 DSG 2020 於第 7 節設有「聯邦資料保護及資訊委員（Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, EDÖB）作為獨立專責機關，負責個人資料保護相關事務。EDÖB 之任務依第 58 條第 1 項規定包括：（1）向聯邦機構及個人提供資料保護方面之資訊、培訓及建議；（2）協助地方機構並與負責資料保護之外國政府合作；（3）提升民眾對資料保護之重視；（4）向當事人提供有關如何行使其權利的資訊；（5）針對資料處理之法令草案及聯邦措施表示意見；（6）執行 2004 年 12 月 17 日的《公共資料法》或其他聯邦法律分配之任務；（7）開發工具以提供良好作法之建議。

有關 EDÖB 之調查權限，依第 49 條規定當有合理依據認有違法處理資料之虞，EDÖB 得依職權或接獲通知對聯邦機構或個人進行調查，除非違反情形輕微得免進行調查；又除有第 50 條第 2 項為履行保密義務外，聯邦機構或個人應向 EDÖB 提供調查所需資料及相關文件。另經相關人員申訴，EDÖB 應告知其所採取措施及調查結果。復依第 50 條規定若聯邦機構或個人未能履行合作義務，EDÖB 得在調查範圍內採行之措施包括：（1）近用調查所需相關資訊、文件、處理活動列表及個人資料；（2）進入處所及設施；（3）證人訊問；（4）專家評估。而 EDÖB 執行上述措施得召集其他聯邦機關與地方政府警察機關協助。若認組織有違法情形，依第 51 條規定 EDÖB 得命令全部或部分調整、終止或中斷處理、推遲或禁止國際傳輸，及全部或部分刪除、銷毀個人資料。另同條第 3 項規定 EDÖB 得對聯邦機構或個人作出之命令尚包括告知義務、當事人權利、資料保護影響評估、諮詢、安全維護措施等事項之通知或提供資訊。

至於 EDÖB 之處分權限，依第 60 條第 1 項規定 EDÖB 得對違法之個人處以罰鍰。另依 DSG 2020 第 56 條登記之規定，EDÖB 負責對聯邦機構的資料處理活動進行登記並公佈，並依第 57 條規定應每年向聯邦議會報告其活動情形。

貳、我國規定

我國目前在個人資料保護領域並無設置獨立之專責機關，係由中央目的事業主管機關或直轄市、縣市政府負責管轄，而因資源、預算差異等因素，對各產業在個人資料保護法遵循之監督與管理程度可能有所不同。

我國個人資料保護法賦予之調查權限，依個資法第 22 條規定，中央目的事業主管機關或直轄市、縣市政府得實施行政檢查。又依個資法第 23 條規定有關扣留物或複製物之適當處置或保管。復依個資法第 24 條規定對於要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣市政府聲明異議，並規範中央目的事業主管機關等機關，當其受理聲明異議後，有理由者應停止或變更，無理由者應繼續執行；而不得對該案件聲明不服者，得單獨提起行政訴訟。另依個資法第 26 條規定，中央目的事業主管機關或直轄市、縣市政府依第 22 條實施行政檢查後，如未發現違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。另外，依個資法第 52 條規定，中央目的事業主管機關或直轄市、縣市政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理。

至於在處分權限的部分，依個資法第 25 條規定非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣市政府除依本法規定裁處罰鍰外，並得為下列處分：（一）禁止蒐集、處理或利用個人資料。（二）命令刪除經處理之個人資料檔案。（三）沒入或命銷燬違法蒐集之個人資料。（四）公布非公務機關之違法情形，及其姓名或名稱與負責人。又中央目的事業主管機關或直轄市、縣市政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對

該非公務機關權益損害最少之方法為之。又依第 47 條非公務機關有違反個人資料蒐集、處理或利用、國際傳輸等規定者，由中央目的事業主管機關或直轄市、縣市政府處以罰鍰，並令限期改正。復依第 48 條規定非公務機關有違反告知義務、當事人權利、目的外利用、安全維護措施義務等情事者，由中央目的事業主管機關或直轄市、縣市政府限期改正，屆期未改正者，按次處以罰鍰。因此得見中央目的事業主管機關或直轄市、縣市政府對於違法者得分別處以各種裁罰性或非裁罰性之不利益處分。

參、分析與小結

一、 比較法之分析[8]

（一） 調查權之行使方式

綜觀各國法制，可見各國獨立專責機關之調查權限大致相似，多數皆類似於歐盟 GDPR 賦予獨立專責機關之調查權，主要包含命提供資訊、進行調查、通知違法情況、獲取資訊，以及實地調查等權限。而針對調查權之執行，依各國行政程序差異，在規範上略有不同，如德國要求機關須在一定之期限內作出回應；英國則強調命提供資訊應先為資訊通知、進行調查應先為評估通知；新加坡則分為持法院搜索令進入場所檢查，或在必要時透過發出通知後直接進入場所檢查。

而除了歐盟之外，多數國家並未規範怠於行政處理之救濟程序。在歐盟 GDPR 體系，若獨立專責機關未處理當事人之申訴或是未於三個月內通知調查進度或結果，當事人有權向成員國國內法院訴求司法救濟。

另在調查委外的部分，日本、韓國可委由其他單位協助進行調查。如日本有關「權限委任」規定，委員會為確保個人資料適當處理

[8] 美國之「加州隱私保護機關」及新加坡之「個人資料保護委員會」係「專責機關」，尚非「獨立機關」，惟為利於討論，仍列為本章關於「獨立專責機關」之比較法範疇。

必要及其他政令所訂事項，得將報告及進入檢查之權限委任由事業所管大臣、金融廳、證券交易監視委員會等行使；而前述機關應向委員會報告前述權限行使結果。韓國則規範資料控管者於處理個人資料有侵害資料當事人權益之虞時，受侵害者得將被侵害事實向委員會通報，委員會得依施行細則指定專門機關 KISA 之隱私申訴中心受理，進行調查與個人資料保護爭議有關之申訴案件。瑞士則有規範聯邦資料保護及資訊委員得在調查範圍內召集其他聯邦機關與地方政府警察機關執行。惟多數國家係由獨立專責機關獨立完成調查。

表 1 各國獨立專責機關有關調查權限之規範

國別	命提供資訊	進行調查	實地調查	通知違法情形	獲取資訊	稽核評估	受理申訴	提供建議	扣押或複製	傳喚取證	委外調查	其他
歐盟	O	O	O	O	O	O	O	O	O	-	-	-
英國	O	O	O	O	O	O	O	O	O	X	X	-
德國	O	O	O	O	O	O	O	O	X	X	X	-
美國 CPRA	O	O	O	O	O	O	O	O	O	O	X	聽證通知
日本	O	O	O	O	O	X	O	O	X	X	O	-
韓國	O	O	O	O	O	O	O	O	O	X	O	申訴中心
新加坡	O	O	O	O	O	O	O	O	O	O	X	-
瑞士	O	O	O	O	O	X	O	O	X	O	X	專家評估

資料來源：本計畫研究團隊自行整理

（二）　處分權之行使方式

綜觀各國法制，目前各國對於獨立專責機關之處分權限大抵內容相似。各國之處分權限主要包括發布警告、發布訓誡、命令遵循當事人要求、命令符合法規規範、命令通知侵害、課予限制、命令更正刪除、行政罰鍰、命令停止國際傳輸、執行通知（限期改正）等權限。在受處分之救濟程序上，多數國家採直接進入司法救濟程序有關救濟程序之細節，亦因各國行政程序體系而略有差異。例如美國加州檢察長雖有權優先接手案件移轉，加州隱私保護機關(California Privacy Protection Agency, CPPA)不得限制州檢察長執行本法之權力，惟若CPPA 處分已作成，則受處分企業應依據處分結果，直接進行司法救濟。而新加坡則針對替代性紛爭解決、違規指示、自願承諾或依審查權等作出之任何指示或決定，可依書面申請由 PDPC 重新再議；若不服再議結果，則可在規定期間內向再申訴小組主席提出再申訴。

至於在裁罰規範上，除美國、新加坡之個資法本身即未規範公務機關之外，僅瑞士與我國類似，針對公務機關均無裁罰相關規範，其他多數國家之獨立專責機關可針對公務機關進行裁罰。（有關公務或非公務機關之具體裁罰標準得參見第二章第二節「罰則」）另在處分權限的委外規定，日本賦予個人資料保護委員會得將勸告及命令之權限委任由事業所管大臣、金融廳長官、證券交易監視委員會等行使；而前述機關應向個人資料保護委員會報告該權限行使之結果。

表 2 各國獨立專責機關有關處分權限之規範

國別	發布警告	發布訓誡	命令遵循當事人要求	命令遵循法規	命令通知侵害	課予限制	命令更正刪除	行政罰鍰	命令停止國際傳輸	執行通知（限期改正）	裁罰公務機關	其他
歐盟	O	O	O	O	O	O	O	O	O	O	O	-
英國	O	O	O	O	O	O	O	O	O	O	O	-
德國	O	O	O	O	O	O	O	O	O	O	O	-
美國	X	X	O	O	O	O	O	O	X	O	X	-
日本	O	O	O	O	O	X	O	O	O	O	O	-
韓國	O	O	O	O	O	O	O	O	O	O	O	-
新加坡	O	O	O	O	O	O	O	O	O	X	X	得依自願承諾書裁罰
瑞士	O	O	O	O	O	O	O	O	O	O	X	-

資料來源：本計畫研究團隊自行整理

二、 小結

由於我國目前並無個資法之獨立專責機關，係由中央目的事業主管機關與縣市地方政府負責監管之事務，卻可能有各機關在資源、人力上不足的問題，導致各行業在個人資料保護上受到不同程度的監管。我國憲法法庭 111 年憲判字第 13 號判決即認為，「由個人資料保護法或其他相關法律規定整體觀察，欠缺個人資料保護之獨立監督機制，對個人資訊隱私權之保障不足，而有違憲之虞，相關機關應自本判決宣示之日起 3 年內，制定或修正相關法律，建立相關法制，以完足憲法第 22 條對人民資訊隱私權之保障。」。又判決註腳標明例如歐盟 GDPR 即規定各會員國應設置至少一個獨立監管機關，職司個人資訊隱私權之保障；該監管機關應依照 GDPR 規定獨立行使職權（GDPR 第 51 條及第 52 條參照）。由於 GDPR 條文多討論獨立專責機關之行政查察功用，若無獨立專責機關或替代機制，我國恐將難以取得歐盟 GDPR 適足性認定。而獨立專責機關的設置，得以確保個資法各項名詞定義及管理配套之一致性，如進行資料隱私衝擊評估之諮詢、指引之頒布，且在諸如資料去識別、資料可攜等議題，可能需於不同應用領域之法規進行，應由獨立專責機關負責監管，以利建構資料治理等制度達到整體環境之保障。

綜觀各國法制，在獨立專責機關之調查權限上，目前我國個資法第 22 條有關行政檢查之規範，包含進入檢查、命說明提供文件、扣留等，已有與國際立法例相似之調查權規範，此外，日本、韓國、瑞士有與外部單位合作執行調查程序；我國亦有委外調查之規定，惟係主要由各主管機關執法。多數國家於調查程序中，司法不會介入調查，惟美國得由檢察總長隨時介入調查程序，歐盟體系則僅在獨立專責機關三個月內未回覆調查進度或結果時，始得進入司法救濟。

至於在獨立專責機關之處分權限，目前我國個資法第 25、47、48 條已有規定，中央目的事業主管機關或直轄市、縣市政府對於違法者得處以不利益處分。其類型包含禁止蒐集、處理或利用個人資料；命令刪除經處理之個人資料檔案；沒入或命銷燬違法蒐集之個人

資料；公布非公務機關之違法情形及其姓名或名稱與負責人等；命改正或處以行政罰鍰。而我國相較於國際，已有類似於國際之處分權規範，惟尚由各主管機關進行執法。多數國家之獨立專責機關可針對公務機關進行處分，除美國、新加坡本身未規範公務機關之外，僅我國、瑞士之個資法並無針對公務機關之裁罰權限。另外，多數國家之獨立專責機關所作處分結果不受上級管轄，若受處分者不服獨立專責機關之處分，新加坡有採另組委員會進行審議，而其他國家則採以直接進行司法程序救濟。

綜上所述，各國獨立專責機關之監督權限行使方式，與我國目前個資法所賦予之權限並無太大差異。惟考量個人資料保護之監管機關應具有獨立性及專責性，由獨立專責機關統一監管個資法，並統一解釋法律與認定事實、執行行政裁罰、監管標準，始能促進個人資料保護的專業化，在法律監管方具備高度專業性，以及具有專屬財務與足夠人力有利推動法律之執行。又設立獨立專責機關可於個人資料保護的事前遵循與教育訓練等事務推動上，符合國際潮流並強化個人資料保護的國際合作。

第二節　罰則

壹、比較法國家

一、歐盟

（一）　有關刑事罰之規定

依 GDPR 第 84 條第 1 項規定，GDPR 將刑事罰之裁罰權限交予歐盟成員國，特別係針對 GDPR 行政罰鍰裁罰以外之事項，歐盟成員國可另立法制定刑事罰。歐盟成員國應確保刑事罰法律之落實，所訂定之刑事罰則應有效、合比例性、具遏制力。若歐盟成員國有訂立刑事罰相關法規，依 GDPR 第 84 條第 2 項規定，應通知歐盟執委會（European Commission, EC）。惟 GDPR 前言第 149 點強調，科處刑事罰與行政罰時，應遵守一罪不二罰原則（ne bis in idem）。

（二）　有關行政罰之規定

GDPR 之罰則規範係以行政罰鍰為主，又依 GDPR 第 83 條第 7 項規定，歐盟成員國得針對公務機關是否受行政罰鍰制裁及其範圍訂定國內法。關於 GDPR 所處罰之行為，依 GDPR 第 83 條第 3 項規定係以資料控管者或受託處理者意圖或過失為限。EDPB 於 2022 年 4 月發布「行政罰鍰指引」（Guidelines 04/2022 on the calculation of administrative fines under the GDPR）[9]，說明 GDPR 之行政罰鍰分為兩類，第一類規定於 GDPR 第 83 條第 4 項，即違反資料控管者與受託處理者義務、驗證規定、行為守則監督規定，得處最高 1,000 萬歐元或 2%全球年營業額，擇高者；第二類規定於 GDPR 第 83 條第 5、6 項，違反資料處理原則、當事人權利、國際傳輸、特殊資料處理情形、監管機關限制資料傳輸之命令、監管機關之調查權及糾正權等規定，得處最高 2,000 萬歐元或 4%全球年營業額，擇高者。而依 GDPR 第 83 條第 2 項規定，行政罰鍰之金額原則上非固定，乃依個案情形而定；惟監管機關在特定情形下，有權處以固定金額之行政罰鍰。

在評估是否處以行政罰鍰及衡量其金額時，首先應就個案情形評估 GDPR 第 83 條第 2 項第 a、b、g 款之情形。依本項第 a 款規定，應納入評估之具體違法事項，包含違法事項與法律要求之落差，考量資料傳輸之情形、範圍、目的、當事人數量、實際所受損害，及違法期間長短等；同項第 b 款規定應將違法行為係故意或過失納入考量；及同項第 g 款規定應將資料種類納入考量，若涉及特種個人資料或敏感個人資料，則給予較重之懲處。

再者，應判斷個案情形是否符合 GDPR 第 83 條第 2 項其他事項：

1. 依同項第 c 款規定資料控管者或受託處理者是否採取任何減免

---

9 European Data Protection Board [EDPB], Guidelines 04/2022 on the calculation of administrative fines under the GDPR (2022), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (last visited July 8. 2022).

行為以降低違法行為對當事人之傷害，如在技術或組織上所採取之措施得作為減免行為，其時間及效果亦須納入考量[10]。

2. 依同項第 d 款規定資料控管者與受託處理者負責之程度，包括對當事人自由及權利所造成的風險、對當事人所造成的傷害、資料控管者與受託處理者已採取措施但當事人持續所受的損失及所採取措施之補救情形均應納入考量因素。

3. 依同項第 e 款規定資料控管者及受託處理者有無違反 GDPR 之前例。若為累犯時，將影響量刑程度較高[11]。

4. 依同項第 f 款規定為補償其違法事項或減低所造成之傷害，資料控管者與受託處理者對於監管機關之配合度。

5. 依同項第 h 款規定監管機關知悉違反 GDPR 案件之方式，即資料控管者與受託處理者是否主動通報監管機關。

6. 依同項第 i 款規定資料控管者與受託處理者是否遵守監管機關對其施予之糾正命令。

7. 依同項第 j 款規定行為守則及驗證之遵守程度。企業通過驗證且持續維護得被視為減免因素[12]。

8. 依同項第 k 款規定其他可能影響量刑之事項，包含因違法所直接或間接取得之利益、直接或間接避免之損失、疫情之影響[13]。而量刑依個案而定，惟應遵守公平正義原則[14]。

上述行政罰之對象以法人為主，如企業負責人或其他監督管理責任者。但是當違法行為係出於私人活動或自然人所為時，仍得處罰個別自然人[15]。最後，依 GDPR 第 83 條第 1 項規定，監管機關應確

[10] *id*, at para 76-77.
[11] *id*, at para 88.
[12] *id*, at para 105.
[13] *id*, at para 111.
[14] *id*, at para 108.
[15] *id*, at para 123.

保行政罰具有效性、合比例性、遏制力。

二、英國

（一）　有關刑事罰之規定

英國關於刑事罰的種類僅有處以罰金。依據 DPA 2018 第 198 條規定因個人資料相關犯罪行為，將受到刑事追訴及相應處罰者，包含董事、經理、秘書、個人，以及法人團體。當法人團體觸犯 DPA 2018 規範之犯罪行為時，當證明係出於董事、經理、秘書或類似人員之故意、放任或疏忽下導致，前述人員均可能負有刑事責任。亦即，無論為自然人或法人均可能受有刑事追訴。

至於與個人資料相關的犯罪規定在 DPA 2018 第 170 條到 173 條，如行為人因故意或重大過失（knowingly or recklessly）未經控管者同意近用或揭露個人資料，或在取得個人資料後，未經取得個人資料時的控管者同意而保留該資料等行為。依照 DPA 2018 第 197 條規定，若要依本法起訴犯罪，需要獲得委員（Commissioner）或檢察署長（Director of Public Prosecutions）同意，且若已在犯罪事實發生 3 年後即不得再行追訴。

在 DPA 2018 中並未明定罰金額度，但依第 196 條第 1、2 項的規定，個人資料相關犯罪均屬於簡易定罪（summary conviction），而關於簡易定罪的罰金依照英國 2020 年量刑法（Sentencing Act 2020）第 122 條，處罰最高額度不超過 5000 英鎊。

（二）　有關行政罰之規定

UK GDPR 第 83 條行政罰之規定同於 GDPR 分為兩類，第一類依 UK GDPR 第 83 條第 4 項，即違反資料控管者與受託處理者義務、驗證規定、行為守則監督規定，得處最高 870 萬英鎊或 2%全球年營業額，擇高者；第二類依 UK GDPR 第 83 條第 5、6 項，違反資料處理原則、當事人權利、國際傳輸、特殊資料處理情形、ICO 之命令等規定，得處最高 1,750 萬英鎊或 4%全球年營業額，擇高者。

依 UK GDPR 第 83 條第 2 項規定得視個案情形於行政罰鍰附加或取代第 58 條第 2 項第 a 至 h 款及第 j 款所定措施（參見第二章第一節獨立專責機關監督權限行使方式）。另依 DPA 2018 第 115 條第 9 項規定當 ICO 處以行政罰鍰時，須先依 DPA 2018 第 155 條發出處罰通知（penalty notice），讓受罰者得依 DPA 2018 第 162 條向法院提起救濟程序。

三、德國

（一）　有關刑事罰之規定

BDSG 第 42 條第 1 項針對故意或未經授權將未公開之個人資料，基於商業目的予以傳輸第三方或供其取用，處以 3 年以下有期徒刑或罰金。同條第 2 項就未公開之個人資料，基於對價或基於滿足自己或侵害他人之意圖，未經授權或詐欺取得，最高得處以 2 年有期徒刑或罰金。另在程序上，依同條第 3 項規定，僅有在資料持有者、控管者、聯邦專員與監管機關等有權提出申訴之主體進行申訴程序後，始可依本條起訴相關刑責。

（二）　有關行政罰之規定

有關 BDSG 第 41 條規定主要處理 GDPR 與本法處罰之競合規定，除本法另有規定外，應適用 GDPR 第 83 條第 4 項至第 6 項之行政罰鍰規定，即違反 GDPR 第 83 條第 4 項各款事由者，最高處以 1,000 萬歐元罰鍰或 2%全球年營業額，擇高者。若違反 GDPR 第 83 條第 5、6 項各款事由者，則最高處以 2,000 萬歐元罰鍰或 4%全球年營業額，擇高者。

此外，依據 BDSG 第 43 條行政秩序罰之規定，針對故意或過失違反 BDSG 第 30 條第 1 項之規定，未能適當地處理資訊的請求；或違反 BDSG 第 30 條第 2 項未通知消費者、行為不當、不完整或延遲者，則視為違反秩序罰。依據第 42 條第 2 項之規定，違反秩序罰最高得處以 5 萬歐元罰鍰，但同條第 3 項規定於本法第 2 條第 1 項所

稱機關不得被處以罰鍰。

四、美國

（一）　CCPA 及 CPRA

CCPA、CPRA 無刑事罰則之規定[16]，依據 CPRA 第 1798.199.55 條規定，CPPA 認定營利事業有違反 CCPA、CPRA 之合理依據，經舉辦聽證後確定有違法行為時，CPPA 應發布命令要求停止、中止違法行為，並依第 1798.155 條規定處以最高 2,500 美元罰鍰；又對於各項故意違法行為、涉及未成年消費者個人資料之違法行為，處以最高 7,500 美元罰鍰，罰鍰均歸入消費者隱私基金（Consumer Privacy Fund）[17]。

而 CPPA 或法院在決定民事懲罰金額時，依第 1798.199.100 條規定得考量營利事業、服務提供者、承包商或他人之善意合作。依第 1798.199.90 條規定，營利事業、服務提供者、承包商或他人有違反 CCPA、CPRA 之行為時，除禁令外，得處以最高 2,500 美元的民事懲罰金（civil penalty）；又對於各項故意違法行為、涉及未成年消費者個人資料之違法行為，處以最高 7,500 美元的民事懲罰金，由州檢察長以加州公民之名義於法院提起訴訟並追繳。關於訴訟所得之民事懲罰金或和解金，依第 1798.199.90 條第 b 項均應存入消費者隱私基金。

---

[16] CCPA、CPRA 無刑事罰則，惟無刑事罰則並非指加州沒有與隱私侵害相關之刑事責任，因 CCPA、CPRA 係針對營利事業之消費者保護規定，並非如我國個資法針對個人資料一體適用之一般性法律；若個人資料的揭露或隱私權侵犯違反加州《刑法典》之規定，則有相關刑事處罰。

[17] CPRA §1798.160 (a)規定於州庫普通基金下設立特別基金「消費者隱私基金」，經立法部門撥款後，先行用於抵銷州法院執行 CPRA 訴訟所生的任何費用、州檢察長履行職責之支出，次用於州庫設立投資基金，將基金的所有收入及利息存入普通基金，並撥款予促進和保護消費者隱私權、教育兒童有關線上隱私、資助國際執法組織合作計畫、打擊與消費者資料洩露有關詐欺活動。

（二）　UPDPA

UPDPA 並未明定罰則規定，但為配合各州州法可能已就消費者保護法規之侵害訂定不同個人救濟的作法或規定，以及提供泛州適用 UPDPA 之彈性，故執法條文設計為可讓各州引入州消費者保護法有關罰則規定之方式。依據 UPDPA 第 16 條第 a 項規定，違反 UPDPA 之執法機關、救濟程序、處罰依該州消費者保護法規定；另依同條第 b 項規定，州檢察長得依該州行政程序法實施本法並訂定規則。故 UPDPA 主要係由州檢察長根據現有州級消費者保護法中規定的權限及罰則進行執法[18]。

五、日本

（一）　有關刑事罰之規定

日本個資法有關罰則明定於第八章，主要係對違反本法之行為處以刑事罰之規定。首先關於非公務機關之部分，以下分述之：

1. 依第 178 條規定有違反第 148 條第 2 項或第 3 項委員會之命令者，處 1 年以下有期徒刑或 100 萬日幣以下罰金。

2. 依第 179 條「不法提供資料庫罪」，規定個人資料處理事業者（法人情形包括其董監事、代表人或管理人）或其從業人員或上開等人，意圖為自己或第三人之不當利益，提供或盜用其業務所處理之個人資訊資料庫，處 1 年以下之有期徒刑或 50 萬日幣以下罰金。

3. 依第 182 條規定，有下列違法行為者處 50 萬日幣以下罰金，包括：（1）未提出依第 146 條第 1 項規定之報告或資料，或為虛偽

[18] Uniform Law Commission, *Prefatory Note*, DRAFT FOR APPROVAL UNIFORM PERSONAL DATA PROTECTION ACT, at 3, (2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=6f7e81fb-9c3e-8f4b-1907-d59fb4fa61ec&forceDialog=0P13 (last visited July 5, 2022).

之報告、提出虛偽之資料，或對該當職員之質詢不為答辯，或為虛偽之答辯、拒絕、妨礙、迴避檢查者；（2）未依第 153 條規定為報告，或為虛偽之報告者。

另針對法人之處罰，依第 184 條第 1 項規定法人之代表或法人及本人之代理人、使用人、其他之從業人員，關於其業務有違反下列各款行為，除行為者之外，對該法人處以各款之罰金刑；對上述之人處以各條之罰金：（1）違反第 178、179 條者，處 1 億日幣以下之罰金；（2）違反第 182 條者，處同條之罰金刑。

其次，關於公務機關之罰則，分述如下：

1. 依第 176 條規定行政機關現任或曾任之職員，或是現在或曾經從事第 66 條第 2 項或第 73 條第 5 項、第 121 條第 3 項的受行政機關委託處理個人資料、匿名化資料或假名化資料之受託處理者，無正當理由，而提供記錄屬於個人秘密事項之第 60 條第 2 項第 1 款之個人資料檔案（包括對該個人資料檔案之全部或一部分進行複製或是加工後之個人資料檔案），處 2 年以下有期徒刑或 100 萬日幣以下罰金。

2. 第 177 條規定委員會成員或事務局職員有違反第 143 條保密義務而洩漏秘密或盜用者，處 2 年以下有期徒刑或 100 萬日幣以下罰金。

3. 依第 180 條規定具有第 176 條身分者，意圖為自己或第三人之不當利益，提供或盜用在業務上知悉之保有個人資料者，處 1 年以下有期徒刑或 50 萬日幣以下罰金。

4. 依第 181 條規定，行政機關的職員濫用職權，意圖為供其專門職務使用以外之用途，而蒐集屬於個人秘密事項之文書、圖畫或電磁記錄者，處 1 年以下有期徒刑或 50 萬日幣以下罰金。

另外關於罰則之域外效力，依第 183 條規定第 176、177、179 及 181 條於日本境外違法者亦適用之。

（二）　有關行政罰之規定

日本個資法關於行政罰僅於第 185 條規定有下列情形之一者處 10 萬日幣以下罰鍰，包括：(1) 違反第 30 條第 2 項提供個人資料予第三方（包括準用第 31 條第 3 項提供個人關聯資料予第三方之情形）或有第 56 條冒用經認定之個人資料保護團體名稱者；(2) 未依第 51 條第 1 項規定提出申報或為不實申報者；(3) 以詐欺或其他之不當手段，基於第 85 條第 3 項規定受有以公開決定為依據保有個人資料者。

六、韓國

（一）　有關刑事罰之規定

PIPA 針對刑事罰除設有刑責之規定外，尚設有沒收或追徵之規定，以下分述之：

1. 第 70 條規定以妨害個人資料處理業務為目的，更改或刪除公務機關保有之個人資料，致公務機關執行業務有中斷或癱瘓等重大障礙者；或以虛偽或其他不當方法取得個人資料，意圖營利並以不當方法向第三方提供、教唆或幫助者，處以 10 年以下有期徒刑，併科最高 1 億韓圜罰金。

2. 第 71 條規定未取得當事人同意向第三方提供或違法蒐集、處理或利用個人資料，及洩露、毀損、變造個人資料等情形，處以 5 年以下有期徒刑，併科最高 5,000 萬韓圜罰金。

3. 第 72 條規定違反影像資料處理器設置相關規定者，處以 3 年以下有期徒刑，併科最高 3,000 萬韓圜罰金。

4. 第 73 條規定違反必要安全維護措施義務致個人資料外洩、未設置更正、停止、刪除、銷毀等措施；或資通訊業者未即時銷毀個人資料等情形者，處 2 年以下有期徒刑，併科最高 2,000 萬韓圜罰金。

若違反第 70 條至第 73 條所定任一罪並取得利益，但存有無法沒收之情事，得追徵其價額。於此情形，沒收或追徵得附加於其他刑責，一併裁處。又當法人或個人有違反第 70 條規定且未盡注意義務之情形，得對該法人之代表人、代理人、使用人及其他從業人員，處以最高 7,000 萬韓圜罰金；若違反第 71 條至第 73 條所定義務時，亦得對該個人處以對應條文之罰金刑。

（二）　有關行政罰之規定

PIPA 之行政罰規定於第十章罰則第 75 條，依照違反 PIPA 不同行為之類型，區分罰鍰與怠金。首先，關於罰鍰的規定分述如下：

1. 違反第 28 條之 6 規定假名資料處理義務者，處以 3%全球年營業額罰鍰；若無年營業額或計算顯有困難者，處以 4 億韓圜或 3%資本額，擇高者。

2. 資通訊業者違反第 39 條之 15 規定有違法運用個人資料之行為，處以 3%全球年營業額罰鍰。

委員會在裁罰時應評估之事項，包括：（1）違反之內容及程度；（2）違反之期間及次數；（3）取得利益之多寡，作為裁罰金額之核定基準。若行政罰鍰未於期限內繳納，按年利率 6%計算滯納金，並自繳納期間屆滿次日起算。

其次，關於怠金之規定，係因怠於履行 PIPA 義務所課與之金錢上處罰。PIPA 第 75 條依照違反作為義務內容而定有不同額度之怠金，並由委員會或相關中央行政機關首長課徵，違反各行為及對應之裁罰額度，以下分述：

1. 違法蒐集個人資料者（包含取得同意、特定目的內利用、告知義務、最小蒐集原則、合理必要關聯等）、未經法定代理人同意運用未成年人個人資料、設置影像資料處理器於供不特定多數人使用之更衣室等侵害個人隱私之場所，處以最高 5,000 萬韓圜怠金。

2. 違反當事人權利告知義務、拒絕當事人近用請求、資料處理未適當加密、未設置適當安全維護措施、未向當事人通知或向委員會通報個人資料事故、未遵循委員會之糾正命令等，處以最高 3,000 萬韓圜怠金。

3. 資通訊業者有違反採取保險或加入公債、提撥準備金等必要措施；或未指定國內代理人、國際傳輸前未告知當事人者，處以最高 2,000 萬韓圜怠金。

4. 違反假名化資料分別儲存及管理、委託文書未列法定事項、未公開委託內容及受託者、未訂定個人資料管理政策、未指定個人資料保護責任者等；拒絕或以虛假方式提出證據、文件等資料；拒絕、妨礙或規避行政檢查者，處以最高 1,000 萬韓圜怠金。

另第 76 條規定當有適用第 75 條相關規定時，若該行為已裁處行政罰鍰者，則不得再處以怠金。

七、 新加坡

（一） 有關刑事罰之規定

根據 PDPA 第 51 條規定，未經授權近用、更改或傳輸個人資料之行為，得處一年以下有期徒刑及最高 5,000 新幣罰金。若組織或個人有下列事由將構成犯罪，包括：

1. 為逃避當事人近用或更正之請求，處置、更改、偽造、隱藏或銷毀個人資料，或指示他人為之，處以最高 5,000 新幣罰金及一年以下有期徒刑；對組織得處以最高 50,000 新幣罰金。

2. 明知或故意未經授權揭露個人資料，或未經授權近用個人資料以謀取他人利益或對他人造成侵害、重新識別匿名化資料者，處以最高 5,000 元新幣罰金或 2 年以下有期徒刑。

3. 妨礙 PDPC 或相關人員，或故意向 PDPC 作出虛假陳述或誤導 PDPC 者，處以最高 1 萬元新幣罰金及一年以下有期徒刑，且對

組織得處以最高 10 萬元新幣罰金。

4. 拒絕遵守 PDPC 命令，或無理由拒絕提供任何資訊，或 PDPC 書面通知中指定的任何文件，處以最高 5,000 元新幣罰金及一年以下有期徒刑。

此外，根據 PDPA 第 56 條，犯有本法其他罪行且未明定刑責者，處以最高 10,000 新幣之罰金及 3 年以下有期徒刑；若為繼續犯，處以每日最高 1,000 新幣之罰金。

（二）　有關行政罰之規定

依 PDPA 第 48J 條規定，若組織故意或過失違反 PDPA 第 3、4、5、6、6A 或 6B、9 章之行為，PDPC 得發布指示要求組織停止違法蒐集、利用或揭露個人資料，或銷毀違法蒐集之個人資料、提供當事人近用權或更正權。又上述違法行為，對組織得處以最高 100 萬新幣；對個人得處以最高 20 萬新幣。在 2020 年修法後預計於 2022 年實行大幅加重罰款額度，PDPC 得對故意或過失違反 PDPA 之組織，處以最高 100 萬元新幣罰鍰或 10%全球年營業額，擇高者。

PDPC 依第 48J 條第 1 項在決定裁罰額度時，其考慮事項包括：（1）組織或個人違法性質、嚴重程度及持續時間；（2）受組織或個人違法影響的個人資料類型及性質；（3）組織或個人是否因違法而獲取任何利益或減少任何損失；（4）組織或個人是否採取任何行動來減輕違法行為之影響，以及該行動的及時性與有效性；（5）組織或個人是否已採取充分且適當之措施遵守本法要求；（6）組織或個人是否有違法前例；（7）組織或個人遵守 PDPC 依第 48I 條或 48L 條第 4 項為補救所發指示；（8）所施加裁罰是否相稱及有效；（9）罰鍰對組織或個人可能之影響，包括該組織或個人繼續其通常活動的能力；（10）任何其他可能相關的事項。

八、菲律賓

DPA 2012 第 8 章罰則針對違反行為態樣、資料類型處以不同額

度、身分效果之刑罰，以下分別說明：

1. 對於未經授權運用個人資料及敏感性個人資料之行為，依第 25 條第 1 項規定未經當事人同意或無法律授權運用個人資料者，將處以 1 年以上至 3 年以下之有期徒刑，並處以 50 萬以上至 200 萬以下比索之罰金；第 2 項規定未經授權運用敏感性個人資料，處以 3 年以上至 6 年以下之有期徒刑，並處以 50 萬以上至 400 萬以下比索之罰金。

2. 過失近用個人資料及敏感性個人資料之行為依第 26 條第 1 項規定未經本法或其他法律授權而因過失近用個人資料者，將處以 1 年以上 3 年以下之有期徒刑，並處以 50 萬以上至 200 萬以下比索之罰金;第 2 項規定未經本法或其他法律授權而因過失近用敏感性個人資料者，將處以 3 年以上至 6 年以下之有期徒刑，並處以 50 萬以上至 400 萬以下比索之罰金。

3. 不當處理個人資料及敏感性個人資料之行為，依第 27 條第 1 項明定不當處理個人資料者，包括故意或過失處理、廢棄、遺棄個人資料之行為，處以 6 個月以上 2 年以下有期徒刑，並處以 10 萬以上 50 萬以下比索之罰金；第 2 項規定不當處理敏感性個人資料者，將處以 1 年以上 3 年以下之有期徒刑，並處以 10 萬以上 100 萬以下比索之罰金。

4. 未經授權運用個人資料及敏感性個人資料之行為，依第 28 條第 1 項明定未經授權運用個人資料者，處以 1 年 6 個月以上至 5 年以下之有期徒刑，並處以 50 萬以上 100 萬以下比索之罰金；第 2 項規定未經授權運用敏感性個人資料者，將處以 2 年以上 7 年以下之有期徒刑，並處以 50 萬以上 200 萬以下比索之罰金。

5. 未經授權近用或故意違反之行為，依第 29 條規定對於故意非法侵害資料機密與安全制度者，處以 1 年以上 3 年以下之有期徒刑，並處理 50 萬以上 200 萬以下比索之罰金。

6. 隱瞞涉及敏感性個人資料的安全漏洞之行為，依第 30 條規定對於明知安全漏洞而故意或隱瞞事實者，處以 1 年 6 個月以上至 5 年以下之有期徒刑，並處以 50 萬以上 100 萬以下比索之罰金。

7. 惡意揭露之行為，依第 31 條規定任何個人資料控管者或處理者、官員、僱員或代理人，出於惡意，揭露所取得的任何個人資料或敏感性個人資料有關之無根據或虛假資料，處以 1 年 6 個月以上至 5 年以下之有期徒刑，並處以 50 萬以上 100 萬以下比索之罰金。

8. 未經授權揭露之行為，依第 32 條第 1 項規定任何資料控管者或資料處理者及官員、雇員、代理人未經當事人同意，向第三方揭露前條之個人資料者，處 1 年以上 3 年以下之有期徒刑，並處以 50 萬以上至 100 萬以下比索之罰金；第 2 項規定若揭露前條之敏感性個人資料者，則處以 3 年以上至 5 年以下之有期徒刑，並處以 50 萬以上至 200 萬以下比索之罰金。

而依第 33 條結合或接續犯之規定，有第 25 條至第 32 條任何結合或接續之行為者，處以 3 年以上至 6 年以下之有期徒刑，並處以 100 萬以上至 500 萬以下之罰金。另依第 34 條責任範圍之規定，當行為人是公司、合夥企業或任何法人，應根據具體情形對參與犯罪或因重大過失允許犯罪的負責人處以刑罰；若為法人時，法院得依本法暫停或撤銷其本法之權利；若為外國人時，除依本法處罰外，經執行刑罰後得逕將其驅逐出境；若為公務員或公務機關雇員時，因謊報或本法第 27 條、第 28 條行爲被判有罪時，除依契約為處罰外，尚應視情形予以永久或暫時完全喪失職務資格。再者，依第 35 條之規定，涉及超過 100 人以上大規模個人資料之行為，依行為類型得處以對應之最高刑。最後，依第 36 條公務人員犯相關行為之規定，即行為人為菲律賓《行政法典》（Administrative Code of the Philippines）所稱之公務人員尚應適用褫奪公權等從刑。

貳、我國規定

一、有關刑事罰之規定

我國個資法有關刑事罰規定於第 41 至 46 條。依個資法第 41 條規定，意圖為自己或第三人不法之利益或損害他人之利益，而違法蒐集、處理或利用個人資料及特種個人資料或國際傳輸，足生損害於他人者，處 5 年以下有期徒刑，得併科新臺幣 100 萬元以下罰金。又依個資法第 42 條規定，意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處 5 年以下有期徒刑、拘役或科或併科新臺幣 100 萬元以下罰金。關於第 41 條修正之說明，行為人非意圖為自己或第三人不法之利益或損害他人之利益，而違反本法相關規定者，因其可受非難性之程度較低，原則以民事損害賠償、處以行政罰為已足。惟行為人如有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定，因其可受非難性之程度較高，仍有以刑罰處罰之必要，爰為本條之修正。故可見目前我國個資法之刑事罰，乃依行為人之意圖限縮處罰之範圍，並限定於意圖為自己或第三人不法利益或損害他人利益之情形。

此外，第 43 規定中華民國人民在中華民國領域外對中華民國人民犯前二條之罪者，亦適用之；第 44 條公務人員加重條款，針對公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一；第 45 條規定本章之罪，除犯第 41 條或對公務機關犯第 42 條外，須告訴乃論；第 46 條犯本章之罪，其他法律有較重處罰規定者，從其規定。

二、有關行政罰之規定

我國個資法有關行政罰之罰則，依個資法第 47 條規定，非公務機關有違反蒐集、處理或利用個人資料及特種個人資料或國際傳輸之情形，由中央目的事業主管機關或直轄市、縣市政府處新臺幣 5 萬元以上 50 萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰

之。又依第 48 條規定，非公務機關有違反告知義務、當事人權利、行銷方式、適當安全維護措施義務之情事之一者，由中央目的事業主管機關或直轄市、縣市政府限期改正，屆期未改正者，按次處新臺幣 2 萬元以上 20 萬元以下罰鍰。因此依據違法行為之類型，有分為強制依法限期改正之先行程序，或得以併行處罰之規定。

此外，依個資法第 49 條規定，非公務機關無正當理由違反第 22 條第 4 項行政檢查之規定者，由中央目的事業主管機關或直轄市、縣市政府處新臺幣 2 萬元以上 20 萬元以下罰鍰。又依個資法第 50 條規定，非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。因此在行政罰之裁罰對象，除了得對法人處以罰鍰，亦得對法人之代表人等自然人處以同一額度之罰鍰。

參、分析與小結

一、 比較法之分析

（一） 刑事罰之規範

綜觀各國法制，除美國 CPRA 未訂有刑事罰之規範，歐盟 GDPR 亦無統一規範刑事罰，其他國家則均有刑事罰之規範。其中歐盟 GDPR 係將刑事罰的訂定權限授權給予各成員國，於各自國內法訂定刑事罰之規範，惟各成員國訂定後應向歐盟 EDPB 報備。目前英國、德國、日本、韓國、新加坡、菲律賓均有明定刑事罰之相關規定，處罰行為主要針對明知、違反委員會命令、偽證等情形有以刑事罰規範，並對主觀要件有故意、意圖營利，或施以不當手段者處以較重之罰責。在處罰類型主要有財產刑及自由刑兩者，以下分別說明：

1. 多數國家之財產刑係採固定額度上限，如英國最高為 5000 英鎊以下罰金、日本最高為 100 萬日幣以下罰金、韓國最高為 1 億韓圜以下罰金、新加坡最高為 1 萬新幣以下罰金、菲律賓最高為 400 萬比索以下罰金。而德國刑事罰則係依犯罪行為人

之收入、財產及其他量處每日額罰金額之基礎，最高為 360 日整日額（此為德國刑事法特殊計算方式）。

2. 各國針對自由刑之額度多為 1 至 3 年，德國、日本、韓國、新加坡、菲律賓均有採自由刑作為刑事罰懲罰手段。如德國最高為 3 年以下有期徒刑、日本最高為 2 年以下有期徒刑、韓國最高為 10 年以下有期徒刑、新加坡最高為 3 年以下有期徒刑、菲律賓為 1 年以上 5 年以下有期徒刑。

在有刑事罰則之國家，均有處罰主觀要件有過失之行為，如英國、德國、日本、韓國、新加坡、菲律賓。惟多數國家並未依據行為人之意圖限縮刑事罰之範圍，僅韓國針對「以妨害個人資料處理業務為目的」及「以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供、教唆或幫助者」另設有較重之刑事罰則。又日本、韓國、菲律賓亦針對行為人之身分訂有特別規定，如日本、菲律賓針對公務員身分有加重處罰之規定，韓國則針對資通訊業者設有資通訊業者專章特別義務規範。其中僅有菲律賓針對違反個資法之數個犯罪行為樣態有結合或接續之狀態，設有加重刑事處罰之規定。

另在各國刑事罰之客觀要件各不相同，除了各國刑事法體系本有存在差異之外，亦有部分事項特別以刑事罰處罰之。例如，日本將違反個人資料保護委員會命令等行為納入刑事罰規範，新加坡則將未經同意行使當事人權利、更改、偽造、隱藏或銷毀，或教唆者拒絕提供委員會資料或偽證等納入刑事法規範。

表 3 各國針對刑事罰之規範

國別	有無刑事罰	財產刑額度	自由行額度	是否處罰過失	是否依據意圖限縮刑事	身分特別規定	是否針對法人處罰
歐盟	各國自行訂定	—	—	—	—	—	—
英國	O	固定額度	—	O	X	X	O
德國	O	—	3 年以下	O	X	X	O
美國	X	—	—	—	—	—	—
日本	O	固定額度	2 年以下	O	意圖為自己或第三人不當利益，將業務所處理資料庫提供或盜用	公務員加重	O
韓	O	固定額	10 年	O	針對十年刑責	違反資通訊業	O

國		度	以下		有主觀意圖要件	者專章規定	
新加坡	O	固定額度	3 年以下	O	X	X	O
菲律賓	O	固定額度	5 年以下	O	出於惡意揭露所取得之個人資料	公務員加重	O

資料來源：本計畫研究團隊自行整理

（二）　行政罰之規範

綜觀各國法制，目前多數國家針對個資法設有行政罰之規定，如歐盟體系、英國、美國、日本、韓國、新加坡均有於個資法罰則中訂定行政罰之處罰。行政罰主要裁罰類型為罰鍰，在是否係固定額度上限或依受處分對象規模調整，各國規範並不相同，以下分別說明：

1. 歐盟 GDPR、德國、英國、新加坡、韓國係依據受處分對象規模計算比例，調整裁罰金額。

(1) 歐盟 GDPR、德國處最高 2,000 萬歐元或 4%全球營業額。（依較高者）

(2) 英國最高 1750 萬英鎊或前一會計年度全球年營業額之 4%。（依較高者）

(3) 新加坡原為固定額度上限，2020 年修法後大幅加重罰款額度及增加依比例計算之規定，一般中小企業仍維持固定額度，

上限最高 100 萬新幣；新加坡年營業額 1000 萬新幣以上之組織，最高處新加坡年營業額 10%。

(4) 韓國則為 4 億韓圜或資本額 3%。（依較高者）

2. 美國、日本罰鍰係固定額度上限

(1) 美國 CPRA 規範對象已排除小規模企業，故 CPRA 罰鍰額度雖可調整，其考量因素不包括處分對象規模，而係企業的善意合作作為。罰鍰最高為 2,500 美元，或於每項故意違規行為、每項涉及未成年消費者個人資料的違規行為處以最高 7,500 美元行政罰鍰。

(2) 日本為固定罰鍰額度上限，最高為 10 萬日幣以下罰鍰。

在處以行政罰前是否須有先行程序，目前各國均未明定要求機關須先命其改正，始得處罰。歐盟體系、英國、美國、日本、韓國、新加坡皆未要求專責機關須先命令其改正後，如處罰對象仍未改正，再進行行政裁罰。另外，多數國際立法例於法人處罰時，未同時於個資法規範處罰其負責人或其他有監督管理責任者。目前多數國家均針對法人設有行政罰之規定，但除新加坡以外，多數國家未處罰其負責人或其他有監督管理責任者；而新加坡則處罰組織高層或參與管理且可影響違法行為之個人，若同意、縱容或與他人共謀實施違法行為，或以任何方式（包括作為與不作為）明知、可得而知或可預期其涉及或參與組織違法行為，而未採取一切合理步驟防止或制止者，一經確定，應受到相應的懲罰。

至於日本、韓國雖無針對負責人之行政罰，但在刑事部分，尚得對該法人之代表人、代理人、使用人及其他從業員課處對應條文之罰金刑。除美國、新加坡未規範公務機關外，多數國際立法例皆有針對公務機關處以行政罰之規定。

表 4 各國針對行政罰之規範

國別	有無行政罰	罰鍰係固定額度上限，或得依據受處分對象規模調整	是否以命令改正為前提	是否針對法人處罰	是否處罰其負責人或其他有監督管理責任者	裁罰公務機關
歐盟	O	併行	X	O	X	O
英國	O	併行	X	O	X	O
德國	O	併行	X	O	X	O
美國	O	固定額度	X	O	X	—
日本	O	固定額度	X	O	X	X (另有刑事罰)
韓國	O	併行	X	O	X	O
新加坡	O	併行	X	O	§52 同意知情或未盡防止義務者	—
菲律賓	X	—	—	—	—	— (另有

						刑事罰)

資料來源：本計畫研究團隊自行整理

二、 小結

首先在刑事罰之規範，我國現行個資法第 41 至 46 條針對刑事罰之規定均有處罰故意犯，而未處罰過失犯，刑責最高得處 5 年以下有期徒刑，且得併科新臺幣 100 萬元以下罰金，另針對公務人員有加重處罰之規定。而各國雖有部分國家在行政罰會依據受處分對象規模調整，但在刑事罰之罰金部分，皆似我國係採固定額度上限之作法。至於各國在罰金之額度換算大約為 20 萬至 200 萬新臺幣區間，我國為 100 萬新臺幣以下，在各國罰金之額度屬居中之位置。

目前國際立法例僅韓國有特別針對意圖部分課予加重刑責規定，多數國家則未針對意圖限縮刑事罰範圍，且有處罰過失情形，處罰範圍較大。我國原則以民事損害賠償、行政罰，將刑事罰限縮在行為人有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定之情形。至於日本、新加坡針對有違反主管機關命令或偽證等情形處以刑事罰之規範，若未來我國設置個人資料保護之獨立專責機關，亦可考慮增加相關刑責規定。

其次，各國在行政罰之規範可見，相較於國際立法例未要求機關須先命其改正才可處罰，我國則在個資法第 47 條至第 50 條針對行政罰規定中，分別有不同規範。針對第 47 條為同時命改正及處罰；第 48 條則須先命改正，未依命令改正者再為行政罰鍰；第 49 條則無命改正相關規定。又多數國際立法例有裁罰公務機關，我國則未針對公務機關有裁罰機制。而在非公務機關之部分，我國另針對非公務機關受罰鍰處罰時，其代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰；新加坡亦有處罰負責人之規定，但要件限縮於明知違反個資法等情形。

另在罰鍰額度的規定上，歐盟體系、英國、新加坡、韓國係依據

受處分對象規模調整罰鍰之額度，以針對不同規模的對象達成懲罰之效果，而我國罰鍰則係採固定額度上限。又綜觀各國行政罰之規定，主要係針對違反資料運用之合法要件、控管者義務、當事人權利、目的外利用、國際傳輸、妨礙調查等情形規範，且針對特種個資之處理設有較重的罰則。而較具特色的規範模式，如美國僅有行政罰，菲律賓則無行政罰之規範。

綜上所述，由於個人資料之保護，有賴於個資法之罰則作為最後一道防線，嚇阻違法蒐集、處理或利用個人資料之各種行為態樣。我國個資法之罰則規定，由於規範之行為態樣本與各國有所差異，又不論罰金或罰鍰之額度，對於科技巨頭或大型電子商務企業均難以達到相應之懲罰效果。未來我國如設立獨立專責機關後，在處分權限及罰則之規範應做相應之調整，以促使公務機關與非公務機關落實個人資料保護。

第三節　共通規定

第一項　豁免情形

壹、比較法國家

一、歐盟

依 GDPR 第 2 條第 2 項，符合下列情形之一者，為全域豁免，得免除 GDPR 之適用，包括：

1. 歐盟法領域外的活動（outside the scope of Union law）。本情形涉及歐盟立法權，歐盟法中僅有針對特定的主題予以歐盟有立法權（union competence）。歐盟的立法權分為絕對立法權，即會員國不得針對該類主題立法，如海關議題等；關於優先立法權，即當歐盟已針對該主題立法時，會員國則不得進行立法，如能源議題等；而關於平等立法權，即歐盟或會員國兩者皆可立法，如教育

議題等[19]。

2. 外交安全政策綱領規範之活動（common foreign and security policy），如政黨、人權侵犯（human rights violations）相關之活動。

3. 自然人之個人或私人活動（purely personal or household activity），歐盟法院判定本情形僅適用於與個人私生活或家庭相關活動。舉例而言，CCTV 影像如攝影範圍超過私人住宅，則不適用本豁免情形[20]。

4. 辦理刑事案件之機關。

二、英國

英國個人資料保護規範同時涉及 UK GDPR 及 DPA 2018，其中以 UK GDPR 為主要規定，而 DPA 2018 訂有更詳細之說明。首先，關於全域豁免之規定，依 UK GDPR 第 2 條第 2 項，於下列情形得排除本法適用，包括：

1. 單純個人或家庭活動過程中對個人資料之處理。

2. 主管機關出於任何執法目的處理個人資料，依 DPA 2018 第 29 條包括主管機關完全或部分透過自動化方式處理個人資料，及由主管機關以自動化以外的方式，處理構成歸檔系統一部分的個人資料。

3. DPA 2018 第 4 部分之情報服務處理，依 DPA 2018 第 82 條包括情報部門完全或部分通過自動化方式處理個人資料，及由情報部門以自動化以外的方式，處理構成歸檔系統一部分的個人資料；此部分所稱之情報部門，包含英國安全局（Security Service）、英

[19] ROSEMARY JAY, DATA PROTECTION LAW AND PRACTICE 230-231 (5th ed. 2020).
[20] *id*, at 236.

國祕密情報局（Secret Intelligence Service）以及政府通信總部（Government Communications Headquarters）。

而關於部分豁免之規定，依 DPA 2018 第 15 條對於本法所賦予資料控管者義務及當事人權利，於特定情形得有部分豁免，包括：

1. 犯罪、稅務、移民。

2. 維持公眾保護功能、監察功能等公共機能。

3. 衛生、社會、教育工作者進行資料測試時。

4. 其他商業行為如法律專業特權、自證其罪、企業融資等。

5. 新聞、學術、藝術、文學等表意自由相關。

6. 研究、統計、公益目的之歸檔。

各種情形有對應之不同豁免範圍，詳細規定得參酌本文第二章第六節第三項「權利限制規定」之說明，此處不再贅述。另依 DPA 2018 第 16 條第 1 項第 b 款規定，內閣大臣有權限制 UK GDPR 第 23 條第 1 項權利義務範圍以維護公共利益；而本項第 c 款規定，內閣大臣得於必要時依 UK GDPR 第 85 條第 2 項規定，豁免 UK GDPR 部分章節以協調個人資料保護與言論及資訊自由。最後，依 DPA 2018 第 26 條第 1 項及第 2 項第 b 款基於國家安全及防衛目的，得豁免 UK GDPR 第二章個人資料處理原則、第三章當事人權利、第 33 條、第 34 條、第五章國際傳輸、第 57 條、第 58 條、第八章救濟與責任及罰則等，以及 DPA 2018 的第 17 條、第 115 條、第 119 條、第 142 至 154 條、第 170 至 173 條、第 187 條。

三、德國

BDSG 在規範豁免情形上與 GDPR 相似，均包含歐盟法領域外的活動、外交安全政策綱領規範之活動、自然人之個人或私人活動及辦理刑事案件之機關。依據 BDSG 第 1 條規定本法適用對象包含聯

邦政府、各邦政府以及適用於非公務機關全部或一部以自動化方式運用個人資料，且適用其他非自動化方式處理而構成檔案系統之一部分或旨在構成檔案系統之一部分個人資料。但當事人所為之單純個人或家庭活動，則不適用本法之規定，此係因 BDSG 於 2018 年 5 月 25 日生效後，規範更為複雜、影響層面更大，因此將當事人所為單純個人或家庭活動所蒐集、處理或利用之個人資料，豁免於 BDSG 適用範圍之外，以免影響到一般人民的日常生活。

四、美國

（一）　CCPA 及 CPRA

關於 CCPA 及 CPRA 之豁免情形得分為以下類型：

1. 基於其他法令，依 CPRA 第 1798.145 條第 c 項醫療資料、第 d 項信用資料處理活動、第 e 項金融資料、第 f 項駕駛人資料均已受其他法令規範，故排除本法適用，惟不豁免第 1798.150 條有關營利事業因違反為保護個人資料所實施、維護合理安全程序及操作實務之義務時，對個人資料侵害所應負之責任。

2. 公開可得資料，依第 1798.140 條第 v 項排除於個人資料定義，故不受本法規範。

3. 特定責任豁免規定，依第 1798.140 條第 i 項營利事業向服務提供者、承包商揭露個人資料，當服務提供者、承包商有違反 CCPA、CPRA 之情形，營利事業若並無實際知悉（actual knowledge）或無理由相信（no reason to believe）服務提供者或承包商意圖違法，則免除責任。

4. 勞雇關係資料，依第 1798.145 條第 m 項第 1 款規定排除本法適用，其條件係營利事業蒐集個人資料是基於該人為營利事業的應徵者、員工、所有人、主管、醫療工作人員、獨立承攬人（independent contractor），且於該職務環境範圍內蒐集；或營利事業蒐集個人資料是基於該人為營利事業的應徵者、員工、所有

人、主管、醫療工作人員、獨立承攬人，且蒐集之資料僅用於緊急聯絡；又或營利事業蒐集個人資料是基於該人為營利事業的應徵者、員工、所有人、主管、醫療工作人員、獨立承攬人，且保留個人資料是為了管理與上訴有關之其他自然人的利益所必要，並僅在管理該等利益的範圍內蒐集、運用個人資料；惟不豁免第 1798.150 條對個人資料安全侵害所應負之責任。

5. 工作單位之機關手足，依第 1798.145 條第 n 項第 1 款規定，若係反映自然人作為其他公司、合夥公司、獨資經營、非營利組織或公務機關的員工、所有人、主管、醫療工作人員、獨立承攬人，「僅在提供或自該公司接收產品或服務、善盡相關責任時，與營利事業文書或口頭溝通」之個人資料，則排除本法課予營利事業之義務。

6. 特定主體情境豁免規定，依第 1798.145 條第 o 項第 1 款規定，「商業信用報告機構」（commercial credit reporting agency）所蒐集、處理、販售或揭露業務負責人（business controller）之資料，如僅用於聯繫消費者，或識別消費者與其所擁有事業的關係，則 CCPA、CPRA 賦予之刪除權、退出個資販售及分享權的規定將排除適用。

（二）　UPDPA

有關 UPDPA 之豁免情形規定於本法第 3 條，首先本法並不適用公務機關，而得豁免的資料類型依第 3 條第 c 項規定，包括：（1）已公開可得之資料；（2）人體試驗研究資料；（3）法院令狀要求資料；（4）資訊公開法規要求之公開資料；（5）勞雇資料。其中所謂「已公開可得之資料」，依第 2 條包括：（1）政府紀錄中合法提供之資料；（2）在廣泛傳播的媒體上向公眾開放之資料，如電視、網站論壇；（3）可從公開場所觀察之資料；（4）個人可合理認為資訊係合法地向公眾提供。

另關於已受其他聯邦法律規範而豁免之資料處理態樣，依第 11

條第 b 項規定，受特定聯邦隱私法制約束的資料處理，資料控管者、處理者的資料處理若已符合聯邦法制對該類型資料處理之規定者，視為符合 UPDPA 之規範。該條所稱聯邦法制包括：HIPAA、《公平信用報告法》（Fair Credit Reporting Act, FCRA）、《金融服務法現代化法》（Gramm-Leach-Bliley Act, GLBA）、《駕駛人隱私保護法》（Drivers Privacy Act of 1994）、《家庭教育權利及隱私法》（Family Education Rights and Privacy Act of 1974, FERPA）、《兒童線上隱私保護法》（Children's Online Privacy Protection Act of 1998, COPPA）。

五、日本

日本個資法針對非公務機關之豁免情形，依第 57 條「適用除外」規定，第 1 項共有四款情形，包括：（1）廣播機關、新聞社，通訊社及其他報導媒體（包含以報導為業之個人）供報導之用，所稱「報導」係指將客觀事實告知非特定且多數人（包括基於此陳述意見或見解）。（2）以著述為業者，供著述之目的利用。（3）宗教團體為供宗教活動（包含其附隨活動）目的之利用。（4）政治團體為政治活動（包含其附隨活動）之目的之利用。惟依同條第 3 項規定，仍應致力採取資料安全管理上必要且適當之措施，有關個人資料處理上申訴之處理，及其他為確保個人資料適當處理之必要措施，並公告內容。

而公務機關之豁免情形規定於第 124 條「適用除外」，第 1 項規定在刑事案件或少年保護案件相關之裁判、檢察官、檢察事務官、司法警察所為之處分、刑罰或者保護處分的執行、更生緊急保護、赦免有關之保有個人資料，不適用本法第 5 章公務機關之義務第 4 節「開示、更正及停止利用」部分。而同條第 2 項規定，在保有個人資料（以記錄在行政機關資訊公開法第 5 條規定之專門記錄不公開資訊的行政文書為限）中，由於尚未進行分類及作其他整理，且有關相同利用目的之資訊數量龐大，而在其中檢索特定之保有個人資訊明顯困難時，於適用第 4 節規定則視為未被行政機關所保有者。

六、韓國

韓國 PIPA 有關豁免情形，分為第 58 條「部分豁免」以及第 58 條之 2「全域豁免」規定。

首先有關「部分豁免」之規定，以下分述之：

1. 符合下列各款之一者，不適用第 3 章至第 7 章規定[21]：(1) 公務機關處理依《統計法》所蒐集之個人資料。(2) 以國家安全為目的所蒐集或被要求提供之個人資料。(3) 與公共衛生等公共安全及利益有關，並須為緊急且必要處理之個人資料。(4)媒體報導、宗教團體傳教、政黨推薦候選人等目的所蒐集、處理及利用之個人資料。

2. 依第 25 條合法公開設置影像資料處理器所處理之個人資料，不適用第 15 條蒐集處理原則、第 22 條取得當事人同意之方式、第 27 條第 1 項及第 2 項移轉個人資料予第三方之限制、第 34 條個資外洩通報義務及第 37 條停止處理要求之規定。

3. 資料控管者為經營校友會、俱樂部等聯誼團體而處理個人資料時，不適用第 15 條、第 30 條個資處理方針及第 31 條指定個資保護專員之規定。

然而上述情形，仍應於達成目的所需之最短期限處理最少量之個人資料，並應採行技術上必要保護措施、設置處理申訴管道及其他適當管理措施。

其次，關於「全域豁免」依第 58 條之 2 規定，除了匿名化資料之情形，得排除 PIPA 之適用。當個人資料涉及與執行公務、國家安全、公共安全及福祉有關之政府行為，以及基本權競合(如集會結社、

21　PIPA 第 3 章至第 7 章分別規範：處理假名資料、個人資料安全管理義務、資料當事人的權利保障、資通訊服務提供者處理個人資料，以及個人資料紛爭調停委員會之相關規定。

言論自由）等合理事由，亦得排除 PIPA 之適用。

七、新加坡

新加坡 PDPA 第 4 條第 4 項第 1 款，規定本法第 3 條個人資料保護責任之一般規定、第 4 條個人資料蒐集與利用及揭露、第 5 條個人資料之近用及更正、第 6 條個人資料保管、第 6A 條資料外洩通知及第 6B 條資料可攜權等部分，排除個人家庭活動、組織員工以及公務機關之適用。另依同項第 2 款針對以書面形式證明或訂立契約之資料中介處理，或代表另一組織並為之目的處理個人資料之情形；依同項第 4 款規定已存在至少 100 年記錄之個人資料，或已故超過 10 年之亡者個人資料；及同項第 5 款規定，除商業契約明訂外之商務聯繫資訊（business contact information），如姓名、職位或頭銜、業務電話號碼、業務地址、業務電子郵件等，以上均排除 PDPA 之適用。

此外，依第 62 條規定，經部長批准後，PDPC 可於公報（Gazette）發布命令，豁免特定類別之個人或組織，不受本法之全部或部分條款之拘束，但須遵守其指定之條款或條件。

八、菲律賓

菲律賓之 DPA 2012 有關豁免情形之規定，依第 4 條明定本法適用於所有類型之個人資料，以及參與運用個人資料之任何自然人及法人，包含雖未在菲律賓設立，但使用設備設於菲律賓之資料控管者與資料處理者。惟本法並不適用於以下情形：

1. 任何現職或曾任職於政府機關之個人，與其職位和職能相關之資料，包含該個人現職或曾為政府機關之官員或職員之事實、頭銜、工作地址及辦公室電話號碼、職位、薪資範圍及職責；以及該個人任職於政府機關時，工作過程中於文件填寫的名字。

2. 任何過去與現在，個人為政府機關提供服務所訂之契約，包含契約條款以及於提供服務過程中所提供之個人姓名。

3. 任何與社會福利相關之個人資料，如包含個人姓名及福利類型之許可證。

4. 為新聞、藝術、文學或研究目的而運用之個人資料。

5. 政府機關為執行其職務所需之個人資料。

6. 《反洗錢法》及其相關法律所需之個人資料。

7. 外國法具備管轄權之個人資料，包含最初自外國蒐集與目前於菲律賓運用之個人資料。

此外，依《資料隱私法施行細則》（Implementing Rules and Regulations of the Data Privacy Act of 2012, IRRDPA 2012）第 5 條規定除有上述情形，本法與本規則不適用於以下特定資料，僅限於相關目的、功能或活動所需的最低限度蒐集、近用、利用、揭露或其他運用範圍，包括：（1）依相關法律、規定或倫理標準爲條件，以公共利益爲研究目的運用之個人資料。（2）根據憲法或法定授權有關執法或監管之職能，包括獨立的中央貨幣機關職能，在法律規定爲履行公共權力職能所必需的資料。（3）在遵守《信用資訊系統法》（Credit Information System Act, CISA）所必需的範圍內，銀行、中央貨幣機關或菲律賓中央銀行管轄的其他金融機構及法律授權的其他機構所必需的資料，包括《反洗錢法》及其相關法律所需之個人資料。

另依 DPA 2012 第 5 條有關記者及其消息來源提供保護之規定，明定本法賦予任何新聞報導的出版者、編輯者或合法授權的記者，免於被迫揭露該公眾刊登的任何新聞報導或出版物內容資訊的來源。惟不適用本法及本規則之資料控管者及資料處理者，仍須遵守採行個人資料保護安全措施，且前述個人資料的運用僅限於實現特定目的、功能或活動所需的最小限度內免除法律要求。

九、瑞士

瑞士 DSG 2020 有關豁免情形之規定，依第 2 條第 1 項本法規範

對象主要為私人（包括自然人及法人）與聯邦機構。而依同條第 2 項本法不適用之情形包括：

1. 自然人基於個人使用所處理的個人資料。

2. 聯邦議會及議會委員會在審議期間處理的個人資料。

3. 未決之民事訴訟程序、刑事訴訟程序、國際互助程序、憲法程序以及除一審程序外的行政訴訟程序。

4. 基於民法的公開登記。

5. 國際紅十字會所為的資料處理。

另依同條第 4 項規定民法的公開登記，當聯邦法律有特別規定者，將受其拘束；若無規定者，始適用本法規定。

貳、我國規定

我國個資法第 51 條第 1 項：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」。本條立法理由係依修正條文第 2 條第 8 款規定，個資法所稱非公務機關包括自然人，惟有關自然人為單純個人（例如：社交活動等）或家庭活動（例如：建立親友通訊錄等）而蒐集、處理或利用個人資料，因係屬私生活目的所為，與其職業或業務職掌無關，如納入個資法之適用，恐造成民眾之不便亦無必要，爰增訂第 1 項規定，予以排除。

又網際網路上張貼之影音個人資料，亦屬表現自由之一部分，為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意始得為之，且其本身共同使用之合法目的亦已相當明確，則應不適用於個資法規定，而回歸適用於民法規定。而參照法務部 104 年 11 月 5 日法律字第 10403514100 號函，實務見解認為係根據該行為之目的進行判斷。舉例而言，民眾於公職人員選舉開票作業之公開活動中進

行攝影，如僅為單純個人活動目的而蒐集自然人之資料，或僅攝影不特定自然人影像且未與其他個人資料結合時，尚無個資法之適用。又參照法務部 106 年 2 月 15 日法律字第 10603502190 號函，實務見解認為消防人員於執行緊急救護勤務中所錄存之影音資料若涉及可直接或間接識別特定個人之資料，自有個資法之適用。故並未因可能係公開場所或公開活動之影音資料，而逕引為公務機關（消防機關）豁免適用個資法之依據。

參、分析與小結

一、 比較法之分析

綜觀各國法制，可將常見的豁免類型概分政府行為、私人活動或其他私領域行為，以及基本權競合等三類；又針對不同豁免類型可分為全域豁免（例如具有歐盟 GDPR 第 2 條第 2 項所規定之四種豁免情形之一者得排除整部 GDPR 之適用），以及細分為部分豁免之情形，如下說明：

1. 「政府行為」主要包含統治行為、公務機關執行公務、刑事案件機關程序、刑事案件或少年保護案件之程序、議會訴訟程序等。目前歐盟、日本、韓國等國家在刑事訴追過程等程序上，因有其他法律調和，故於個資法有豁免。

2. 「私人活動或其他私領域行為」則主要為個人日常活動、單純個人或家庭活動、商業契約或商業活動、民法公開登記、受雇或應徵資料等。在個人家庭活動之部分，幾乎所有國家皆有豁免，較無爭議；受雇應徵資料、或企業內部管理為美國特別強調；商業契約則為新加坡特有規範。

3. 「基本權競合」則有例如新聞媒體或出版自由、宗教自由、政治自由、學術自由、藝術自由等基本權利，該相關權利與隱私權競合。例如歐盟體系特別針對言論自由相關權利（如新聞目的及學術、藝術及或文學表意目的）有部分豁免規定；日本、韓國等國

家則有進一步針對宗教、政治等權利給予部分豁免；有關新聞、藝術、文學或研究目的，菲律賓為全域豁免。

表 5 各國針對豁免情形之規範

國家		政府行為	私人活動或其他私領域行為	基本權競合	其他
歐盟 GDPR		• 刑事案件機關程序 • 外交安全政策	單純個人或家庭活動	表意自由與資訊自由，包括新聞目的及學術、藝術及或文學表意目的（部分豁免）	歐盟法領域外活動
德國					
英國		特定領域政府活動（執法行為、情報服務）			內閣大臣得以法律制定更多豁免規定
美國	CPRA	公務機關	• 企業內部管理（部分豁免） • 一般個人 • 受雇或應徵資		• 聯邦法律已規範 • 公開可得資料 • 特定類型豁免（部

			料（部分豁免）		分豁免） • 特定責任豁免
	UPDPA	• 公務機關 • 法院令狀、命令或其他法律允許 • 政府資料公開	• 受雇或應徵資料		• 聯邦法律已規範 • 公開場所觀察所得資料 • 人體試驗研究
日本		刑事案件或少年保護案件之程序（部分豁免）		新聞或出版、宗教、政治、學術自由（部分豁免）	
韓國		• 公務機關執行公務（部分豁	個人日常活動（部	媒體、宗教團體、政黨基於	• 法令具體准許

	免） • 預防犯罪及搜查所必要（部分豁免）	分豁免）	報導、傳教、推薦候選人等目的（部分豁免）	部分排除之情形 • 經合理評估，且使用其他資料也無法識別個資時得全部排除
新加坡	公務機關	• 單純個人或家庭活動 • 商業契約或商業活動（部分豁		專責機關得發布豁免名單

		免）		
菲律賓	政府活動		新聞、藝術、文學或研究目的	• 外國法具備管轄權 • 公眾關注事項
瑞士	• 聯邦議會 • 政府訴訟程序	• 自然人個人使用 • 民法公開登記		紅十字會

資料來源：本計畫研究團隊自行整理

而有關公開場所影音資料之管理，我國個資法第 51 條第 2 項「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」規定，僅係指豁免個資法適用，尚非監視設備之管理規定，然並未見於其他國家有相類似之豁免立法例。而以各國規範觀察之，目前德國、韓國針對監視器規範於個資法中，有訂定「得例外設置」之情形，並針對監視器之設置加強個資保護義務。其他國家，如英國規範於《自由保護法》（Protection of Freedoms Act 2012）、日本發布「監視器影像利用指引」（カメラ画像利活用ガイドブック）、美國依判例等，多數國家未明文規範於個資法。

二、 小結

我國個資法規定之豁免情形，已將個人日常生活中合理利用行為或是公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，予以排除個資法之適用範圍。依我國個資法第51條立法理由觀之，我國個資法第51條第1項第2款，為我國獨有之張貼表現自由，其本質或可能與我國個資法第51條第1項第1款相似。而我國個資法排除自然人單純為個人活動目的，而各國相較我國，則有更多針對政府行為、私法行為（如商業契約）、基本權（如言論自由）等之豁免情形。然而在擴大豁免情形之範圍前，仍應衡酌各該領域是否已有完備法制作為個人資訊隱私權之保護。

此外，我國個資法第51條第2項「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」規定，未見於其他國家有相類似之豁免立法例，且條文因缺少規範主體，易滋生豁免主體範圍爭議。雖相關函釋之實務見解已排除豁免基於職業或業務職掌之公開場所或公開活動影音資料蒐集、處理及利用，惟我國個資法並無類似公開場所或公開活動錄影監視錄影設備之管理規定。相較德國、韓國已將之納入個資法規範，或日本發布指引等作法，有值得我國參考借鑑之處。

第二項　域外效力

壹、比較法國家

一、歐盟

依GDPR第3條第2項規定，非位於歐盟境內的資料控管者與處理者，如以下列方式處理歐盟境內當事人之資料時，則仍有GDPR之適用，包括：

1. 提供歐盟境內資料主體產品或服務。

2. 涉及監控歐盟境內資料主體之行為。惟不享有GDPR第56條賦

予之一站式（one stop shop）機制[22]。

所謂「提供歐盟境內當事人產品或服務」，EDPB 強調「歐盟境內當事人」並非係以國籍或居住地作為判斷依據，然而當事人是否處於歐盟境內為判斷條件之一，因歐盟認為 GDPR 為一部適用於全球的法律[23]。判斷當事人處於歐盟境內的時間點為提供產品或服務的當下，而該項產品或服務提供期間之長短，並非本條判斷標準[24]，若係免費提供產品或服務之情形亦適用本條規定[25]。另外，依 GDPR 前言第 23 點規定，提供產品或服務之行為必須係意圖提供予身處歐盟境內當事人，意即資料控管者必須鎖定（target）歐盟當事人[26]，下列情形為判斷資料控管者是否「鎖定」歐盟當事人之因素[27]：

1. 於提供產品或服務的網站中直接提及歐盟或歐盟會員國之名稱。
2. 歐盟境內消費者為資料控管者所架設網站之目標使用者。
3. 資料控管者之行銷對象包含歐盟境內消費者。
4. 提供國際產品或服務，如觀光旅遊服務等。
5. 於提供產品或服務的網站中提及歐盟境內國家之地址或電話。
6. 使用非本國之網域名稱，如非使用.tw 而係.eu 等，代表該網域並非僅限於本國境內使用。
7. 於提供產品或服務的網站中提及至歐洲旅遊之交通資訊。
8. 提供產品或服務的網站中呈現含有不同國家之客群。

---

22 EUROPEAN DATA PROTECTION BOARD [EDPB], *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (2019), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en (last visited May 23, 2022) at 13.

23 *id*, at 14-15.

24 *id*, at 15.

25 *id*, at 16.

26 *id*, at 15.

27 *id*, at 17-18.

9. 提供產品或服務的網站使用歐盟國家通用之語言。

10. 提供產品或服務的網站以歐盟國家幣值收費。

11. 提供產品或服務的網站直接提及特定歐盟國家之消費者。

12. 產品可送達至歐盟國家。

當產品或服務僅提供給歐盟境外消費者，但是當消費者進入歐盟境內時，仍未停止提供產品或服務，則該情形並不適用 GDPR 第 3 條第 2 項第 a 款，因為該項提供產品或服務的行為本身其意圖提供給歐盟境外之消費者[28]。而關於「涉及監控歐盟境內當事人之行為」，依 GDPR 第 3 條第 2 項第 b 款之適用條件，即當事人應位於歐盟境內、監控之行為應於歐盟境內，以及監控行為係指對自然人進行決策或對其個人喜好、行為及態度進行分析或預測之剖析行為[29]。監控行為之媒介包含網路、智慧器材、智慧手環等[30]。由於資料控管者應對該資料之處理含有監控目的，方能構成第 3 條第 2 項第 b 款之「監控」，因此 EDPB 認為監控行為包含下列行為[31]：

1. 行為定向廣告（behavioural advertisement）。

2. 以定位位置資訊進行行銷（Geo-localisation activities for marketing purposes）。

3. 網路識別符號如 Cookies 追蹤或指紋追蹤。

4. 記錄追蹤個人健康飲食服務業者，包含以 APP 記錄。

5. 監視記錄。

6. 產業調查及以個人資料為基礎所進行之研究。

---

28 *id*, at 15.
29 *id*, at 19.
30 *id*.
31 *id*, at 20.

7. 對自然人健康狀態進行之監控行為及定期回報行為。

二、英國

關於 UK GDPR 之域外效力同 GDPR，依 UK GDPR 第 3 條第 1 項規定，UK GDPR 適用於在英國設立之資料控管者或處理者所為之個人資料運用活動，不論該運用是否發生於英國境內。因此若該資料控管者或處理者設立於英國，即使個人資料運用係位於境外，仍有 UK GDPR 之適用。若非設立於英國境內之控管者或處理者，依 UK GDPR 第 3 條第 2 項，對於英國境內當事人有下列情形仍適用 UK GDPR，其一為對英國境內當事人提供商品或服務，不論是否有償；其二係涉及監視英國境內當事人之行為。此外，UK GDPR 亦適用非設立於英國，但根據國際公法適用英國國內法之資料控管者。依 DPA 2018 第 207 條之規定，若該資料運用屬於 DPA 2018 第二部分（即 UK GDPR 之補充規定），則其域外效力適用 UK GDPR 第 3 條。反之，若非屬於 DPA 2018 第二部分，則應依 DPA 2018 第 207 條第 2 項規定，本法適用於在英國設有機構之控管者或處理者的活動內容，無論該運用是否在英國進行。

再者，依 DPA 2018 第 207 條中所稱之在英國設有機構，包括通常居住在英國的個人；根據英國或英國一部分法律成立的機構、合夥企業或其他非法人團體；或非前述情形，但在英國有常設辦事處、分支機構或代理機構並有展開活動者。

三、德國

BDSG 之域外效力與 GDPR 相仿，依 BDSG 第 1 條第 4 項第 1 款及第 2 款之規定，凡於德國境內運用個人資料之資料控管者（Verantwortliche）及受託處理者（Auftragsverarbeiter）；或資料控管者以及受託處理者之活動範圍於德國境內者，均有本法之適用。其中，不適用德國 BDSG 第 1 條第 1 項及第 4 項第 1 款及第 2 款情形者，如資料控管者或受託處理者未於歐盟成員國或歐洲經濟共同體之締約國境內設立登記，惟符合 GDPR 第 3 條規定時，則依 BDSG

第 1 條第 4 項第 3 款亦有本法之適用。

四、美國

（一）　CCPA 及 CPRA

CCPA 及 CPRA 所規範主體係營利事業，依第 1798.140 條第 v 項規定，本法之地域效力除了以「加州居民之消費者」之個人資料為限制，並不要求營利事業須實體存在於加州，而僅要求營利事業有於加州展開業務。故 CCPA、CPRA 事實上具有某種程度的域（州）外效力，除了營利事業不須實體存在於加州，也透過第 1798.140 條第 d 項第 2 款將營利事業的定義延伸到「包括任何控制或由營利事業控制的實體，並且與營利事業共用品牌名稱、服務標識或商標」，使位於加州境外的實體也可能受到 CCPA、CPRA 規範。此外，依第 1798.145 條第 a 項第 7 款規定，若消費者資料的蒐集、販售和共享之商業行為完全沒有任何一部份發生在加州境內，亦無任何個人資料係消費者位在加州時所蒐集，則不適用於本法規範。

（二）　UPDPA

依據 UPDPA 第 3 條第 a 項規定，UPDPA 的適用範圍包括在該州開展業務的資料控管者及處理者，或以該州居民為提供產品或服務為標的之資料控管者及處理者，惟並未要求資料控管者及處理者須實體存在於州內，故具有某種程度的域外效力。此外，同條第 a(3) 項將規範主體定義延伸至代表控管者且知道該控管者是 UPDPA 規範對象的處理者。使不在一州境內的處理者也可能受 UPDPA 規範。

五、日本

日本個資法有關域外效力可見於第 171 條「適用範圍」規定，即個人資料處理事業者對於國內之人提供物品或勞務，而取得本人之個人資料，並於國外處理該當個人資料或利用該當個人資料所作成之假名化資料處理事業、匿名化資料處理事業者，亦適用本法之相關規定。因此個人資料處理事業者設立於外國，而向日本國內居民提供

物品或服務取得個人資料，具體而言，如國外網路電商業者為經營銷售及運送商品，從日本國內消費者取得該個人資料之情形；又或者國外電子郵件服務提供業者爲設定個人帳戶，從日本消費者取得該個人資料並提供郵件服務之情形，均有適用日本個資法之相關規定。日本個資保護委員會可對其行使其權力，以請求報告或命令之方式為之。

六、韓國

PIPA 適用於韓國境內的所有資料控管者及資料處理者，惟本法並未明定域外效力。然而依 PIPA 第 39 條之 11 有關指定國內代理人之規定，若在韓國未登記地址或營業場所的資通訊服務提供者，經評估若於韓國境內使用者人數、營收等條件符合 PIPA 施行細則第 48 條之 9 所指定之基準，則仍須以書面方式指定國內代理人。是以在決定外國實體是否適用 PIPA 時，需同時考慮有無對韓國境內公民提供服務，抑或透過跨境提供商品或服務而產生收入等因素。

七、新加坡

新加坡 PDPA 未明定域外效力，惟依 PDPA 第 2 條有關組織之定義，係指包括任何個人、公司、協會或團體、公司或非法人團體，無論是否根據新加坡法律成立或認可；或者在新加坡居住、設有辦事處或營業地點。故本法適用於所有在其境內進行個人資料之蒐集、利用或揭露個人資料的所有組織，無論該組織是否依據新加坡法律設立，或在境內是否設有實體營業據點。此外，無論是向境內或境外之母公司、子公司傳輸個人資料，或將個人資料從新加坡跨境轉移至境外組織，均適用於 PDPA 之規定。

八、菲律賓

DPA 2012 有關域外效力規定於第 6 條，當有下列情形將適用本法之規定：

1. 涉及菲律賓公民或居民之個人資料。

2. 蒐集、持有、運用或利用個人資料之自然人或法人於菲律賓境內，或於境外運用關於菲律賓個人或居民之個人資料，包含但不限於下列情況：(1) 在菲律賓簽訂契約。(2) 並未設立於菲律賓，但於菲律賓境內有管理和掌控之法人。(3) 法人於菲律賓境內有分公司、辦事處、辦公室或子公司，並可近用個人資料。

3. 於菲律賓境內經營事業，或自菲律賓境內蒐集或持有相關個人資料。

此外，依 IRRDPA 2012 第 4 條規定，本法與本規則適用於公務機關或非公務機關之任何自然人及法人對個人資料之運用。若發生在菲律賓境外有以下情形仍適用本法，包括在菲律賓設立參與個人資料運用之法人，該行為、實施或運用個人資料係由與菲律賓有聯繫之自然人或法人所作，並應適當考慮國際法及禮儀之情形。

貳、我國規定

有關我國個資法之法律適用效力範圍規範，在常見之域外效力有二，其一係「蒐集主體在境外，對境內自然人個人資料之蒐集處理利用」，其二係「我國蒐集主體在境外，對境外之我國公民個人資料之蒐集處理利用」之情形。而我國個資法目前尚未針對未在境內設有實體，但有蒐集、處理、利用我國境內人民個人資料之情形予以規範。

我國個資法「域外效力」係規範於第 51 條第 2 項，規定「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」。其立法理由為「由於科技之進步與網際網路使用普遍，即使在我國領域外蒐集、處理或利用國人之個人資料，亦非常容易。為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任，爰增訂第 2 項，明定在我國領域外，亦有本法之適用。」。

表 6 我國個資法域外效力

對象 行為主體		蒐集、處理、利用對象	
		我國人民	外國人民
我國公務機關及非公務機關	我國境內	適用	適用
外國公務機關及非公務機關			
我國公務機關及非公務機關	我國境外	適用（第 51 條第 2 項）	不適用
外國公務機關及非公務機關		不適用	不適用

資料來源：本計畫研究團隊自行整理

惟參照法務部 107 年 3 月 12 日法律字第 10703502240 號函釋，個資法第 51 條第 2 項規定，在我國領域外蒐集、處理或利用個人資料行為，須合於以下要件，始有個資法之適用：其一為從事蒐集、處理或利用行為者為我國之公務機關及非公務機關；其二為所蒐集、處理或利用者為我國人民之個人資料。故將我國個資法之域外效力管轄範圍，採特有規範境外我國人民，且蒐集主體必須為我國之公務機關或非公務機關之情形，始受有我國個資法之適用。

參、分析與小結

一、 比較法之分析

綜觀各國法制，在域外效力上主要可分為三種立法例，以下分別說明：

1. 歐盟 GDPR 體系國家（例如德國）、英國、日本、新加坡、瑞士等：

（1） 依據《競爭法》概念，若對市場有產生影響者，皆納入規範管制。故針對提供歐盟境內資料主體產品或服務；涉及監控

歐盟境內資料主體之行為。

（2）　主體適用境內設立之控管者或處理者所為之個資處理活動，無論該處理是否發生於境內。

（3）　其對象針對歐盟境內之人，無論當事人國籍。

（4）　日本、新加坡、瑞士等國，其域外效力皆仿效歐盟模式。

2. 美國 CPRA：

（1）　要求營利事業有於加州展開業務，無論營利事業是否實體存在於加州。營利事業的定義延伸到「包括任何控制、或由營利事業控制的實體，並且與營利事業共用品牌名稱、服務標識或商標」，使位於加州境外的實體也可能受到規範。

（2）　對象針對加州居民。

（3）　若消費者資料的蒐集、販售和共享之商業行為皆未發生在加州境內，亦無任何個資為消費者位在加州時所蒐集，則 CPRA 規定將不適用於該資料。

3. 菲律賓

（1）　域外效力範圍較為寬泛，規範涉及菲律賓公民或居民之個人資料。

（2）　運用個人資料之自然人或法人於菲律賓境內，或於境外運用關於菲律賓個人或居民之個人資料，包含但不限於下列情況：在菲律賓簽訂契約；並未設立於菲律賓，但於菲律賓境內有管理和掌控之法人；法人於菲律賓境內有分公司、辦事處、辦公室或子公司，並可近用個人資料。

表 7 各國針對域外效力之規範

國家		受規範之蒐集主體	受規範行為	對象
歐盟 GDPR 德國 英國		• 提供境內資料主體產品或服務（包括免費提供） • 涉及監控境內資料主體之行為 • 適用不在境內設立，但根據國際公法適用國內法之控管者	處理行為（適用境內設立之控管者或處理者所為之個資處理活動，不問該處理是否發生於境內）	境內之人(無論國籍)
美國	CPRA	特定標準之企業（符合下列門檻之一：1.年營業額達 2500 萬美金或年度購買、販售、分享超過 10 萬消費者之個人資料；2.公司有 50%以上之年營業額來自販賣、分享消費者個人資料	蒐集、購買、販售、分享行為	當地居民
	UPDPA	特定標準之企業	蒐集、購買、販售、分享行為	當地居民
日本		個資處理事業者對境內之人提供物品或勞務，而取得本人個資於境外處理或利用者	處理或利用行為	境內之人(無論國籍)
韓國		• 未明文規定域外範圍 • 公司對境內公民提供服務，或透過跨境提供商品或服務而產生收入	處理或利用行為	未明文

新加坡	境內蒐集、利用或揭露個資之組織（無論境內是否設有實體營業據點）	蒐集、利用、揭露行為	境內之人（無論國籍）
菲律賓	• 境內運用個資者 • 境內簽約者 • 境內有控管之法人者 • 境內設有設備或分公司者	蒐集、處理、利用行為	境內之人（無論國籍） 境外公民

資料來源：本計畫研究團隊自行整理

二、 小結

依據我國個資法第 51 條第 2 項法條結構觀之，僅針對保護我國公民，而我國域外效力管轄範圍，僅針對境外之我國蒐集主體對我國人民個人資料之蒐集、處理、利用行為。惟我國個資法第 51 條第 2 項不宜逕以解讀為類似歐盟 GDPR 第 3 條第 2 項之域外效力。至於我國個資法否應納入域外效力之規範，除了順應國際個資法制趨勢之外，亦應考慮國際貿易上是否會產生相關影響，對於我國政治經濟背景與競爭力能否有效支持。

在域外效力之範圍上，需否當個人資料之蒐集、處理或利用之行為有涉及我國人民之個人資料時，無論我國或他國之公務機關、非公務機關均有我國個資法之適用，應衡酌我國與鄰近國家之密切關係，如有頻繁牽涉跨國之個人資料運用行為，則應有納入規範之必要。而參酌現行已有將「針對境外法人或自然人對境內人民之行為」納入規範之國家，均已設有個資法之獨立專責機關，惟我國個資法目前係由各中央目的事業主管機關採分別管理，因此如將來我國個資法明定域外效力，則應建置相關配套措施，避免行政量能不足，在執法面上方有可行性。

第三項　國際傳輸

壹、比較法國家

一、歐盟

（一）　國際傳輸之原則

依據 GDPR 第 44 條明定傳輸個人資料到第三國或國際組織，係採「原則限制，例外允許」。GDPR 前言第 101 點說明此規定，係為確保 GDPR 給予歐盟民眾的隱私保護，不致於個人資料傳輸至歐盟境外即失去保護力，因此 GDPR 要求第三國個人資料保護法規體制達到 GDPR 相似標準。GDPR 雖未有「國際傳輸」之定義，惟 EDPB 於 2021 年發布指引[32]，當資料傳輸符合下列情形時，則視為國際傳輸：

1. 評估該次資料傳輸情形，資料控管者或受託處理者依 GDPR 第 3 條第 2 項規定，符合 GDPR 之適用範圍。

2. 由資料控管者或受託處理者提供個人資料予其他資料控管者或受託處理者，個人資料由當事人直接提供給位於第三國的企業，或資料傳輸於同一資料控管者或受託處理者間。

3. 資料接收方必須實際位於第三國或為國際組織。

如有符合以上情形之一，則應遵守 GDPR 第五章規定，於該當國際傳輸之合法要件時，始得例外允許為國際傳輸[33]。

---

[32] EUROPEAN DATA PROTECTION BOARD [EDPB], *Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR* (2021), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en, at para 6-19, (last visited Jan. 12, 2022).

[33] *id*. at para 20, 24-25.

（二）　國際傳輸之合法要件

對於例外允許之合法要件，GDPR 採用階層模式，僅於無法取得適足性認定時，得考慮採行適當保護措施，而若同時無法取得適足性認定及採行適當保護措施時，始得依據例外條款為國際傳輸。以下將針對三種合法要件逐一說明。

1.　適足性認定

依 GDPR 第 45 條第 1 項、前言第 103 點規定，第三國應取得適足性認定（Adequacy Decision）始得與歐盟國家傳輸個人資料，而適足性認定係由歐盟執委會（the European Commission, EC）審核。目前於 GDPR 施行前已取得適足性認定之國家有安道爾、阿根廷、加拿大、法羅群島、根西島、以色列、馬恩島、澤西島、紐西蘭、瑞士及烏拉圭；GDPR 施行後取得適足性認定之國家則有日本、英國、韓國等[34]。依 GDPR 第 45 條第 2 項、前言第 104 點及第 105 點規定，歐盟執委會審核適足性認定申請時應考慮下列要件：

（1）民主法治精神、人權與基本權利之尊重、第三國之個人資料保護法規體系、第三國之國家安全法規體系、刑法體系、法院判決、當事人權利之行使、行政法或司法救濟。

（2）獨立個人資料監管機關之權力、職責及執法力。

（3）與個人資料保護相關的國際條約、參與之多邊或區域隱私規則體系。

雖然適足性認定未訂有期限，惟依 GDPR 第 45 條第 3 項規定，歐盟執委會應於每 4 年例行審查，且應持續關注已取得適足性認定國家之個資法制動態。

---

[34] EUROPEAN COMMISSION [EC], *How the EU determines if a non-EU country has an adequate level of data protection*, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (last visited Jan. 1, 2022).

2. 適當保護措施

如第三國未取得適足性認定，資料控管者得採用適當保護措施（Appropriate Safeguards）進行國際傳輸。歐盟法院（European Court of Justice, ECJ）於 *Schrems II* 判決中強調，GDPR 第 46 條適當保護措施必須搭配補充措施（supplementary measures），即必須確保第三國之個人資料保護程度達到 GDPR 相似水準（essentially equivalent level of protection）[35]，如資料輸出者應個案檢視適當保護措施是否會受第三國個人資料保護法制影響，而無法提供有效保護，且應確保資料輸入者協助完成義務，包括適時回報第三國個人資料保護法規動態及個人資料保護程度是否受法規變化所降低。有關適當保護措施得區分為以下類別：

（1） 標準契約條款

依 GDPR 第 46 條第 2 項第 c 款明定標準契約條款（Standard Contractual Clauses）為適當保護措施之一，係將 GDPR 之規定以契約形式規範於資料輸入者與資料輸出者，雙方得將標準契約條款併入所簽訂之商業契約中，亦得新增更強力度的條款，惟需留意新增條款不應牴觸標準契約條款且須尊重當事人之基本權利自由[36]。歐盟執委會於 2021 年 6 月公布新版標準契約條款，其採用模組化方式（modular approach）針對控管者或處理者之不同關係，得依個案選擇所適用之條款[37]。又依 GDPR 第 46 條第 2 項第 d 款明定，監管機

---

[35] EDPB, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (2021), https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, at para 23, (last visited Jan. 1, 2022).

[36] EUR-LEX, *COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council* (2021), https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj, at para 3, (last visited Jan. 1, 2022).

[37] *id*. at para 10.

關得自訂標準契約條款，但須經 EC 核定。

（2）　企業自我拘束規則

依 GDPR 第 46 條第 2 項第 b 款明定企業自我拘束規則（Binding Corporate Rules）為適當保護措施之一，其主要適用於跨國企業，將 GDPR 規範納入企業內規或章程。依 GDPR 第 47 條第 1 項第 a 款及第 b 款規定企業自我拘束規則應由監管機關核定，並須經其確認企業自我拘束規則適用於企業所有子公司、分公司、員工，以確保當事人之權利。

（3）　行為守則

依 GDPR 第 46 條第 2 項第 e 款明定行為守則（Code of Conduct）與有拘束力且可執行之約定，為適當保護措施之一。行為守則係一種自願性、責任性的法遵工具，為各產業的指標性工具書，並須經監管機關審核通過[38]。EDPB 表示通常係由同業公會、各產業之專業組織、學術組織及對該產業領域關注之團體所撰寫之行為守則[39]。此類別主要適合中小企業，使其得以最少成本落實 GDPR 法遵，達到最大效益[40]。且 EDPB 認為有拘束力且可執行之約定最常見的方式係屬契約[41]。

（4）　驗證

依 GDPR 第 46 條第 2 項第 f 款明定驗證為適當保護措施之一，

---

[38] EDPB, *Guidelines 04/2021 on codes of conduct as tools for transfers* (2021), https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en, at para 7, (last visited Jan. 1, 2022).

[39] *id*. at para 6.

[40] EDPB, *Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679* (2019), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en, at para 8, 11 (last visited Jan. 1, 2022).

[41] EDPB, *supra* note 38, at para 25-26.

又 GDPR 第 42 條明定驗證相關規定。驗證應由第三方為之[42]，而驗證方式應經監管機關或 EDPB 審核通過；依 GDPR 第 42 條第 5 項及第 7 項規定，驗證證書及標章應由 GDPR 第 43 條之驗證機構或監管機關發放，其效期為 3 年。驗證機構僅得驗證會員國境內組織[43]，受驗組織則僅限資料控管者及受託處理者，而驗證範圍僅限於公司內部治理流程及組織流程[44]。

3. 例外條款

依 GDPR 第 49 條例外條款明定符合下列情形之一時，始得為國際傳輸[45]：

（1）當事人明確同意：資料控管者須告知當事人未有適足性認定及適當保護措施傳輸資料之風險，公務機關不適用之。當事人必須對資料傳輸逐項表示同意，並應有隨時得撤回同意之權利[46]，且資料控管者應於資料傳輸前取得同意[47]。

（2）履行契約所必要：當國際傳輸為履行契約或終止契約所必要，或為採取契約前相應措施之必要，公務機關不適用之。此情形應具有必要性，即資料傳輸須與契約目的緊密連結，且限於非經常性傳輸。

（3）重要公共利益必要：因重要公共利益必要，如國際競爭法、稅務、海關、金融機關、社會安全、傳染病防疫等[48]。公共

---

[42] EDPB, *Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation*, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en, at para 15-17, (last visited Jan. 1, 2022).

[43] *id*. at para 34.

[44] *id*. at para 54-55.

[45] EDPB, *supra* note 35 at para 24.

[46] EDPB, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679* (2018), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en , at 7-8, (last visited Jan. 12, 2022).

[47] *id*. at 7.

[48] *id*. recital 112.

利益之判定以歐盟法角度為準，即須雙方國家均認定為重要公共利益而進行跨國合作，並得以國際公約作為佐證[49]。依前言第 111 點及第 112 點，此情形不限於非經常性傳輸，但仍應遵守 GDPR 第 49 條基本原則[50]。

（4）訴訟必要：因訴訟必要之情形，依前言第 111 點規定包括司法訴訟、行政訴訟、監管機關調查。此情形亦須符合必要性及非經常性要件[51]。

（5）個人重要利益必要：因保護當事人或自然人重要利益之必要，但此情形僅適用於當事人事實上或法律上難以給予同意時。主要適用於醫療行為、天災等情形[52]。

（6）立法授權之系統清單：GDPR 第 49 條第 1 項第 g 款及前言第 111 點規定，國際傳輸係經由歐盟或歐盟會員國立法授權之系統清單，以提供公眾資訊，如公布公司或土地所有權資訊、形式資訊的公開網站，惟系統內蒐集的個人資料不得全部傳出，且以當事人提出國際傳輸之要求為限[53]。

（7）重大正當利益必要：因重大正當利益必要時，且限於上列所有情形均未能適用時。故有諸多限制，如為一次性傳輸、涉及少數當事人、進行利益衡量、通知監管機關以及履行資料當事人告知義務[54]。EDPB 認為當資料控管者傳輸資料係為保護組織避免遭受立即重大傷害，或為避免重大懲罰所造成之財物損失，均該當重大正當利益[55]。

---

[49] EDPB, *supra* note 46, at 10.
[50] *id*. at 11.
[51] *id*. at 12.
[52] *id*. at 12-13.
[53] EDBP, *supra* note 46, at 13-14.
[54] EDPB, *supra* note 46, at 14-17.
[55] *id*. at 15.

二、英國

（一）　國際傳輸之原則

依 UK GDPR 第 44 條所示，移轉之一般原則：「任何已經處理或已移轉至第三國或國際組織之個人資料，若欲再移轉該個人資料，僅得於控管者及處理者遵循本章之條件下進行，並符合本規則其他條文，包括從第三國或國際組織所為之進一步移轉。為確保本規則保證之當事人保護程度不受減損，本章所有條文應受適用」。故英國對於國際傳輸係採「原則限制，例外允許」模式，應於符合 UK GDPR 及 DPA 規範時，始得為國際傳輸。

（二）　國際傳輸之合法要件

英國 UK GDPR 允許例外得國際傳輸之情形近似於歐盟 GDPR 之規定，例如 UK GDPR 第 45 條、DPA 第 17A 條及第 17B 條規定之適足性認定、UK GDPR 第 46 條規定適當保護措施與標準契約條款、UK GDPR 第 47 條企業自我拘束規則，以及 UK GDPR 第 49 條及 DPA 第 18 條第 2 項例外條款。

比較特別的是，UK GDPR 第 49 條第 5A 項賦予國務大臣得基於公共利益依法限制或放寬資料傳輸；DPA 第 17C 條規定標準契約條款得作為適當保護措施，並由國務大臣依法指定之，且國務大臣須持續審查現行有效之標準契約條款；DPA 第 119A 條規定，英國資訊委員得發布文件指定標準契約條款，並認定該條款符合 UK GDPR 第 46 條為個人資料傳輸至第三國或國際組織作為適當保障措施，其後亦得修改或撤回之。而根據本條簽署文件前，資訊委員須先諮詢國務大臣及合適之行業協會、當事人、足以代表當事人利益者。

三、德國

（一）　國際傳輸之原則

德國有關個人資料國際傳輸主要依循 GDPR 之相關規定，故亦

採「原則限制，例外允許」模式。

（二）　國際傳輸之合法要件

國際傳輸須符合 GDPR 規定，而 BDSG 針對公務機關傳輸資料有更嚴格之規範。當公務機關處理行為涉及資料傳輸時，應依 BDSG 第 25 條規定為之。

1. 傳輸至公務機關

依 BDSG 第 25 條第 1 項規定，基於執行職務之必要而傳輸個人資料至公務機關，尚須符合第 23 條公務機關合法處理事由之一，始得傳輸個人資料。

2. 傳輸至非公務機關

當公務機關將個人資料傳輸至非公務機關時，則須符合 BDSG 第 25 條第 2 項所列事由之一，始得為之：（1）非公務機關為履行傳輸機關所屬任務必要，且具同法第 23 條處理要件；（2）資料傳輸之接收方得透過信賴方式，闡明其對資料傳輸正當利益之認知，當未取消傳輸行為時，當事人應有更重要利益；或（3）為適用、主張或對抗法律上請求權所必要者。同樣地，資料接收方有義務向傳輸機關承諾，於傳輸之目的內進行處理；如涉及目的外處理時，應取得傳輸機關之同意，始得為之。

3. 傳輸特種個人資料

當公務機關依據 BDSG 第 25 條第 1 項或第 2 項規定進行傳輸行為，且資料屬於特種個人資料時，應具有 GDPR 第 9 條第 2 項合法處理事由之一，或符合 BDSG 第 22 條合法事由之一，並採行適當具體措施。符合上開規定者，始得跨境傳輸特種個人資料。

四、美國

美國不論為 UPDPA 或各州個人資料保護法均未針對個人資料

國際傳輸予以限制，故採「原則開放，例外限制」模式。惟美國在亞太經濟合作組織（Asia Pacific Economic Cooperation, APEC）力推APEC 跨境隱私保護規則（Cross Border Privacy Rules , CBPR）體系（下稱 CBPRs），該體系係嵌入 APEC 原有的 APEC 隱私權保護綱領（the APEC Privacy Framework）之個人資料隱私保護制度。該體系自 2011 年正式實施以來，成員國包含我國、美國、墨西哥、加拿大、日本、韓國、新加坡、澳洲、菲律賓等 8 個會員體。美國於 2012 年成為 CBPRs 的成員，在其與墨西哥和加拿大的貿易協定（United States- Mexico-Canada Agreement, USMCA）中，針對數位貿易應採用提供個人資料保護的法律框架的約定，並提及各國可參考 APEC 隱私權保護綱領的原則及指引建立保護框架，該協議更明文承認 APEC CBPRs 為國際傳輸保護個人資料的有效手段，且闡明各國應致力於推進與發展包括 APEC CBPR 在內的隱私保護互通機制。

五、日本

（一）　國際傳輸之原則

日本個資法針對國際傳輸之規範，依第 28 條第 1 項規定，當個人資料處理事業向外國（除經個人資料保護委員會認定與日本具有同等水準之個人資料保護制度之國家外）之第三人提供個人資料時，除有第 27 條第 1 項各款[56]所揭示之事由外，應事先得到當事人同意。

---

[56] 依本法第 27 條第 1 項各款事由包括，(一)基於法令；(二)為保護人之生命、身體或財產而有必要，於得到當事人同意有困難時。(三)為提升公眾衛生或推展兒童健全育成有特別必要，於得到當事人同意有困難時；(四)對國家機關或地方自治團體或受其委託者，為遂行法定事務有協助之必要，因得到當事人同意，對該當事務之遂行有造成障礙之虞時。(五)個人資料處理事業為學術研究機關等，且個人資料之提供係為學術研究成果之發表或教學而出於不得已之情形。（有不當侵害個人權利利益之虞者，除外）。(六)個人資料處理事業為學術研究機關等，且個人資料於學術研究之目的而有提供之必要（包含提供該個人資料之部分目的係為學術研究。有不當侵害個人權利利益之虞者，除外）（僅限該當個人資料處理事業與學術研究機關共同進行學術研究者）。(七)第三人為學術研究機關等，且第三人於學術研究之目的而有處理個人資料之必要（包含處理該當個人資料之部分目的為學術研究。有不當侵害個人權利利益之虞者，除外）。

因此日本係採「原則限制，例外允許」模式，僅於個人資料保護委員會認定接收國個人資料保護制度水準相當，或經當事人同意、具有例外事由時，始得為之。

（二）　國際傳輸之合法要件

1. 接收國個人資料保護制度水準相當之認定

有關接收國個人資料保護制度水準相當之認定，依《個人資料保護法施行令》（個人情報の保護に関する法律施行令）第 11 條第 1 項規定有下列考量因素：（1）具有個人資料處理事業相關法規，足認其履行在接收國得以確保之情形；（2）存在相當於個人資料保護委員會的獨立監管機關，且具有必要適當之監督體制；（3）在正確有效地使用個人資料與保護個人權益方面，接收國與日本在相互理解的基礎上協力合作；（4）在保護個人資料必要範圍外得允許國際傳輸，且接收國與日本間在保護個人資料同時得允許彼此間順暢傳輸；（5）允許傳輸至接收國將有助於產業創新實現充滿活力的經濟社會及富裕民生。而個人資料保護委員會依同條第 2 項得基於保護日本境內個人權益之必要，附加其他必要條件，以限制無須經當事人同意即可傳輸外國的個人資料範圍。另個人資料保護委員會依同條第 3 項規定，為確認上述情形應得對該外國的個人資料保護相關制度或有關附加條件的對應狀況進行必要調查，如認定結果未通過時，則得依同條第 4 項規定予以撤銷。

2. 適當保護措施

如接收國未被認定具相當水準，則國際傳輸應事先取得當事人同意。依個資法第 24 條第 2 項規定，個人資料處理事業應事先向當事人提供該國個人資料保護相關制度、接收方採行個人資料保護措施及其他資訊。又依同條第 3 項規定，個人資料處理事業爲確保接收方持續實施相應必要措施，必須依當事人要求提供必要相關資訊。而所謂「確保接收方持續實施相應必要措施」，依《個人資料保護法施行令》第 11 條之 2 規定得包含以下情形：（1）個人資料處理事業

與接收方之間處理個人資料，應通過適當、合理方法確保接收方實施本法第 4 章第 1 節相關措施；（2）個人資料接收方於處理個人資料已取得國際框架認證，如 CBPR。

六、韓國

（一）　國際傳輸之原則

韓國為提升資料於國際間商業運用，以及強化國際間合作關係，於 PIPA 第 14 條揭示「政府應制定必要政策以提升個人資料保護在國際環境之水準，且應制定相關政策使個人資料不因移轉至國外而侵害當事人之權利」。因此 PIPA 對於國際傳輸係採「原則限制，例外允許」的立法模式，須符合 PIPA 第 39 條之 12 對國際傳輸之合法要件，始得例外允許為國際傳輸。另 PIPA 第 39 條之 13 揭示互惠主義，對於限制個資傳輸至國外之資通訊服務提供者，得依該國標準採取相應之限制。但為履行條約或其他國際協定所必要，則例外不在此限。

（二）　國際傳輸之合法要件

依 PIPA 第 39 條之 12 第 1 項規定，資通訊服務提供者就有關使用者個人資料部分，不得締結與 PIPA 相違背之國際契約。另資通訊服務提供者為國際傳輸前，應依第 17 條第 3 項取得當事人同意，其告知事項應包括：（1）傳輸個人資料之項目；（2）接收國、傳輸時間及方式；（3）接收方身分（若為法人時，則為該法人名稱及管理者之聯繫方式）；（4）接收方對個人資料之利用目的及保有利用期間。惟若上述應告知事由均已依施行細則規定透過公開方式向當事人告知[57]，則得例外不須經當事人同意。

此外，資通訊服務提供者為國際傳輸時，仍應依照 PIPA 施行細則採行適當安全維護措施。依 PIPA 施行細則第 48 條之 10 有關適當

[57] 依 PIPA 施行細則第 48 條之 10 規定公開方式得包括以書面、電子郵件通知等方式為之。

安全機制規定包括：(1) 依 PIPA 第 39 條之 12 第 2 項第 4 款實施保障措施，如確保個人資料保護安全的措施符合施行細則第 48 條之 2 規定、建立有關處理個人資料侵權申訴及爭議解決、保護個人資料所需其他措施；(2) 資通訊服務提供者應於傳輸前與接收方討論前項保障措施，並將其納入協定條款。

七、新加坡

（一）　國際傳輸之原則

PDPA 對於個人資料國際傳輸係採「原則限制，例外允許」之模式，組織必須遵守傳輸限制義務，依據 PDPA 第 26 條第 1 項規定，原則上不得將任何個人資料傳輸至新加坡以外之國家或地區，除非組織確保資料接收方所在國家或地區具備不低於 PDPA 所規範之保護標準，以確保個人資料獲得與 PDPA 相當的保護措施，始得例外允許國際傳輸[58]。

（二）　國際傳輸之合法要件

由於境外接收方不受 PDPA 拘束，故國際傳輸必須確保個人資料將受法律強制義務所保護始可為之。為具備法律效力之義務要求，依據 PDPA 第 11 條得區分以下情形：(1) 有無任何法律規範；(2) 有無與 PDPA 保護標準相符且載明傳輸國家或地區之契約條款，如東協資料跨境傳輸契約條款範本[59]（ASEAN Model Contractual Clauses for Cross Border Data Flows, MCCs）；(3) 有無企業自我拘束

---

58 PERSONAL DATA PROTECTION COMMISSION [PDPC], *ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA*, at 121, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en (last visited Jan. 10, 2022).

59 PDPC, *GUIDANCE FOR USE OF ASEAN MODEL CONTRACTUAL CLAUSES FOR CROSS BORDER DATA FLOWS IN SINGAPORE*, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.pdf?la=en (last visited Jan. 10, 2022).

規則，若接收方為關係企業，得透過企業自我拘束規則（Binding Corporate Rules, BCR）要求採行與 PDPA 保護標準相符的保護措施，並載明適用 BCR 之接收方資訊、可能傳輸之國家或地區及權利義務內容；（4）任何具有法律拘束力之文件。

如未符合上述規定，亦得依據 PDPA 第 12 條規定透過取得特定認證之方式，如 APEC CBPR 體系或資料處理者隱私認可（Privacy Recognition for Processors, PRP）體系之認證，此時接收方將被視為符合傳輸限制義務要求，得將個人資料傳輸至已取得認證之接收方。

然而，若接收方無法依據前述法律強制義務或取得特定認證時，若有以下情形亦可視為符合傳輸限制義務之要求[60]：（1）組織必須以書面方式告知當事人其個人資料所受到之保護措施，並取得國際傳輸之同意，組織不得將同意作為提供產品或服務之條件，亦不得提供虛假或誤導性資訊以取得同意[61]；（2）為締結或履行契約之必要；（3）基於個人重要利益或國家利益有利用或揭露個人資料之必要，且組織已採取合理措施確保個人資料不會受到任何目的外利用或揭露；（4）該個人資料為傳輸中資料[62]；（5）該個人資料為國內公開資料。

此外，依據 PDPA 第 26 條規定，組織可向 PDPC 申請豁免國際傳輸限制，PDPC 得附加條件且不須刊登於新加坡公報，並得隨時撤銷該豁免決定，亦得隨時增加、變更或撤銷本條規定所設任何條件。

八、菲律賓

（一）　國際傳輸之原則

依據 DPA 第 3 條第 h 款有關個人資料控管者之定義，除蒐集、持有、處理或利用個人資料之自然人及法人外，亦同時包含指示或委託他人傳輸個人資料之自然人及法人。無論「國內傳輸」或「國際傳

60　Personal Data Protection Regulations 2021, Section 10(2).
61　Personal Data Protection Regulations 2021, Section 10(3).
62　Personal Data Protection Regulations 2021, Section 9.

輸」之自然人及法人，均該當於 DPA 之控管者定義，而須遵守 DPA 2012 及相關法規。依據 DPA 第 21 條有關「傳輸個人資料之責任」，須符合以下規定：(1) 當控管者傳輸予接收方時，須與接收方簽訂個人資料保護協議等合理手段，以確保接收方將確實採行符合 DPA 2012 之保護標準；以及 (2) 控管者應指定一名或多名人員確認接收方是否確實遵守 DPA，同時應將指定人員身分向當事人揭露。

此外，菲律賓於「國家隱私委員會」(National Privacy Commission, NPC) 權責規定，NPC 在國際傳輸議題上具有「為促進與落實個人資料隱私保護必要行動」之權限。因此 DPA 雖未明文規定國際傳輸之原則，惟課予控管者應於傳輸前履行相當義務，始得為之，故仍較接近於採行「原則限制，例外允許」模式。

（二）　國際傳輸之合法要件

承前所述，依 DPA 2012 規定控管者於傳輸前，須落實「符合 DPA 2012 保護標準之合理手段」與「指定一名或多名人員確認接收方有無確實遵守 DPA 2012」之義務。此外，亦須遵守 NPC 針對國際傳輸提出之必要行動要求。NPC 轄下的隱私政策辦公室 (Privacy Policy Office) 於 2017 年 4 月 21 日發布具有拘束效力之法律文件「第 2017-018 號諮詢意見」(Privacy Policy Office Advisory Opinion NO. 2017-018)，針對控管者進行國際傳輸所須遵守之法律規範與注意事項進行說明。依據 DPA 第 4 條與 IRRDPA 2012 第 4 條規定，無論國際傳輸之原因，當傳輸之個人資料與菲律賓公民或居民相關，或控管者與接收方其一與菲律賓存在關係，該傳輸行為即應遵守 DPA、IRRDPA 等相關法規[63]。惟 NPC 的隱私政策辦公室於 2020 年 3 月 31 日發布的「第 2020-018 號諮詢意見」，當控管者得證明與接收方之間，雙方已簽署權利義務之範圍，及確認雙方均受 DPA 2012、IRRDPA 2012

[63] National Privacy Commission [NPC], *PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2017-018* 2, Apr. 21, 2017, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-018.pdf (last visited Jan. 3, 2022).

等相關法規管轄之文件，即得該當於已盡一切合理手段，保障個人資料當事人權利之證明[64]。

另所謂「符合 DPA 保護標準之合理手段」之標準，NPC 於 2020 年 12 月 23 日發布第 2020-03 號官方公告，提出「個人資料共享協議」（Data Sharing Agreement, DSA）範本，方便控管者進行個人資料分享時，可直接提供接收方簽署[65]。內容包含雙方應採取組織、物理及技術上安全措施，以確保對 DSA 所記載、共享之個人資料得受到適當保護，且應建立「個人資料事故發生時的應變與管理程序」。

九、瑞士

（一）　國際傳輸之原則

依據 DSG 有關「揭露」（Bekanntgeben）個人資料之行為，定義上包含「傳輸個人資料」與「提供個人資料」。針對「在國外揭露個人資料」（Bekanntgabe von Personendaten ins Ausland）係規定於 DSG 第 2 章第 3 節。依據 DSG 第 16 條第 1 項規定，國外揭露個人資料須經瑞士最高行政機關「聯邦委員會」（Bundesrat）檢視確認，接收國或國際組織是否具有完整保障個人資料當事人權利的規範，始得為之。因此瑞士聯邦委員會針對個人資料國際傳輸行為具有「事前審查」之權力，故係採「原則限制，例外允許」模式。

（二）　國際傳輸之合法要件

依據 DSG 第 16 條第 2 項規定，瑞士聯邦委員會將審查個人資料國際傳輸行為是否具備下列項目之一：(1)接收國或國際組織是否與瑞士簽署國際條約；(2)控管者或處理者與接收方之間是否已簽署

---

[64] NPC, *PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2020-018 3*, Mar. 31, 2020, www.privacy.gov.ph/wp-content/uploads/2020/10/Redacted-Advisory-Opinion-No.-2020-018.pdf (last visited Jan. 4, 2022).

[65] NPC, *NPC Circular No. 2020-03*, Dec. 23, 2020, www.privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf (last visited Jan. 7, 2022).

經「聯邦資料保護及資訊委員」（Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, EDÖB）確認的個人資料保護協議；（3）特定事業主管機關是否針對個人資料國際傳輸行為，制訂具體保障個人資料當事人權利的措施，並經 EDÖB 確認；（4）EDÖB 是否針對個人資料國際傳輸行為，事先批准並發布個人資料保護協議範本；（5）接收國或國際組織的個人資料主管機關是否提出證明，其個人資料保護規範與 DSG 具備同等保護效力。故主要合法要件與 GDPR 規範相似，均包括適足性認定、適當保護措施及例外條款。

貳、我國規定

我國有關國際傳輸之相關條文，首先可見於個資法第 2 條第 6 款針對國際傳輸之定義為「指將個人資料作跨國（境）之處理或利用」，因此對於機關內部之資料傳送，或將資料提供當事人以外第三人，若具有將個人資料作跨國（境）傳輸之客觀條件，不論為資料處理或利用行為，均該當於個資法之國際傳輸。

其次，依個資法第 21 條國際傳輸條款之規定，中央目的事業主管機關發現有本條所列各款情形之一，得視事實狀況，以命令或個別之行政處分限制非公務機關國際傳輸個人資料。從法條觀之，原則上允許非公務機關進行個人資料之國際傳輸行為，僅於涉及國家利益、國際條約或協定有特別規定、接受國對於個人資料未有完善之法規及以迂迴方法向第三國（地區）傳輸個人資料規避本法等四種情形時，中央目的事業主管機關得限制之。因此我國對國際傳輸係採「原則開放，例外限制」之模式。

又參照法務部 102 年 1 月 3 日法律字第 10100226680 號函釋意旨，「法律賦予中央目的事業主管機關，遇有個資法第 21 條所定各款情事之一時，對於人民自由權利限制之依據及裁量權。至於具體個案中央目的事業主管機關是否限制，仍應由主管機關本於權責審認。」復參照法務部 107 年 8 月 21 日法律字第 10703511390 號函釋意旨，「應由主管機關依非公務機關對個人資料之處理利用情形是否

涉有國際傳輸行為，以及資料接受國對於個人資料之保護有無完善法規，本於權責審認。」目前我國各部會有國家通訊傳播委員會依個資法第 21 條規定，於 2012 年以大陸地區之個人資料保護法令尚未完備，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區（參照國家通訊傳播委員會 101 年 9 月 25 日通傳通訊字第 10141050780 號令)；衛生福利部亦於 2022 年限制社會工作師事務所將當事人個人資料國際傳輸至大陸地區(參照衛生福利部 111 年 1 月 21 日衛部救字第 1111360009 號公告)。

參、分析與小結

一、比較法之分析

（一）　國際傳輸之限制

綜觀各國法制，由於當個人資料進行國際傳輸至外國後，即非其本國法律可以當然發生作用之範圍，該外國法律究將提供何種程度之保護，亦已非其本國之立法者所得掌握。早期國際上對於個人資料國際傳輸之基本立場，可概分為「自由說」及「限制說」二類，前者係基於資訊自由化及貿易自由的角度，鼓勵資料跨國流通及分享；後者則根據保護當事人隱私權、保障經濟利益及維護資訊主權等理由，主張限制個人資料跨國流通。然隨著網路與資訊科技快速發展，使個人資料得輕易為國際傳輸，為避免個人資料被傳輸至缺乏妥適保護的國家或地區，用以規避內國法律原本加諸之限制，故國際上多數國家針對國際傳輸之規範，已多採「原則限制，例外允許」模式，如歐盟體系僅於資料接收國之個人資料保護水準相當或企業採取適當保護措施、具特定情形時，始得例外允許進行國際傳輸。而亞洲國家如日本、韓國、新加坡、菲律賓亦均仿效此立法模式，其中韓國有採互惠主義，即當他國限制傳輸至韓國時，對他國得採相應之限制。而美國強調以業者自律方式解決隱私權保護問題，故未針對國際傳輸予以規範，惟積極推動 APEC 跨境隱私保護規則體系（CBPRs），期能建構受信賴的資料自由流通環境，以隱私保護為社會信賴基礎。

然而限制國際傳輸之影響，可能造成企業需增加營運成本，並採行資料在地化相關措施（如於當地設置伺服器、資料中心等）、配合法規例外允許所要求之條件，甚至可能影響外國企業選擇退出本土市場；對於當事人而言，則有利個人資料被妥善保護，促進當事人對資料持有者之信賴，並得作為本國發展資料經濟之重要因素，且亦有利於本土資料處理業者茁壯。

（二）　國際傳輸之合法要件

1.　接收地之個人資料保護水準相當

目前歐盟、英國、德國、瑞士、日本、新加坡對於例外允許國際傳輸之合法要件有採納「接收地之個人資料保護水準相當」。此要件之相當性認定條件，得參考歐盟體系之適足性認定，或日本之白名單制度，主要考量因素包括：(1) 有無個人資料保護相關法規；(2) 有無獨立專責監管機關；(3) 有無與個人資料保護相關國際條約、參與之多邊或區域隱私規則體系。

有關接收地之個人資料保護水準相當此一要件，概念相近於我國個資法第 21 條第 3 款規定「接受國對於個人資料保護未有完善之法規，致有損當事人權益之虞」。惟此要件屬於不確定法律概念，需依個案具體判斷。另日本基於此要件允許國際傳輸時，倘個人資料保護委員會認為有必要保護國內個人權益時，仍得附加其他必要條件限制無須經當事人同意即可傳輸個人資料之範圍。此外，韓國未明文採納此要件，強調應由企業取得當事人同意始得為之。

2.　企業採取適當保護措施

目前歐盟、英國、德國、瑞士、日本、韓國、新加坡、菲律賓對於例外允許國際傳輸之合法要件有採納「企業自主採用符合規範之適當保護措施」，如企業自我拘束規則、標準契約條款、行為守則及認證。首先，企業自我拘束規則係由企業將本國個人資料保護相關法規訂於企業內規或章程、公司治理規範，並須經監管機關核定同意。

其內容至少應包含：企業結構及聯絡資訊、個人資料流、內規法律效力、處理個人資料原則、當事人權利行使、承諾、告知義務、配置個人資料管理人員及教育訓練、紛爭解決機制、稽核及改善措施、事故通報、監管機關合作等。目前歐盟、英國、德國、日本、新加坡有採納此類型。

其次，標準契約條款係以制式的契約形式將本國個人資料保護法規範於資料傳輸者與接收者雙方，標準契約條款須經監管機關核定同意，或由監管機關所訂定之。另參考歐盟執委會所公布之新版標準契約條款，得採用模組化方式針對控管者與處理者之間，因應不同關係選擇所適用之條款。目前歐盟、英國、德國、瑞士、日本、新加坡、菲律賓有採納此類型。

再者，行為守則係由同業公會、各產業團體、學術組織訂定之行業守則，為自願性、責任性之法遵工具，作為各產業指標性工具書。行業守則須經監管機關核定同意，其內容至少應包含：處理個人資料原則、未成年人之資料提供、假名化、當事人權利行使、控管者職責、隱私納入設計、事故通報、國際傳輸、紛爭解決機制等。目前歐盟、英國、德國有採納此類型。

最後，認證為企業得作為證明其資料處理活動已遵行個資保護相關規範之方式。認證應係自願申請，透過透明程序取得，由第三方進行認證。認證之範圍應限於流程，如公司內部治理流程及組織流程，而認證標章應由認證機構或監管機關核發。有關認證規則應經監管機關核定同意，其內容至少應包含：處理個人資料原則、當事人權利行使、事故通報、隱私納入設計、資料保護影響評估、安全措施等。目前歐盟、英國、德國、日本、新加坡有採納此類型。其中 APEC CBPR 為日本、新加坡所承認之認證制度之一，而韓國、菲律賓亦為 CBPR 會員國，鼓勵企業取得認證，以提升消費者對跨境資料傳輸的信賴，促進跨國商務發展。

有關企業採取適當保護措施此一要件，歐盟強調仍須配合補充措施，如契約上、技術上及組織上的措施，以確保接收方履行義務，

包括適時回報接收地之國家個人資料保護法規動態，以及個人資料保護程度是否會因法規變化而降低。而日本則強調透明性，因此企業仍需取得當事人事前同意並提供當事人有關接收方之國家個人資料保護法制及接收方所採取之個人資料保護措施參考，且後續仍應提供相關資訊確保接收方持續實施。

表 8 各國承認企業採行適當保護措施之類型

	企業自我拘束規則	標準契約條款	行為守則	認證
歐盟	O	O	O	O
英國	O	O	O	O
德國	O	O	O	O
瑞士		O		
美國				△CBPR 會員國
日本	O	O		O
韓國				△CBPR 會員國
新加坡	O	O		O
菲律賓		O		△CBPR 會員國

資料來源：本計畫研究團隊自行整理

△：未明文規定

3. 特定情形時

目前歐盟、英國、德國、瑞士、日本、韓國、新加坡對於例外允許國際傳輸之合法要件有採納「因特定情形而得排除國際傳輸限制」。各國規範普遍以類型化方式規範特定情形，如告知當事人並取得明確同意、基於法令、履行契約、保護個人利益、保障公共利益、司法訴訟等。較多國家所採類型，為告知當事人並取得明確同意，其

係指經告知當事人國際傳輸之風險，並事前取得當事人之明確同意，且當事人得隨時撤回同意。目前有採納此類型的國家有歐盟、英國、德國、日本、韓國、新加坡。其中韓國另要求須有保障措施，如確保個資處理安全、建立申訴爭議解決機制。

其次，保護個人利益應限於重大利益，且以事實上、法律上難以取得當事人同意為必要。目前歐盟、英國、德國、日本、新加坡有採納此類型。其中日本對於個人利益有採生命、身體、財產類型。再者，保障公共利益，須具有重要性，各國類型化後的公共利益類型有所差異，但多數集中在國家高權、行政相關、公共衛生等類型。目前歐盟、英國、德國、日本、新加坡有採納此類型。

有關特定情形此一要件，係於接收地未符合個人資料保護水準相當性或企業未採行適當保護措施時，須符合特定情形，始得為國際傳輸，適用上應從嚴解釋，僅於偶發與非重複性之傳輸時允許。而特定情形之類型化，仍須採取相應之配套措施，如當事人同意時須課予更嚴格之告知義務及保障措施、保護個人限於重大利益及難以取得當事人同意、保障之公共利益須有重要性。

表 9 各國承認特定情形之類型

	告知及同意	基於法令	履行契約	保護個人利益	保障公共利益	司法訴訟
歐盟	O		O	O	O	O
英國	O		O	O	O	O
德國	O		O	O	O	O
瑞士						
美國						
日本	O	O	O	O		
韓國	O					
新家坡	O		O	O	O	
菲律賓						

資料來源：本計畫研究團隊自行整理

二、小結

由於數位經濟的快速發展，個人資料國際傳輸已為常態，然而如何保障國際傳輸後之個人資料仍可以受到一定程度保護，為各國亟欲解決之問題。自歐盟施行 GDPR 以後影響日本、韓國、新加坡等亞洲國家對於資料保護之態度。綜觀各國個人資料保護規範，對於個人資料國際傳輸之限制有不同處理模式，如美國基於資訊自由化及貿易自由的角度，採取「原則開放，例外限制」；而歐盟及日本、韓國等多數國家為強化個人資料保護，則採「原則限制，例外允許」。其中韓國採行之互惠條款，得作為國際傳輸之武器對抗他國不合理之限制。

有關例外允許個人資料得國際傳輸之合法要件，得考慮採納接收地之個資保護水準相當、企業採行適當保護措施及例外情形。首先，接收地之個資保護水準相當得參考日本建立白名單制度，由主管機關公布可信賴國家以免除國際傳輸之限制，且於必要時仍得附加條件限制傳輸之範圍。

其次，企業採行適當保護措施得分為企業自我拘束規則、標準契約條款、行為守則及認證，企業得視其規模選擇所採行之類型，並應採取補充措施。

最後，當接收地之個資水準未相當且企業無採行適當保護措施時，僅於特定情形時得允許國際傳輸，如當事人知悉風險仍同意、保護個人重要利益及保障重要公共利益時，惟若依據此一要件時應就個案判斷，並採行相應之配套措施，且許可應限於一次性傳輸。我國面對快速變化的數位經濟發展，以及國際對於國際傳輸之立法潮流，應重新評估現行國際傳輸之管制模式，以完備個人資料保護法制，並接軌國際資料保護模式。

第四節　蒐集主體及受託處理者

第一項 蒐集、處理及利用之合法要件探討（不含當事人同意）

壹、比較法國家

一、歐盟

（一）　一般及特種個人資料及處理之定義

依據 GDPR 第 4 條第 1 項規定，所謂「個人資料」（personal data）係指可識別或可得識別自然人的資料，包含姓名、身分證字號、位置資訊、網路識別碼、身體心理特徵、基因、精神狀態、經濟狀況、文化、社會認同等，而死亡之人的個人資料非 GDPR 個人資料。而所謂「特種個人資料」（special categories of personal data）依據 GDPR 第 9 條第 1 項，則係包含揭露種族或人種、政治意見、宗教或哲學信仰、工會會員、基因資料[66]、用以特定識別自然人之生物特徵識別資料[67]、涉及健康之資料[68]、與自然人性生活相關以及與性傾向相關

---

[66] 依 GDPR 第 4 條第 13 項將基因資料定義為經生物樣本分析後，與自然人先天繼承或人工取得的基因特徵相關的個人資料，該資料透漏與身體健康相關的特殊資訊。GDPR 前言第 34 點說明生物樣本分析包含染色體分析（chromosomal analysis）、去氧核醣核酸分析（deoxyribonucleic acid (DNA) analysis）、核醣核酸分析（ribonucleic acid analysis）等。

[67] 依 GDPR 第 4 條第 14 項將生物特徵識別資料定義為經由特定技術處理後，與自然人的身體特徵、心理特徵及行為特徵相關的個人資料，且依這些特徵可辨識出或可確認自然人的特殊識別性（unique identification of a natural person），舉例而言，自然人的特殊識別性包含臉部圖像或指掌紋資料[67]。*See* Case C(2020) 8599, Commission Implementing Decision (EU) 2020/2165 of 9 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D2165&rid=7 (last visited Oct. 8, 2021)

[68] 依 GDPR 第 4 條第 15 項將涉及健康之資料定義為與自然人身體及心理相關的個人資料，包含健康照顧服務業者所持有之資料因為該資料透漏自然人的健康狀況。另依 GDPR 指引中列舉出以下幾種涉及健康之資料：（1）提供健康照顧服務之業者由病患紀錄所蒐集的資料，包含，病史、檢查結果（2）資料交叉引用或交叉比對（cross referencing）後透露出自然人之健康狀況或健康風險，例如經長期觀察，某人長期患有高血壓，因此透露出他有心臟病發之高度風險（3）當事人填寫與其健康狀況相關之問卷，在問卷中所填寫的病徵（4）資料本身非涉及健康之資料，但因為被使用於特定的情境中而變成涉及

等資料。

另外，所謂「處理」（processing）依據 GDPR 第 4 條第 2 項規定，係指任何針對個人資料之運用行為，包含蒐集、儲存、使用、變更、刪除等行為。而「進階處理」（further processing）依據 GDPR 第 6 條第 4 項規定，係指將資料使用於其他的目的，如組織是依履行契約、保護生命利益或正當利益任一要件處理資料時，只有當新目的與舊目的相容（compatible）時，始得將資料使用於新目的，與目的外利用之概念並不相同。而相容性之檢驗考量因素，包含舊目的與新目的之連結、蒐集時的脈絡（context）、個人資料的性質（nature）、新目的處理之可能後果，以及適當安全措施之落實。

（二）　一般個人資料之合法要件

依據 GDPR 第 6 條第 1 項規定，如符合下列事由之一者，得合法處理個人資料：

1.　因履行契約必須處理資料

依據 GDPR 第 6 條第 1 項第 b 款規定，可包含二種情形：（1）如客觀上為履行與資料當事人締結之契約而處理資料，須契約已成立、依據國內法該契約為有效，並且處理行為客觀屬於履行契約所必要[69]；或（2）客觀上為準備締結契約，應資料當事人要求必須處理資

健康之資料，例如定位或路徑資料本身非涉及健康之資料，但如被醫生用於診斷有無確診新冠肺炎，該資料因為被使用於與醫療相關的特定情境則變成涉及健康之資料。*See* EDPB, *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak* (2020) https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (last visited Oct. 8, 2021).

[69] 必要性檢驗包含辨識資料處理的目的，契約關係中有可能會有多個目的，資料處理目的必須清楚地傳達給資料當事人；但如果有其他較實際或較不侵略性的資料處理方式可使用，目前所採取的資料處理方式即非必要。*See* EDPB, *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* (2019) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en, at para 22, 24-26, (last

料。

2. 因履行法定義務必須處理資料

依據 GDPR 第 6 條第 1 項第 c 款規定，法律明定之義務，係指歐盟或歐盟成員國法律所明定之義務，若依據第三國之法律所產生的義務，則無本款之適用[70]。

3. 因保護自身或他人生命利益必須處理資料

依據 GDPR 第 6 條第 1 項第 d 款、前言第 31 點之規定，生命利益為重大利益（vital interests），特別限於攸關生死的議題，或對自然人可能造成外傷或健康傷害之威脅[71]。

4. 因公共利益或執行公務必須處理資料

依據 GDPR 第 6 條第 1 項第 e 款之規定，所謂「公共利益」或「公務」限於歐盟或歐盟成員國之公眾利益，以及歐盟或歐盟成員國範圍內所執行之公務；因此，第三國的公共利益或第三國公務機關所執行之任務，無本款之適用[72]。

5. 因追求自身或第三方正當利益（legitimate interests）必須處理資料，但如資料當事人的基本權利及自由較正當利益重要時，不適用之

依據 GDPR 第 6 條第 1 項第 f 款之規定，本款得基於追求正當利益而處理個人資料，惟須通過比例原則之檢驗，即正當性檢驗（legitimate interest test）、衡平性檢驗（balancing test）以及必要性檢驗（necessity test）。所謂「合法性檢驗」係指依歐盟及歐盟成員國國

---

visited Oct. 8, 2021).

70 ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (2014) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf, at 19 (last visited Oct. 8, 2021).

71 *id*, at 20.

72 *id*, at 21.

內法該利益是合法的，且事實上現存之利益[73]。而「衡平性檢驗」係指要求衡量控管者或第三方的正當利益，必須大於資料當事人的利益或當事人的基本權利與自由[74]。最後，「必要性檢驗」則要求處理資料的手段，對於控管者達到目的是必要的[75]。

此外，有關「犯罪紀錄相關的個人資料」雖 GDPR 第 10 條未列為特種個人資料，但處理犯罪資料須符合 GDPR 第 6 條第 1 項之合法處理要件，且受主管機關監管或基於歐盟成員國國內法規定，且採取適當安全措施時，始得處理與犯罪紀錄相關的個人資料[76]。

（三）　特種個人資料之合法要件

按 GDPR 第 9 條第 1 項規定，非經當事人同意，原則禁止處理特種個人資料，只有在符合同條第 2 項所列合法要件之一者，始得例外處理特種個人資料：

1. 基於勞動法、社會安全法及社會保護法而為必要之處理

依據 GDPR 第 9 條第 2 項第 b 款之規定，當資料處理係為履行法律規定之義務及權利之目的而必要時，得處理特種個人資料。本條所指的法律是依歐盟法、歐盟成員國國內法、歐盟成員國依法制定之共同協議而制定的勞動法、社會安全法及社會保護法，且該法應保護當事人的基本權利與利益。

2. 當事人身體上或法律上無法同意，基於保護重大利益而處理

依據 GDPR 第 9 條第 2 項第 c 款之規定，當資料處理是因為保

---

[73] *id*, at 24-25.

[74] 衡平性檢驗考量之要素包含：控管者的正當利益；評估資料處理對資料當事人的利益或資料當事人的基本權利與自由之影響，影響包含正面與負面的影響。風險產生之可能性及後果的嚴重程度為評估事項；控管者是否採取額外防護措施。*See* ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 70, at 23, 33, 36, 37, 38.

[75] ARTICLE 29 DATA PROTECTION WORKING PARTY, *supra* note 70 at 29.

[76] *id.*

護當事人或自然人的生命利益（vital interests）所必要時，得處理特種個人資料，但限於當事人因身體因素無法給予同意，或依法律定義為無能力給予同意的情形。

3. 與非營利組織相關之處理

依據 GDPR 第 9 條第 2 項第 d 款之規定，非營利組織[77]得處理特種個人資料，但非營利組織除應於合法活動範圍內、已採取適當保護措施，且該處理只能與非營利組織現任或歷任成員有關，或是與非營利組織有頻繁交流者有關且是因為業務而交流。除此之外，控管者必須確認在當事人未同意的情況下，並無對外揭露個人資料。

4. 當事人自行公開之處理

依據 GDPR 第 9 條第 2 項第 e 款之規定，當特種個人資料已明顯地（manifestly）被當事人公開時，始得處理該特種個人資料。

5. 與訴訟司法有關之處理

依據 GDPR 第 9 條第 2 項第 f 款之規定，如因訴訟或法院執行司法職責而有必要時，得處理特種個人資料。

6. 與重要公共利益（substantial public interest conditions）有關之處理

依據 GDPR 第 9 條第 2 項第 g 款之規定，基於歐盟法或歐盟成員國國內法之規定，為保護重要公共利益而有必要處理特種個人資料時，如欲達成之目標與處理特種個人資料間符合比例原則，屬於合法之處理行為，但應採取特定的、適合的措施，以保護當事人的基本權利和利益。

7. 與醫療及社會福利有關之處理

[77] 本條所稱「非營利組織」係指有政治、哲學、宗教、工會目標導向或性質之組織。

依據 GDPR 第 9 條第 2 項第 h 款之規定，凡根據歐盟法、歐盟成員國國內法或基於契約之基礎，基於醫療及社會福利之規定處理特種個人資料，包含因預防醫學（preventive medicine）或職業醫學（occupational medicine）目的而處理；評估員工工作能力而進行處理；為診斷（medical diagnosis）目的而處理；提供醫療行為、醫療照顧、社會照護（health, treatment, social care）而有必要處理特種個人資料；或為管理醫療或社會福利系統或服務而有必要處理特種個人資料等情形，得處理特種個人資料。除此之外，GDPR 第 9 條第 3 項規定，處理者應受相關保密義務條款之拘束。

8. 與公共衛生相關之處理

依據 GDPR 第 9 條第 2 項第 i 款之規定，明定因公共衛生而必要時得處理特種個人資料，例如，保護大眾免於受跨境疾病威脅或維持醫療、醫療產品及醫療儀器的高品質及水準。本條所指的公共利益必須基於歐盟法或歐盟成員國國內法且該法應含有特定的、適合的措施，保護當事人的基本權利和自由。

9. 與建檔、研究及統計相關之處理

依據 GDPR 第 9 條第 2 項第 j 款之規定，如基於歐盟法或歐盟成員國國內法之法規（on the basis of Union or Member State law），而以公共利益建檔目的（archiving purposes in the public interest）、科學或歷史研究目的（scientific or historical research purposes）、統計目的（statistical purposes），且達成目的與處理個人資料之間符合比例原則，得依本款處理特種個人資料。惟為保護當事人的基本權利及利益，應採取特定且適當安全維護措施（Safeguards）。此外，依 GDPR 第 89 條第 1 項之規定，該適合的保護措施須符合資料最小化原則（data minimisation）。

二、英國

（一）　一般及特種個人資料之定義

依據 UK GDPR 第 4 條：「個人資料係指自然人的姓名、身分證字號、位置資訊、網路識別碼、身體、生理、基因、心理、經濟、文化、社會身分等，得直接或間接識別特定自然人的資料。」而同法第 9 條第 1 項規定，所謂「特種個人資料」係指揭露種族或人種、政治意見、宗教或哲學信仰或工會會員之個人資料、以及基因資料、用以識別自然人之生物特徵識別資料、與健康相關或與自然人之性生活或性傾向有關個人資料之處理。

（二）　處理一般個人資料之合法要件

依據 UK GDPR 第 6 條之規定，處理一般個人資料之合法要件與 GDPR 第 6 條第 1 項之規定相同，但特別有二點值得說明：第一，UK GDPR 第 6 條第 1 項第 e 款「因公共利益或執行公務必須處理資料」事由，在 DPA 第 8 條特別說明，明定司法或立法單位執行法定職務時，應基於下列目的之一，始得處理一般個人資料：（1）司法行政；（2）行使議會任一院的職權；（3）執行法令或法律賦予的職能；（4）行使王室、王室部長或政府部門的職能；（5）支持或促進民主參與的活動。第二，在 UK GDPR 第 6 條第 1 項第 f 款規定「因追求自身或第三方正當利益必須處理資料」提及，本款不適用於公務機關執行其任務時所為之處理，且基於「正當利益」應限於訂定有限且詳盡的正當利益清單，始得處理之[78]。

而有關目的外處理之合法要件，依據 DPA 第 87 條之規定與 GDPR 規定相同，主要要求在任何情況下蒐集個人資料之目的必須明確、合法，且處理行為不得與蒐集目的不符，應符合下列二項要件：（1）控管者依法律規定，且其處理有必要性，並與該目的相稱；（2）

[78] 根據 2021 年 UK Data Protection Law 的計畫提案中，英國政府也希望澄清何時可以基於「正當利益」處理資料，包括，例如：針對某些 cookie 或人工智慧等。

個人資料處理與蒐集目的一致，包括出於公共利益之建檔目的而進行之處理、以科學或歷史研究為目的之處理，或用於統計目的之處理，以及為當事人的權利自由提供適當的保障。另外，英國資訊委員辦公室（Information Commissioner's Office, ICO）針對目的外處理表示，DPA 並未完全禁止進階處理之行為，若個人資料的使用目的改變，或產生原先未預期的新目的，且符合下列事由之一：(1) 與原目的相容；(2) 當事人明確同意；(3) 依法且該規定出於公共利益目的，若新舊目的相容，得進階處理個人資料[79]。

（三）　處理特種個人資料之合法要件

UK GDPR 第 9 條第 2 項所列例外得處理特種個人資料之事由，原則上與 GDPR 第 9 條第 2 項之規定相同，而 DPA 第 10 條就特種個人資料及刑事犯罪相關資料，得基於 UK GDPR 第 9 條第 2 項之例外情形加以處理。有關就業、社會安全、醫療診斷、公共利益、科學研究等目的使用特種個資，應符合 DPA 附表 1 中所列條件，以符合法律授權。另外，在 DPA 第 10 條第 5 項亦明訂，處理與刑事定罪和犯罪相關的個資，僅在符合 DPA 附表 1 的條件的情況下，處理才符合 UK GDPR 第 10 條第 1 項之法律授權要求。前述 DPA 附表 1 已詳細規範個別目的之個資判斷標準，同時，國務大臣可依法修訂 DPA 附表 1。

有關犯罪等涉及前科及犯罪之個人資料處理，則規範於 UK GDPR 第 10 條第 1 項：「依第 6 條第 1 項處理涉及前科及犯罪之個人資料或相關安全措施，僅有下列情形之一者，始得為之：於公務機關控制下所為之處理，或依國內法已為當事人之權利與自由，設有適當保護措施者。且任何全面性的前科紀錄僅限由公務機關控管保存。」，並於同條第 2 項敘明相關規範可依 DPA 第 10 條及第 11 條

[79] Information Commissioner's Office [ICO], *Principle (b): Purpose limitation*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/ (last visited Sep. 22)

第 2 項作為國內法律授權依據。

三、德國

（一）　一般及特種個人資料及處理之定義

德國有關「個人資料」（personenbezogene Daten）之定義，主要規定於 BDSG 第 46 條第 1 款，其內容與 GDPR 第 4 條第 1 款規定相同，主要係指有關識別或可得識別自然人（當事人）之任何資訊，例如參考姓名、身分證號碼、位置資料、網路識別碼或一個或多個該自然人之身體、生理、基因、心理、經濟、文化或社會認同等具體因素，而得直接或間接識別該自然人之資料。而所謂「特種個人資料」（besondere Kategorien personenbezogener Daten）則係規定於 BDSG 第 46 條第 14 款，與 GDPR 第 9 條第 1 項規定大致相同，包含種族、人種、政治意見、宗教或價值信仰及工會資格；基因資料[80]；用以識別自然人的生物特徵資料[81]；健康資料[82]；性生活或性傾向有關的資料。

而所謂「處理」（Verarbeitung）依據 BDSG 第 47 條第 2 款，與 GDPR 第 4 條第 2 款規定相同，係指不論是否透過自動化方式，或執行任何操作個人資料之行為。該處理個人資料之行為應符合 BDSG 第 48 條明訂之基本原理原則，應遵守（1）應以合法、可靠及信任予以處理；（2）蒐集目的須特定、明確及合法，且不得與此目的無關聯之處理；（3）處理限於處理目的、為實現處理目的所必要的，且不會

---

80 所謂「基因資料」（genetische Daten），依據 BDSG 第 46 條第 11 款之規定，係指涉及當事人遺傳性或突變性之基因特徵之個人資料，尤其是經由當事人生物樣本分析後，所取得關於該當事人獨特之生理或健康資訊。

81 所謂「生物特徵資料」（biometrische Daten），依據 BDSG 第 46 條第 12 款之規定，係指透過特定技術處理所得關於當事人身體、生理或行為特徵，而能夠或確認其特別識別性之個人資料，例如臉部圖像或指紋資料（daktyloskopische Daten）。

82 所謂「健康資料」（Gesundheitsdaten），依據 BDSG 第 46 條第 13 款之規定，係指涉及當事人身體或精神健康有關之個人資料，包括出現其健康情況之醫療照顧之資訊。

與此目的不相稱之行為；(4)為與事實相符必要時應即時更新；就此應採取一切合理措施，確保與處理目的不相符的個人資料立即刪除或更正；(5)保存期間不得長於處理目的所必要的期間，當事人之識別資料保存於一定形式等要求[83]。

（二）　一般個人資料之合法要件

德國作為歐盟成員國之一，亦應遵守 GDPR 第 6 條有關個人資料合法處理之原則要求，惟依據 GDPR 第 6 條第 3 項之規定，歐盟成員國得針對法定義務、公共利益或執行公務等合法要件，訂立國內法特別規範。因此，BDSG 第 3 條，補充 GDPR 第 6 條第 1 項第 e 款、第 2 項及第 3 項之規定，公務機關履行其範圍內職務，或委託控管者（Verantwortlichen）行使公權力內職務時，允許其處理個人資料。立法機關認為不論公務機關處理個人資料之行為是否具有「公共利益」，在執行公權力或受託行使公權力職務範圍內皆屬合法行為，特別加強公務機關處理個資之合法性基礎[84]。

除此之外，德國 BDSG 第 23 條及第 24 條針對「目的外處理」之態樣，另有特別規定，以補充 GDPR 第 5 條第 1 項第 b 款及第 6 條第 4 項之規範。其分別針對公務機關（öffentliche Stellen）及非公務機關（nichtöffentliche Stellen）分別予以規範，說明如下：

1. 公務機關目的外處理一般個人資料之合法要件

依據 BDSG 第 23 條第 1 項規定，若符合下列事由之一者，公務機關得於其執行職務範圍之目的外處理個人資料：

（1）明顯地為維護當事人法益，且無理由認為當事人會拒絕同意；

（2）對於當事人的說明有事實根據認為不正確，而須予以審核；

（3）基於必要之情形，為防止公共利益之重大損害，或公共安全、

---

[83] 同 GDPR 第 5 條第 1 項規定，但仍有些微差異。

[84] Taeger, Jügen und Gabel, Detlev, *DSGVO BDSG Kommentar, §3 Verarbeitung personenbezogener Daten durth öffentliche Stellen*, Aufl. 3, Rn. 1-7.

防衛或國家安全之危害；或為維護公眾之重大利益；或確保稅務及海關收益；

（4）有追訴犯罪或違反秩序之行為之必要，以強制執行（Vollstreckung）或執行《刑法典》（Strafgesetzbuch）第 11 條第 1 項第 8 款意義內之刑罰或措施；執行《少年法院法》（Jugendgerichtsgesetz）所定感化教育或教養方法；或為執行罰鍰之必要；

（5）為防止對他人權利嚴重損害之必要；

（6）為執行監督及管控之職權、會計審查或執行對控管者之組織調查；此亦適用於基於教育及考試之目的，由控管者處理個人資料之情形，但以當事人值得保護之法益未有衝突之範圍內為限。

2. 非公務機關目的外處理一般個人資料之合法要件

依據 BDSG 第 24 條第 1 項規定，若符合下列事由之一者，非公務機關得目的外處理個人資料：

（1）基於防止國家或公共安全之危害，或追訴犯罪之必要；

（2）為行使、主張或為對抗民法上請求權之必要。

（三）　處理特種個人資料之合法要件

依據 BDSG 第 22 條第 1 項第 1 款之補充規定，與 GDPR 第 9 條第 2 項之事由有別，不論「公務機關或非公務機關」，符合下列事由之一者，得例外處理特種個人資料：

（1）有行使自社會安全權利及社會保障衍生之權利，並且為履行因而產生之義務之必要；

（2）有必要基於健康照顧目的、為判斷受僱者之工作能力、為醫學診斷、為健康或社會領域之照顧或處置、為健康或社會領域系統及服務之管理，或基於當事人與健康職業成員之契約，並且該個人資料應由醫護人員、具有相應保密義務之特定個人，或控管者監督下予以處理。且資料處理之控管者利益須大於當事人利益；

（3）有必要基於公共健康領域內公共利益之理由，像是預防嚴重跨境的健康危險，或在健康照顧、藥品及醫療產品而維護高品質及安全標準；除第 2 項提及之措施外，職業上及刑法上保密義務應該被遵守。

（4）基於重大公共法益而有急迫之必要。

而同項第 2 款規定，「公務機關」如符合下列事由之一者，並且資料處理之控管者利益須大於當事人利益，得合法處理特種個人資料：

（1）為防止公共安全重大危險之必要；

（2）為防止對於公共利益（Gemeinwohl）之重大不利益，或為維護重大公共利益，有急迫之必要；

（3）基於國防、聯邦公務機關有必要基於在危機處理或衝突預防領域，或人道措施而履行跨國家或國際間之義務。

德國針對特種個人資料目的外之處理，補充 GDPR 第 9 條第 2 項之規定，就公務機關（öffentliche Stellen）及非公務機關（nichtöffentliche Stellen）分別予以規範，說明如下：

1. 公務機關目的外處理特種個人資料之合法要件

依據 BDSG 第 23 條第 2 項規定，公務機關目的外處理特種個人資料，須符合下列二項要件：

（1）公務機關於其執行職務範圍內，並具有下列事由之一：

A. 明顯地為維護當事人法益，且無理由認為當事人會拒絕同意；

B. 對於當事人的說明有事實根據認為不正確，而須予以審核；

C. 基於必要之情形，為防止公共利益之重大損害，或公共安全、防衛或國家安全之危害；或為維護公眾之重大利益；或確保稅務及海關收益；

D. 有追訴犯罪或違反秩序之行為之必要，以強制執行（Vollstreckung）或執行《刑法典》（Strafgesetzbuch）第 11 條第 1 項第 8 款意義內之刑罰或措施；執行《少年法院法》（Jugendgerichtsgesetz）所定感化教育或教養方法；或為執行罰鍰之必要；

E. 為防止對他人權利嚴重損害之必要；

F. 為履行監督及管控之職權、會計審查或執行對控管者之組織調查；此亦適用於基於教育及考試之目的，由控管者處理個人資料之情形，但以當事人值得保護之法益未有衝突之範圍內為限。

（2）具有 GDPR 第 9 條第 2 項或 BDSG 第 22 條之例外合法處理事由。

2. 非公務機關目的外處理特種個人資料之合法要件

依據 BDSG 第 24 條第 2 項規定，非公務機關目的外處理特種個人資料，須符合下列二項要件：

（1）非公務機關具有下列事由之一：

A. 基於防止國家或公共安全之危害，或追訴犯罪之必要；

B. 為行使、主張或為對抗民法上請求權之必要。

（2）具有 GDPR 第 9 條第 2 項或 BDSG 第 22 條之例外合法處理事由。

四、美國

（一）　一般及特種個人資料之定義

1. CCPA 及 CPRA 之相關規定

依照 CCPA 及 CPRA 第 1798.140 條第 v 項第 1 款規定，所謂「個人資料」（Personal information）係指能直接或間接識別、關聯、

描述或能合理相關聯（being associated with）或連結至特定消費者或家庭。可能包含姓名、化名（alias）、地址、獨特個人識別資料（unique personal identifier）、線上識別資料、IP 位址（Internet Protocol address）、電子郵件地址或其他類似識別資料。此外，也包含加州民法典第 1798.80 條第 e 項規定之個人資料；加州或聯邦法律保護的特徵；個人消費歷史紀錄或傾向等商業資料；生物識別資料；消費者瀏覽或搜尋歷史等網路資料；地理位置資料；聲音、電子、視覺、熱能或嗅覺等類似資料；專業或就業相關資料；教育資料；從個人資料所推斷出的個人剖析，反映出消費者的偏好、特徵、心理趨勢、傾向、行為、態度、智力、能力等屬性資料。

另外，所謂「敏感個人資料」（sensitive personal information），依據 CCPA 及 CPRA 第 1798.140 條第 ae 項之規定，包含社會安全號碼（social security number）、駕照號碼、州身分證或護照號碼；消費者的帳戶登入、金融帳戶、簽帳金融卡或信用卡號碼與任何必要之安全或存取代碼、密碼或允許存取帳戶的憑證（credentials）；消費者準確地理位置；消費者的種族或民族血統、宗教或哲學信仰或工會會員資格；消費者的郵件、電子郵件或訊息內容，除非企業是通訊的預期接收者；消費者的基因資料（genetic data）；生物識別資料（Biometric information），以達唯一識別消費者的目的；蒐集與分析消費者有關的健康、性生活或性傾向等個人資料。

然而，不論一般個人資料或敏感個人資料，依據 CCPA 及 CPRA 第 1798.140 條第 v 項第 2 款及第 3 款之規定，有關公開取得的資料、合法取得、公眾關注事件的真實資料以及經去識別化（deidentified）或匯總化（aggregate）之資料，則不屬於本法個人資料適用範圍。

2. UPDPA 之相關規定

依據 UPDPA 第 2 條第 10 款規定，所謂「個人資料」係指透過識別符號（identifier）直接識別或描述當事人的紀錄或假名化資料（pseudonymized data）。而「敏感性資料」則依據 UPDPA 第 2 條第

17 款規定，包含種族、民族、血統、宗教信仰、性別、性傾向、公民身分或移民身分、足以遠程存取帳戶的憑證（credentials）、信用卡或簽帳金融卡號碼或金融帳號、社會安全號碼、稅務號碼、駕照號碼、軍人身分號碼或其他政府核發的身分號碼、即時地理定位、犯罪紀錄、收入、疾病或健康狀況的診斷或治療、基因定序資料（genetic sequencing information）、資料控管者知悉或有理由知悉（knows or has reason to know）當事人未滿 13 歲等資料。

不過，如屬於公開資料；僅作為人體受試研究者的一部分進行處理或保存，並符合保護人體受試者的法律要求；依據令狀、傳票或法院要求或規則或其他法律要求之處理或揭露；受州公共紀錄公開要求之資料；或工作或求職過程中處理或儲存等資料，則依據 UPDPA 第 3 條第 c 項之規定，非屬本法保護範圍。

（二）　一般及特種個人資料之合法要件

1. CCPA 有關合法要件之規定

按照 CCPA 第 1798.100 條之規定，企業應於蒐集個人資料時或蒐集前，依法踐行告知義務，告知事項包含應蒐集的個人資料類別、敏感個人資料類別與相關利用資訊、保存期限或確定該期限的標準等資訊。同時企業保留個人資料或敏感個人資料的時間，不得超過蒐集個人資料目的之合理需求。而作為第三方的企業如果控制消費者個人資料的蒐集，可以透過於網路的主頁面以顯眼的方式提供前述告知義務。另外，作為第三方的企業控制在其場所（包含車輛內）蒐集消費者的個人資料，則企業應於蒐集時（前），以明確且顯眼的方式告知消費者將要蒐集的個人資料類別與使用該類別個人資料的目的，以及該個人資料是否被出售。

2. UPDPA 有關合法要件之規定

UPDPA 第 2 條第 2 項之規定將個人資料的處理，分為下列三種資料作業模式：

（1）相容性資料作業（compatible data practices）：依據 UPDPA 第 7 條之規定，當資料處理符合當事人期望或有利於當事人，控管者或處理者可未經當事人同意進行相容性資料作業；其中，應考量當事人與控管者關係、蒐集個人資料的交易類型、待處理個人資料類型與性質、利用或揭露個人資料對當事人產生負面結果的風險、防止未經授權利用或公開個人資料保障措施的有效性與該處理在何種程度促進當事人的經濟、健康或其他利益等因素。並且應符合下列相容性資料作業之要求：

A. 在當事人知情或參與的情形下，啟動或實施與當事人的交易；

B. 控管者遵循法律義務或監管是合理必要的；

C. 符合控管者或處理者在管理、人事、行政或營運特定且可解釋之需求；

D. 允許對控管者進行適當之內部監督或由政府單位或控管者或處理者的代理人進行外部監督；

E. 對建立假名化資料或去識別化資料是合理必要的；

F. 允許基於產品或服務的研究與開發進行一般研究（generalized research）之分析，一般研究係指利用個人資料來發現與公共衛生、公共政策或其他一般公共利益事項有關的事項，不包含利用個人資料來對特定的當事人進行預測或決定；

G. 對於犯罪之預防、發現、調查、通報、起訴或實際或潛在的補救所必要；

H. 協助根據第 7 款處理之個人或政府；

I. 遵循或維護法律要求之合理必要；

J.　其他可確定為相容性資料作業之目的。

控管者可以利用個人資料或向第三方控管者揭露假名化資料，向當事人提供定向廣告或其他純粹表達性內容，但禁止向當事人為差別對待。另外控管者與處理者可以依據 UPDPA 第 12 條至第 14 條所規定的自願性共識標準（voluntary consensus standard）進行個人資料處理，除非法院禁止該資料處理或該資料處理係屬不相容性的資料處理。

（2）不相容性資料作業（incompatible data practice）：依據 UPDPA 第 8 條之規定，當資料處理不屬於相容性資料作業，或雖符合相容性資料作業卻未落實隱私權政策規定時，即構成不相容性的資料作業。倘蒐集個人資料時，控管者向當事人提供充分的告知與資訊，使當事人理解不相容資料處理的性質，並有合理機會拒絕同意該資料處理，則控管者可以透過不相容資料處理來處理個人資料（但不包含敏感性資料）。此外，如未取得當事人之明確同意，控管者不得以不相容資料處理來處理敏感性資料。

（3）禁止性資料作業（prohibited data practice）：依據 UPDPA 第 9 條之規定，控管者不得從事禁止性資料作業；另外，重新識別或導致重新識別假名化資料或去識別化資料蒐集或建立個人資料，原則也被視為禁止性資料作業。

3. HIPAA 有關合法要件之規定

HIPAA 第 164.502 條、第 164.508 條及第 164.510 條針對「健康資訊」（Health Information）之蒐集、處理與利用為相關規範，原則規範個人健康資訊不得利用與揭露，除非取得個人授權同意、事先告知並給予選擇同意與否機會，或符合第 164.512 條 HIPAA 所定無須取得個人同意的情形。

五、日本

（一）　一般及特種個人資料之定義

依據日本個資法第 2 條第 1 項規定，「個人資料」係指與生存之個人有關的資料，被記載或記錄於文書、圖畫或電磁紀錄上，或使用聲音、動作及其他方法所表示之一切事項而得以識別特定個人者，包含個人識別符號者。依同條第 2 項之規定，所謂「個人識別符號」包括（1）運用電腦設備，將特定個人身體之部分特徵轉換為文字、號碼、記號或其他型態，而可供識別該特定個人者，例如數位化之指紋辨識符號或臉部特徵辨識符號；(2)提供予個人利用之服務或販賣給個人商品上所分配或核發個人之卡片、其他文件上記載或依電磁方式記錄之相關符號，而得以識別特定利用人、購買人或受核發人者，例如護照號碼、身分編號、保險證號碼、信用卡號碼等。上開兩種個人資料，若依政令被指定為「個人符號」則屬於本法之個人資料。

另外，依據日本個資法第 2 條第 3 項之規定，所謂「敏感性個人資料」（要配慮個人情報）係指當事人之種族、信仰、社會身分[85]、病歷、犯罪前科，因犯罪被害事實及其他對於當事人產生不當差別待遇、偏見及其他不利益者，在處理上須特別考量，包含於依政令所規定之記述等個人資料[86]。另依《個人資料保護法施行令》[87]第 2 條規定，「敏感性個人資料」包括（1）身體障礙、智能障礙、精神障礙（包括發展障礙）及其他個人資料保護委員會規則所規定之身心功能障礙；(2)對當事人為預防及早期發現疾病由醫生及其他從事醫療相關

---

[85] 指非依當事人意思、或當事人無法自主變更之出身，但不包含當事人工作之職位。依實務判例所見之例為非嫡出之子，或是被歧視之賤民部落出身等。

[86] 日本針對個人編號（マイナンバー）依個人資料保護法第 2 條第 1 項屬於一般個人資料，原則上蒐集、處理及利用應依個人資料保護法之規定。惟依番號法（行政手続における特定の個人を識別するための番号の利用等に関する法律）第 2 條第 8 項屬於特定個人資料（特定個人情報），僅於番號法有特別規定時始有適用，如限於納稅、社會保障、防災等利用目的及提供第三者之限制。

[87] 個人情報の保護に関する法律施行令(令和三年政令第五十六号による改正)。

職務人員進行之健康診斷及其他檢查結果;(3)根據健康診斷等的結果，或因疾病、受傷及其他身心變化，為改善當事人身心狀態由醫生等作成之指導或診療、調劑;(4) 以當事人作爲犯罪嫌疑人或被告，進行逮捕、搜索、扣押、拘留、提起公訴及其他刑事案件相關程序;(5) 當事人作爲《少年法》[88]第 3 條第 1 項規定之少年且為犯罪嫌疑人，進行調查、觀護措施、裁判、保護處分及其他少年保護事件相關程序。

（二）　一般個人資料之合法要件

依據日本個資法第 20 條規定，要求個人資料處理事業，不得以虛偽、其他不正當手段取得個人資料，以符合「適當取得之義務」之要求[89]。此外，依據第 17 條之規定，事業處理個人資料時，應盡可能特定其利用目的;若變更利用目的，事業不得逾越被認為與變更前利用目的有合理關連性之範圍。而第 21 條亦規定個人資料處理事業於取得個人資料時，除已預先公告其利用目的者外，應迅速將其利用目的通知當事人或公告之，若利用目的變更時，亦應通知當事人或公告變更之利用目的。

在目的外利用之情形，依第 18 條第 1 項規定，事業處理前未得到當事人之同意時，不得逾越前條之特定利用目的達成上所必要範圍，處理個人資料應具有下列合法事由之一：

1. 基於法令者；

2. 為保護人之生命、身體或財產而有必要時，且取得當事人同

---

88 少年法（令和元年法律第四十六号による改正)。

89 例如「未得父母同意，向未具有足夠判斷力之兒童，蒐集其父母之收入等家族或員工個人資料」、「強迫他人違法提供第三人資料」、「明知其他業者以不正當手段蒐集個人資料後，再轉交自己」，等均屬不正當蒐集個人資料事例，採較寬鬆之見解。且為避免業者脫法行為，並周全保障個人權益，如該當業者「明知」其前手為非法蒐集，或因「重大過失」不知前手為不正當蒐集者時，該當業者仍應繼承前手之瑕疵，而受本條之適用。

意有困難者；

3. 因公共衛生、兒童之健全育成而有特別必要者，且取得當事人同意有困難者

4. 為協助國家或地方自治團體或受其委託執行法令所定事務而有必要者，且如須取得當事人同意將使協助或執行受託業務產生困難者。

5. 個人資料處理事業為學術研究機關等，且個人資料係為供學術研究目的而有必要(包含處理個人資訊之部分目的係為學術研究)（有不當侵害個人權利利益之虞者，除外）。

6. 對學術研究機關提供個人資料，該學術研究機關係為研究之目的而有必要(包含處理個人資訊之部分目的係為學術研究）（有不當侵害個人權利利益之虞者，除外）。

除此之外，依據第 19 條規定，事業不得助長違法、不當行為或有誘發危害之方式利用個人資料，以防止不當利用個人資料致當事人權益受損。因此，不得具有下列消極要件：(1)「違法或不當行爲」，係指違反個人資料保護法及其他法令之行爲，或有違公序良俗，在社會觀念上非屬正當之行為（2)「助長或誘發之危害」，在認定上將限縮在以業者提供時有認識第三方將違法利用個人資料，並可預見提供個人資料將受違法利用之情形，以免造成寒蟬效應。

（三）　特種個人資料之合法要件

有關特種個資與一般個資之蒐集、處理及利用之合法要件，日本個資法大致上均相同，僅在取得之合法要件另有規定。依本法第 20 條第 2 項規定事業除下列所揭示情形之外，於事先未獲得當事人同意下，不得取得敏感性個人資料：

1. 基於法令規定者；

2. 為保護人之生命、身體或財產而有必要，於獲得當事人同意

有困難時；

3. 為提升公眾衛生或推廣兒童之健全發育有特別必要時，於獲得當事人同意有困難者；

4. 對國家機關或地方自治團體或受其委託者，為遂行法定事務有協助之必要，因獲得當事人同意，有對該當事務之遂行造成障礙之虞時；

5. 個人資料處理事業為學術研究機關等，且敏感性個人資料為學術研究目的而有必要（包含處理敏感性量個人資料之部分目的為學術研究）（有不當侵害個人權利利益之虞者，除外）。

6. 自學術研究機關取得敏感性個人資料，為學術研究之目的而有處理敏感性個人資料之必要時（包含取得敏感性個人資料之部分目的為學術研究）（有不當侵害個人權利利益之虞者，除外）（僅限個人資料處理事業與學術研究機關共同進行學術研究者）。

7. 敏感性個人資料，係由當事人、國家機關、地方自治團體、第 76 條第 1 項各款所揭示之人[90]（例如新聞媒體或宗教團體等）、其他依保護委員會規則所定之人所公開者；

8. 其他準用上開各款所揭示之情形，而為政令所規定者。例如依《個人資料保護法施行令》第 7 條規定，對於未經當事人同意即可取得敏感性個人資料另有兩款情形：（1）通過目視觀察或拍攝，取得其外觀上明顯屬於敏感性個人資料時（2）本法第 23 條第 5 項各款所揭示之情形[91]（包含依本法第 35

[90] 日本個人資料保護法第 57 條第 1 項除外規定共有 5 款情形，包括：(1)廣播機關、新聞社，通訊社及其他報導媒體（包含以報導為業之個人）供報導之用；(2)以著述為業者，供著述之目的利用；(3)宗教團體為供宗教活動（包含其附隨活動）目的之利用；(4)政治團體為政治活動（包含其附隨活動）之目的之利用 。

[91] 日本個資法第 27 條第 5 項規定，未經當事人同意得提供個人資料予第三人，

條之 2 第 6 項變更適用及本法第 35 條之 3 第 2 項準用變更適用之情形），即因委託、業務繼承或共同利用接收個人資料（個人デ一タ）且屬於敏感性個人資料時。故原則上提供特種個人資料予第三者時，亦應取得當事人同意始得為之。

綜上所列，日本針對敏感性特種個資之取得，除有相較當事人之權利、利益有應優先被保護者，或限制其取得不具有合理性者之法定事由外，原則上應事先得到當事人同意。

六、韓國

（一）　一般及特種個人資料與處理之定義

依據 PIPA 第 2 條第 1 款之規定，所謂「個人資料」係以某一資料雖無法特定個人，但可透過獲得其他資料的可能性而辨識特定個人，並限於現生存自然人之相關資料，符合下列事由之一者：（1）透過姓名、住民登錄號碼 、以及影像等，可以得知該特定人身分的資料（2）即使透過特定資料無法得知該特定人身分，但與其他資料結合後可得而知的情況，亦屬個人資料的範圍[92]。（3）前揭 1、2 款的資料進行假名化處理後，不需使用或結合其他資料，即可將該資料復原並得知該特定人身分者。

所謂「特種（敏感）資料」包含 PIPA 第 23 條第 1 款明列之思想、信仰、工會、政黨的加入或退出、政治傾向、健康、性生活及其他明顯侵害隱私之資料，以及 PIPA 施行細則第 18 條規定之基因檢

共有 3 款例外情形包括：(1)個人資訊處理事業於達成其利用目的所必要之範圍內，伴隨個人資料處理之全部或一部之委託，而該當個人資料被提供者；(2)因合併、其他事由繼承事業，該當個人資料被提供者；(3)於特定人間被共同利用之個人資料，而被提供給該當特定人時，預先將其意旨及被共同利用個人資料之項目、共同利用人之範圍、利用人之利用目的及對該當個人資料之管理負責任人之姓名或名稱、住所，及為法人時其代表人之姓名，通知當事人或置於當事人容易得知之狀態者。

92 屬於此種情況時，須合理考慮與其他資料整合時的難易度、其他資料取得的可能性，以及在整合之後，得知該特定人身分所需要花費的時間、費用、及技術。

測所獲得之 DNA 資料，或犯罪前科相關資料[93]。比較特別的是，PIPA 第 24 之 2 條針對「住民登錄號碼」歸類一般個人資料，惟原則上不得處理，僅有例外依法律明文規定、為免除個資當事人或第三人生命、身體、財產利益之急迫危險而顯有必要時，且應具備適當安全維護措施，始例外允許處理。

而所謂的「處理」根據 PIPA 第 2 條第 2 款之規定，係指對個人資料之蒐集、產生、連結、連動、紀錄、儲存、保留、加工、編輯、檢索、輸出、更正、回復、利用、提供、公開、銷毀及其他類似行為等態樣。

（二）　一般個人資料之合法要件

個人資料之處理主要規定於 PIPA 第三章，依據第 15 條第 1 項之規定，凡針對個人資料之蒐集、處理或利用，應具有下列合法事由之一：

1. 取得當事人同意；
2. 法律有特別規定或為遵守法令上義務而不可避免時；
3. 公務機關為執行法定職務而不可避免時；
4. 為與當事人締約或履行該約而不可避免時；
5. 當事人及其法定代理人陷於無法為意思表示之狀態，或住所不明等而無法取得事前同意，確實有明顯為防止當事人及第三方生命、身體、財產利益急迫之危害且必要時；
6. 為達成個人資料處理者之正當利益所必要，且該正當利益明顯優先於當事人的權利時。此情形僅限於與資料處理者之正

[93] 根據韓國個人資料保護法施行細則（Enforcement Decree）第 18 條規定，除 PIPA 第 23 條第 1 項規定的各款特種個資及公務機關根據第 18 條第 2 項第 5 款到第 9 款外，包含基因檢測所獲得之 DNA 資料，或犯罪前科相關資料。

當利益有相當關係且不超過合理範圍時。

除此之外，在不涉及侵害當事人或第三方利益時，資料處理者得依據 PIPA 第 18 條第 2 項所列事由之一，將個人資料提供予第三方。而資通訊服務提供者僅得適用下列第 1 款或第 2 款，另公務機關僅得適用第 5 款至第 9 款事由：

1. 自當事人取得作為其他用途之同意；
2. 其他法律有特別規定之情形；
3. 當事人及其法定代理人陷於無法為意思表示之狀態，或住所不明等，而無法取得事前同意，且確實有明顯為防止當事人及第三方生命、身體、財產利益急迫之危害且為必要時；
4. 刪除；
5. 若個人資料不得於規範範圍外使用或向第三方提供致無法執行其他法律已規定之業務職責時，保護委員會以審議、議決之；
6. 為履行條約、其他國際協議，而有對外國政府或國際組織提供之必要；
7. 為犯罪之搜查，或與公訴之提起及維持所必要；
8. 法院為執行裁判所必要；
9. 為執行刑罰及監護、保護處分所必要。

（三）　特種個人資料之合法要件

特種個人資料原則上不得蒐集、處理或利用，除非符合下列告知內容之規定，資料處理者始得為之：

1. PIPA 第 15 條第 2 項對於蒐集、處理或利用行為應告知事項有：(1) 資料蒐集及利用目的 (2) 蒐集個人資料的項目 (3)

保有暨利用個人資料的期間，以及（4）有權利拒絕同意之事實，及拒絕同意有不利益時，該不利益之內容。

2. PIPA 第 17 條第 2 項對於提供第三方之行為應告知事項有：（1）資料之接收者（2）資料接收者利用該資料之目的（3）個人資料被提供之項目（4）個人資料接收者保有及利用該個人資料之期間，以及（5）有權利拒絕同意之事實，及拒絕同意而產生之不利益內容。

根據第 23 條第 1 項之規定，資料處理者處理特種個人資料時，應依據本法第 29 條採取適當安全措施，以防止個人資料有遺失、竊取、洩漏、變造及毀損等情事。

七、新加坡

（一）　一般及特種個人資料之定義

依據 PDPA 第 2 條之規定，無論資料真實與否，凡從該等資料、或從該等資料及組織所有或可能得到之其他資訊，可直接或間接識別特定個人，均為本法所規範之個人資料。然而，依據第 4 條第 4 項及 5 項之規定，已保存超過 100 年以上、逝世超過 10 年以上者之個人資料，以及出於商業目的所提供之商務聯繫資訊，例如個人姓名、職稱或職務、業務電話號碼、營業地址、業務電子郵件、傳真號碼，或非專為個人目的所提供之其他類似資訊，則不適用 PDPA。此外，依據第 4 條第 1 項之規定，基於個人或家庭身分所為之個人活動、受雇員工於其組織僱傭期間所為之活動、任何公務機關或組織於其代表公務機關之期間所蒐集、利用及揭露個資的行為，以及任何法令規定基於特定目的應提供個人資料之行為，亦無本法之適用。

PDPA 並無針對特種或敏感個人資料進行定義及規範，但個人資料保護委員會（Personal Data Protection Commission，以下簡稱 PDPC）之諮詢指南[94]指出，個人資料敏感程度將影響組織個資保護政策及程

[94] PDPC, *supra* note 58, at 113.

序對個資安全維護措施之要求程度，進而影響 PDPC 對於違法行為是否加重減輕罰款額度之判斷。因此，蒐集個人資料屬於特別敏感資訊（例如身體或心理健康資訊），應於特定目的內利用並提供適當安全維護措施，否則將成為加重罰款之考量因素。在 PDPC 所發布指南及決定，敏感個人資料包括身分資訊（例如國民登記身分證及護照號碼）、金融財務資訊（例如交易及支付明細）、保險資訊（例如要保人或受益人姓名）、個人犯罪紀錄、醫療敏感資訊以及未成年人個資[95]。

（二）　一般個人資料之合法要件

根據 PDPA 第 13 條及第 14 條之規定，組織處理個人資料原則上應取得當事人同意，或具有認定為「視為同意」（deemed consent）之情形，即 PDPA 附件一[96]與附件二[97]所列事由之一，始得蒐集、利用或揭露個人資料：

1. 未經同意蒐集、利用或揭露個資之合法目的：PDPA 附件一

（1）明顯符合個人切身利益之目的：指有合理理由認為必須因應威脅該人或他人之生命、健康或安全緊急情況，為了聯繫任何傷者、患者或死者之親屬，未能及時取得同意或合理期待不會拒絕同意，並在可行範圍內通知之目的。

（2）影響公共事項之目的：基於公開的個人資料，或符合國家利益、用於藝術或文學目的、用於歷史紀錄或建檔目的、新聞組織用於新聞活動或廣播服務目的。

（3）基於正當利益之目的：例如評估所必要、司法調查或訴訟、

---

[95] PDPC, *supra* note 58, at 7.

[96] PDPA First Schedule: Collection, Use and Disclosure of Personal Data Without Consent.

[97] PDPA Second Schedule: Additional Bases for Collection, Use and Disclosure of Personal Data Without Consent.

債務關係、法律服務、信用報告、私人信託或福利計畫、為他人之個人或家庭目的提供服務、就業或業務需要、建立僱傭關係之目的，若組織蒐集、利用及揭露個資係基於該組織或他人正當利益，但不適用明文列舉之項目時，組織須清楚識別及闡明正當利益之情況或目的，包括利益內容及受益者；事前進行資料保護影響評估（Data Protection Impact Assessment, DPIA），以確定任何可能對個人所產生之不利影響，並採取合理措施以消除或減輕不利影響。經評估認為實施措施後仍可能殘留不利影響，應進行平衡性檢驗（balancing test）確認此正當利益是否高於所殘留之不利影響，並保存評估副本以提供 PDPC 審查；以及於個人資料保護政策揭露正當利益目的並提供資料存取權及諮詢服務[98]。

（4）商業資產交易之目的：係指各項買賣、租賃、併購、處置或融資之商業交易或相關交易行為，雙方或三方進行交易所需蒐集、利用或揭露個資，如未進行或未完成交易則須銷毀或歸還個人資料。

（5）促進商業改進之目的：為了改善或加強所提供之商品或服務，或開發新的商品或服務；改善或發展新興商業模式；瞭解客戶喜好；或客製化商品或服務所必要之目的，若不以單獨識別個人之形式利用所蒐集個人資料，將無法合理實現前述目的，且以契約或公司規則等方式，約束實施與維護適當保護措施的要求下，可未經同意利用或於企業集團內共享所蒐集之現有或潛在客戶之個資，以促進企業創新發展。同時，組織不可依據促進商業改進目的進行發送廣告行銷簡訊，必須獲得明確同意方能向個人發送廣告行銷簡訊。

98 Personal Data Protection Regulation 2021, Section 15.

2. 未經同意蒐集、利用或揭露個資之其他要件：PDPA 附件二

（1）符合公共利益之目的：組織得未經同意蒐集或利用由公務機關所揭露之個人資料，且蒐集或利用目的與公務機關揭露目的相符；若符合公共利益必要、制定政策或審查目的，則可未經同意向公務機關揭露教育機構在校生或畢業生個人資料；或醫療組織或醫療保健組織之患者個人資料；或出示公司負責人書面授權後向執法機關揭露個人資料。

（2）促進商業改進之目的：非公司組織為了改善或加強所提供之商品或服務，或開發新的商品或服務；改善或發展新興商業模式；瞭解客戶喜好；或客製化商品或服務所必要之目的，若不以單獨識別個人之形式利用所蒐集個人資料，將無法合理實現前述目的，且為通常智識之人認為是適當情況下，可未經同意利用所蒐集之個人資料。

（3）基於研究（包括歷史或統計研究）之目的[99]

（三）　特種個人資料之合法要件

由於 PDPA 並無將個人資料區分為一般及特種個人資料，因此，僅就 PDPC 針對身分證明號碼及未成年人個人資料之相關諮詢指南，分別說明如下：

1. 身分證明資訊

新加坡因為 2018 年最大醫療照護組織 SingHealth 遭駭客入侵，造成 150 萬筆患者資料恐已外洩[100]，使得 PDPC 重新審視並加強監管與身分辨識相關個資之蒐集、利用或揭露行為。PDPC 於 2018 年

---

[99] 詳見第五節 產業應用 第一項科學研究 壹、比較法 七、新加坡

[100] MINISTRY OF HEALTH [MOH], *Singhealth's It System Target Of Cyberattack* (Jul. 20,2018), https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack (last visited Oct. 6, 2021).

8 月發布諮詢指南[101]，嚴格規範有關身分證明號碼、複製本或實體卡片之蒐集、利用或揭露限制，並於 2019 年 9 月 1 日起開始實施，提供組織一年緩衝期間[102]。組織原則上不得蒐集、利用、保存或揭露國民身分證或其他類似形式的身分證明，例如出生證明、長期居留證或工作許可證、護照、駕照等號碼、複製本或實體卡片；除非符合下列二種情形，組織必須明確解釋必要性，並確實採取充足安全措施及遵守 PDPA 責任義務規定：

（1）法有明文：其他法律明文（例如入學或入職所必要），或 PDPA 視為同意以及例外允許未經同意之蒐集、利用或揭露行為（例如危及生命身體之緊急狀況），組織應通知個人蒐集、利用或揭露之目的以取得同意[103]；

（2）高度確認真實性之必要：為了避免安全風險（例如幼兒園訪客管制或 COVID-19 接觸者追蹤[104]），或可能造成他人或組織重大影響或損失之情況下，必須精準驗證或核對個人身分，於通知目的並取得同意後則可蒐集、利用或揭露國民身分證號碼。若僅是檢查國民身分證後歸還，則不被視為蒐集行為。

---

[101] PDPC, *Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers* (Aug. 2018), at 2-3, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf?la=en (last visited Oct. 6, 2021).

[102] PDPC, *PDPC Reminds Organisations on NRIC Advisory Guidelines Compliance Deadline* (Aug. 26, 2019), https://www.pdpc.gov.sg/news-and-events/press-room/2019/08/pdpc-reminds-organisations-on-nric-advisory-guidelines-compliance-deadline (last visited Oct. 6, 2021).

[103] PDPC, *Laws Requiring Collection of NRIC Number by Organisations* (Sep. 23, 2019), https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-nric-and-other-national-identification-numbers/nric-extracts (last visited Oct. 6, 2021).

[104] PDPC, *Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry* (Aug. 12, 2021), https://www.pdpc.gov.sg/help-and-resources/2021/05/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing#advisory1 (last visited Oct. 6, 2021).

個人若發現身分證明資料被非法蒐集、利用或揭露，可向 PDPC 提出申訴，經 PDPC 調查確認組織確實從事違法行為，將被要求停止行為，或銷毀、提交及更正資料。

2. 未成年人個人資料

針對蒐集、利用或揭露未成年人個人資料，根據 PDPC 所發布之諮詢指南，指出組織應透過經驗法則，考量未成年人是否理解同意的性質及後果，以確定未成年人是否能自行提供有效同意[105]。換言之，組織應根據實際狀況，足資可信或者可證未成年人並無充分了解所給予的同意及後果，應徵得具有法律地位之代理人同意。此外，如果組織正在或預期蒐集、利用或揭露未成年人個人資料，應考慮強化預防措施。例如為未成年人提供服務的組織，可透過容易理解的語言或者圖片等輔助工具，使隱私條款更容易理解。亦可採取額外安全防護措施，降低未經授權存取或揭露未成年人個人資料之風險，或進行匿名化處理[106]。

八、瑞士

（一）　一般及特種個人資料之定義

依照 DSG 第 5 條第 a 款之規定，所謂「個人資料」係指與可識別之自然人相關之所有資訊。另於同法第 2 條第 2 項規定，如自然人基於個人使用的個資處理；聯邦議會及議會委員會審議過程中處理之個資；或依照《聯邦東道國法[107]》（Gaststaatgesetz, GSG）第 2 條第 1 項於瑞士境內享有豁免權之機構受益人處理之個人資料，凡屬

---

105 PDPC, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (Otc. 2021), Chapter 7 Data Activities Relating to Minors, at 51-55, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (last visited Oct. 6, 2021).

106 *id*. at 54.

107 法律全稱：Bundesgesetz über die von der Schweiz als Gaststaat gewährten Vorrechte, Immunitäten und Erleichterungen sowie finanziellen Beiträge

於上述三種情形之一者，則無 DSG 之適用。

而依照 DSG 第 5 條第 c 款規定，所謂「敏感性個資」包含（1）宗教、意識形態、政治或與工會相關之觀點資料或活動資料（2）與健康、私密領域或種族出身有關之資料（3）遺傳基因資料（4）能識別特定單一自然人之生物辨識資料（5）與行政或刑事訴訟之進行中事項與制裁相關之資料；或（6）與社會扶助措施相關之資料。

另外，所稱之「處理」（bearbeiten）則依據 DSG 第 5 條第 d 款規定，係指所有牽涉個資之操作方式和程序，包含蒐集、儲存、保留、使用、修改、揭露、歸檔、刪除或銷毀等行為。

（二）　一般個人資料之合法要件

依據 DSG 第 2 條第 1 項之規定，將處理個資之主體區分為「私人」（private Personen）和聯邦機關（Bundesorgane），並於第 31 條及第 34 條分別規定處理個資之合法要件，以下分別說明：

1. 私人處理一般個資之合法要件

依據 DSG 第 31 條第 1 項之規定，私人處理個人資料，應具有（1）取得當事人之同意（2）依法律規定；或（3）具備足以凌駕當事人人格權之私人或公共利益，始得為之。其中，針對「足以凌駕當事人人格權之私人或公共利益」則依據同條第 2 項規定，除具有下列情形之一外，尚應納入衡平考量（fällt insbesondere），方屬具備合法要件：

（1）資料控管者為締結或履行契約，進而處理契約當事人之個人資料；

（2）資料控管者正在或即將與某自然人或法人進行商業競爭，因而不向第三方揭露自身之個人資料；

（3）資料控管者處理個人資料之目的，係為檢查該當事人之信

用（Kreditwürdigkeit）[108]；

（4）資料控管者係專業地處理個人資料，且目的僅為在定期出版的媒體上發表。但若未發表，個人資料將僅單獨作為資料控管者個人之專業工作素材；

（5）資料控管者處理個人資料，非為個人私益，而係為如研究、規劃或統計之公益目的[109]；

（6）資料控管者所蒐集之個人資料，為特定公眾人物於公開場合之活動紀錄。

2. 聯邦機關處理一般個資之合法要件

原則上凡法律有明文規定時，聯邦機關得處理個人資料，惟依據 DSG 第 34 條第 2 項之規定，特別下列三種情形：（1）牽涉處理敏感性個資之情形（2）牽涉剖析或特徵分析之情形；或（3）處理個資之目的或方式可能嚴重侵害當事人之基本權利，則必須以聯邦議會通過之法律明文為限。然而，如果（1）為執行法定任務，而處理個人資料為不可或缺之行為時；或（2）處理敏感性個資或進行剖析或特徵分析之目的，不會對個人資料之當事人，構成任何特別風險時，則依據 DSG 第 34 條第 3 項之規定，允許以經法律授權之法規命令為合法基礎。

---

[108] 所謂「目的為檢查該當事人信用」，應符合：（1）個人資料並非敏感性個資，亦非牽涉高風險之剖析或特徵分析（2）資料控管者僅得於「特定第三方以個人資料判斷是否與該當事人締結或履行合約」情形發生時，向該特定第三方揭露個人資料（3）資料控管者持有個人資料期間不得超過十年；以及（4）個人資料之當事人已達法定成年年齡。

[109] 如為研究、規劃或統計之公益目的者，應符合：（1）當資料控管者獲得許可、得以處理個人資料時，需即時將個人資料「匿名化」；若匿名化實為不可能或需付出不相稱之努力，資料控管者需採取適當措施，防止個人資料之當事人遭受識別（2）個人資料為敏感性個資時，資料控管者向第三方揭露個人資料時，須確保個人資料之當事人不會被第三方識別；若無法，資料控管者須確保第三方係非為個人私益而處理個人資料；以及（3）系爭研究、規劃或統計之成果，須以無法重新識別個人資料之當事人之方式公布。

除上述二種情形外，如符合 DSG 第 34 條第 4 項規定下列情形之一時，則聯邦機關得逕自處理個人資料：

（1）經聯邦委員會判斷，個人資料之相關人員之權利並未受到威脅，因而授權聯邦機關處理；

（2）個人資料之當事人已同意聯邦機關於特定、個別情況下處理，或是個人資料已可普遍、公開取得，個人資料之當事人亦無明確禁止聯邦機關處理；

（3）為保護個人資料之當事人或第三方之生命身體完整與安全，所為之必要處理，且無法及時於合理時間內獲得個人資料之當事人之同意。

（三）　處理特種個人資料之合法要件

有關特種個人資料之處理，私人除須符合前述 DSG 第 31 條第 1 項及第 2 項之規定外[110]，其針對特種個人資料，如係為檢查該當事人之信用時，不可處理該當事人之特種個人資料；且資料控管者如基於研究、規劃或統計之公共目的處理時，須確保第三方不會識別出當事人。

貳、我國規定及比較法分析

一、我國有關合法要件之相關規定

我國個資法對於個人資料分為一般個人資料及特種個人資料，依個資法第 2 條第 1 款規定，個人資料係指自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料；復依個資法第 6 條所指有關病歷、醫療、基因、性生活、健

[110] 詳見前文之說明，頁 59。

康檢查及犯罪前科之個人資料，即屬特種個人資料，特種個人資料以外之個人資料為一般個人資料。

（一）　一般個人資料合法要件

我國個資法將一般個人資料之蒐集、處理或利用之合法要件，區分為公務機關與非公務機關，以及特定目的內與目的外利用，以主體區分說明如下：

1. 公務機關有關一般個人資料合法要件之規定

公務機關對於一般個人資料，於特定目的內蒐集或處理時，依據個資法第 15 條規定，應具有下列事由之一，始得蒐集或處理該個人資料：

（1）　執行法定職務必要範圍內；

（2）　經當事人同意；

（3）　對當事人權益無侵害。

原則上公務機關對於個人資料之利用，於執行法定職務必要範圍內，與蒐集之特定目的相符，即得利用個人資料；惟若涉及目的外利用時，應符合個資法第 16 條但書所列各款事由之一，始得為之：

（1）　法律明文規定；

（2）　為維護國家安全或增進公共利益所必要；

（3）　為免除當事人之生命、身體、自由或財產上之危險；

（4）　為防止他人權益之重大危害；

（5）　公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人；

（6）　有利於當事人權益；

（7）　經當事人同意。

2.非公務機關有關一般個人資料合法要件之規定

有關非公務機關對於一般個人資料，依特定目的為蒐集或處理時，依據個資法第 19 條第 1 項之規定，應具有下列事由之一：

（1）法律明文規定；

（2）與當事人有契約或類似契約之關係，且已採取適當之安全措施；

（3）當事人自行公開或其他已合法公開之個人資料；

（4）學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人；

（5）經當事人同意；

（6）為增進公共利益所必要；

（7）個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限；

（8）對當事人權益無侵害。

原則上非公務機關對於個人資料之利用，應於蒐集之特定目的必要範圍內為之，若非公務機關欲目的外利用個人資料時，應符合個資法第 20 條第 1 項所列各款事由之一，始得為之：

（1）法律明文規定；

（2）為增進公共利益所必要；

（3）為免除當事人之生命、身體、自由或財產上之危險；

（4） 為防止他人權益之重大危害；

（5） 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人；

（6） 經當事人同意；

（7） 有利於當事人權益。

綜觀公務機關、非公務機關與特定目的內、目的外利用之規範比較，可從合法事由化約為後續比較法分析之重要論述，故整理一般個人資料之蒐集、處理或利用合法要件如下表：

表 10 我國有關一般個人資料蒐集、處理或利用之合法要件

合法要件		**蒐集、處理或目的範圍內利用**	**目的範圍外利用**
法律規定		○（含法定職務）	○
契約		○（非公務）	
公共利益		○（非公務）	○（公務另含國家安全）
保護個人利益	當事人		生命身體自由財產危險
	其他人		權益
公開或取自一般來源		○（非公務；一般來源須利益衡量）	
有利於當事人或對當事人無侵害		無侵害	有利當事人

註：不含「當事人同意」要件

資料來源：本計畫研究團隊自行整理

（二） 特種個人資料合法要件

我國針對特種個人資料之概念，依據個資法第 6 條第 1 項及個

資法施行細則第 4 條之規定，係指限於病歷[111]、醫療[112]、基因[113]、性生活[114]、健康檢查[115]及犯罪前科[116]之個人資料。原則禁止蒐集、處理或利用，僅有在符合下列合法性要件時，始得蒐集、處理或利用。

1. 法律明文規定；
2. 公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施；
3. 當事人自行公開或其他已合法公開之個人資料；
4. 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人；
5. 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施；
6. 經當事人書面同意。但逾越特定目的之必要範圍或其他法律另有限制不得僅依當事人書面同意蒐集、處理或利用，或其同意違反其意願者，不在此限。

綜觀特種個人資料之規範，相較於一般個人資料之規範架構與

---

111 依據個資法施行細則第 4 條第 1 款之規定，所謂「病歷之個人資料」指醫療法第 67 條第 2 項所列之各款資料。

112 依據個資法施行細則第 4 條第 2 款之規定，所謂「醫療之個人資料」指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。

113 依據個資法施行細則第 4 條第 3 款之規定，所謂「基因之個人資料」指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。

114 依據個資法施行細則第 4 條第 4 款之規定，所謂「性生活之個人資料」指性取向或性慣行之個人資料。

115 依據個資法施行細則第 4 條第 5 款之規定，所謂「健康檢查之個人資料」指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。

116 依據個資法施行細則第 4 條第 6 款之規定，所謂「犯罪前科之個人資料」指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

模式較為單純；因此，同樣地從合法事由化約為後續比較法分析之重要論述，故整理特種個人資料之蒐集、處理或利用合法要件如下表：

表 11 我國有關特種個人資料蒐集、處理或利用之合法要件

合法要件		蒐集、處理或目的範圍內利用	目的範圍外利用
法律規定		◯（含法定職務、法定義務）	需重新認定是否具備特定目的之合法事由
當事人自行公開		◯	
保護個人利益	當事人		
	其他人		
學術研究		◯	

註：不含「當事人同意」要件

資料來源：本計畫研究團隊自行整理

二、一般個人資料之比較法分析

在我國個資法規定尚未將蒐集處理利用樣態整合為單一「處理」行為前，綜觀各國個人資料保護規範，一般個人資料之蒐集處理利用合法要件，若扣除同意及科學研究等要件，主要可歸納為：法律規定、契約、公共利益、保護個人（含資料當事人及其他人）權利、（控管者）正當利益、對當事人權益有利或對其權利無侵害、取自公開資料或一般可得來源等類別，作為下列討論主軸，並同時整併我國與其他國家之比較。而依法律規定及契約二項合法性要件，各國並無顯著差異，故僅就其餘要件整理下列討論內容：

（一）　公共利益要件之類型化討論

目前依據我國個資法第 16 條第 2 款、第 19 條第 1 項第 6 款及第 20 條第 1 項第 2 款之規定，非公務機關在特定目的或目的外利用時，得以公共利益作為蒐集、處理、利用一般個人資料之合法要件，公務機關僅限目的外利用，有此要件，於法理上並無不當。惟因其具

備一定程度之不確定性，是否能以更清楚方式描述公共利益內涵，以使人民對規定能有更充分認識，從而降低適用上之困擾，亦值得進一步考量。

特別是，在觀察其他國家之特定目的內的公共利益要件時，歐盟、德國、英國、美國、新加坡及瑞士，對於公共利益要件有更清楚之說明。例如歐盟 GDPR 第 6 條第 1 項第 e 款限於歐盟或歐盟成員國之公共利益；英國在 UK GDPR 第 6 條第 1 項第 e 款規定，基於公共利益執行的任務或行使控管者的官方權力，亦有明確說明 6 種公共利益之態樣；瑞士 DSG 第 31 條第 1 項利益衡量，以及同條第 2 項規範之公共利益包含特定公眾人物於公開場合之活動紀錄；新加坡 PDPA 附件一亦有詳細明列判斷公共利益之事項(詳見下表整理)。相較於我國單純以廣義「公共利益」作為合法要件之立法形式，英國、新加坡及瑞士之規範方式，對於非公務機關之公共利益以明文方式規範適用之項目，更為清楚且具體化。

表 12 一般個人資料基於公共利益之合法要件比較表

國別	廣義公共利益	國家利益	職務相關	其他情形
我國	◯（限非公務機關）			
歐盟			◯	
德國			◯	
英國			◯	支持或促進民主參與的活動
瑞士	◯＋利益衡量 （限非公務機關）			新聞或公眾人物的公開活動（非公務機關）
美國 CCPA				
美國 UPDPA			◯（司法調查）	

日本				
韓國				
新加坡		○	○（執法）	如藝術文學、新聞廣播、教育、醫療

資料來源：本計畫研究團隊自行整理

另外，在觀察其他國家目的外利用的公共利益要件時，德國、瑞士、日本、韓國及新加坡，對於目的外利用適用公共利益要件時，有更清楚之說明。例如德國 BDSG 第 23 條第 1 項及第 24 條第 1 項明列公務機關及非公務機關適用之態樣；瑞士 DSG 第 31 條第 1 項規範利益衡量，以及同條第 2 項規範之公共利益包含特定公眾人物於公開場合之活動紀錄；日本個資法第 18 條第 3 項規定，因公共衛生、兒童之健全育成而有特別必要者，且取得當事人同意有困難者；韓國 PIPA 第 18 條第 2 項第 6 款限於為履行條約、其他國際協議，而有對外國政府或國際組織提供之必要，以及同項第 7 款至第 9 款所規定限於刑事追訴與執行之態樣；新加坡 PDPA 附件一及附件二，明確列舉影響公共事項與符合公共利益之特種情形。相較於我國僅單純以廣義「公共利益」作為合法要件之立法形式，其他國家多以明確化具體適用情事為立法方式，尤其瑞士允許非公務機關得以公共利益作為目的外利用合法要件，但仍要求應與當事人權益進行利益衡量。

表 13 一般個人資料基於公共利益目的外利用之比較表

國別	廣義公共利益	國家高權	行政目的	司法相關	其他
我國	○	國安（公務）			
歐盟		得立法			
德國		國安、防衛、公安等	如稅務海關、公眾利益、行政及考試監督	追訴犯罪、執行刑罰	
英國		得立法			
瑞士	○＋利益衡量（非公務機關）				如：新聞或公眾人物的公開活動（非公務機關）
美國 CCPA					
美國 UPDPA				司法調查	
日本					如公衛、兒童發展且難以取得同意（非公務機關）
韓國		條約義務		刑事追溯與執行	
新加坡		國家利益	執法		如藝術文學、新聞廣播、教育、醫療

資料來源：本計畫研究團隊自行整理

（二）　避免當事人及他人生命身體危險要件之討論

我國現行個資法第 16 條第 3 款與第 4 款，以及第 20 條第 1 項第 3 款與第 4 款規定，將為保護個人利益限縮於「目的外利用」之合法要件，且個資主體之利益包含生命法益、身體法益、自由法益及財產法益，而相對於當事人之第三人，則限於權益重大危害之情形，始有本款之適用。因此，針對「保護當事人利益」合法要件而言，可以進一步區分為三項值得說明的內容，分別是保護的權利類型、是否限於目的外利用之合法要件，以及是否有其他限縮適用之要件存在，透過下表彙整其他國家與我國之相關規定。

首先，以適用的權利類型而言，其他國家亦限於生命、身體等重要法益；另外，日本、韓國與我國一樣，法益類型包含財產上的權利，而德國則以法益的重大危害概括適用類型。整體而言我國規定與他國並無顯著不同。次者，綜觀其他國家規定，例如新加坡或歐盟體系之國家，將保護當事人或其他人之生命、身體危害作為合法要件之一時，不限於目的外利用之情形，此為我國於資料蒐集時所無之規定。最後，觀察日本、韓國、新加坡及瑞士等國家，除須具備「保護當事人或他人利益」要件，特別要求適用上必須限於「取得當事人同意有困難（或合理認為當事人不會反對）」之情形；相較起來，我國於條文設計上則未特別強調之。

表 14 一般個人資料有關避免當事人及他人生命身體危險要件之比較表

權利類型		生命	身體/健康	財產	自由	廣義規範
當事人權益						
無須考慮同意	目的內	歐、德、英	歐、德、英			
	目的外	我國	我國	我國	我國	
同意取得困難/不會拒絕	目的內	新、瑞	新、瑞			
	目的外	日、韓、新	日、韓、新	日、韓		德國
第三人權益						
無須考慮同意	目的內	歐、德、英	歐、德、英			
	目的外					我國、德國（重大危害）
同意取得困難/不會拒絕	目的內	新、瑞	新、瑞			
	目的外	日、韓、新	日、韓、新	日、韓		

資料來源：本計畫研究團隊自行整理

（三）　正當利益要件之討論

承認控管者正當利益的國家，就其細分之具體類型可分為「不限制正當利益種類，但要求與當事人權益進行利益衡量」以及「限制正當利益種類，但無利益衡量要求」等二大類。

有關以控管者之正當利益（legitimate interest）作為處理個人資料之合法要件，我國目前並無採納此一要件，惟多數國家有承認之合法要件，例如針對正當利益之特定目的內的處理行為，包含歐盟、德國、英國、瑞士、韓國及新加坡皆有廣泛正當利益之合法要件，並且要求資料控管者須符合利益衡量之要求；其中，瑞士 DSG 針對商業競爭以及信譽檢查；美國 UPDPA 針對業務管理、人事管理、行政管理、營運管理、去識別化及監督業務等具體化正當利益之情形；以及新加坡 DPDA 得基於改進商業之目的作為正當利益。

目的外處理得基於廣泛正當利益，並且資料控管者須符合利益衡量，則目前有瑞士與新加坡採納。且上述瑞士 DSG、美國 UPDPA 以及新加坡 DPDA 所列具體化情形，在目的外之正當利益時亦有適用；但德國 BDSG 則只在基於民事權利請求時，始得作為基於正當利益目的而目的外處理之事由。

（四）　對當事人影響、取自公開資料或一般可得來源要件之討論

當事人影響之合法要件，我國規定在個資法第 16 條第 6 款、第 19 條第 1 項第 8 款及第 20 條第 1 項第 7 款，分別承認「有利於當事人權益」、「對當事人權益無侵害」等要件。此種立法例較為少見，針對「有利於當事人權益」目前僅有 UPDPA 第 7 條承認此要件；而「對當事人權益無侵害」則於瑞士 DSG 第 31 條有明列，但限於聯邦機關始得適用此合法要件。參考我國個資法之修法理由，公務機關之規定係於「電腦處理個人資料保護法」立法時，參考當時有效之外

國法（德國及日本）所制定[117]。非公務機關，則係 2015 年修法時，立法委員考量非公務機關立法需要提案增訂。由於我國規定要求對當事人「有利」或「無侵害」，為了避免可能造成當事人權益微小侵害而引發爭端，目前實務上產業應用時，部分業者盡量避免援引此要件[118]。

而取自公開資料或一般可得來源之合法要件，與前述內容理由相同，相較於其他國家而言，立法體例較為少見。目前美國 CCPA 及 UPDPA 將此類個人資料排除法規適用範圍，而新加坡 PDPA 及瑞士 DSG 亦有相似規範，但瑞士 DSG 則是限縮於當事人不為反對意見時。我國目前個資法第 19 條第 1 項第 7 款規定，非公務機關於特定目的內，始有適用；溯其立法理由之說明，公開資料可作為合法蒐集要件，或經過與當事人利益衡量狀況下，以一般可得來源作為合法蒐集要件，係「電腦處理個人資料保護法」及 2010 年修法時，參考當時有效之德國法制定。然而，目前我國實務上，曾發生業者蒐集基於法律或商業上需要所公開之資訊（如律師執業資訊），整理後販賣給其他業者做行銷使用；或利用大學申請入學榜單等公開資訊，整理為查榜系統，而意外拼湊當事人求學歷程，造成當事人困擾等事件。

三、 特種個人資料之比較法分析

特種個人資料之蒐集、處理及利用合法要件，在不討論同意要件之前提，合法要件主要可歸納為：法律規定、公共利益、保護個人（含資料當事人及其他人）權利、當事人自行公開、對當事人權益有利、學術研究及非營利組織等類別[119]。以下就特種個人資料合法要件之重要議題，包含特種個人資料之概念及立法例，以及較有爭議之三項合法要件，整理如下：

---

117 立法院公報，第 83 卷第 45 期，頁 521-541（1994）。

118 立法院公報，第 102 卷第 4 期，頁 14-15（2012）。

119 有關「學術研究」之要件討論，詳見 0 第二章　個人資料保護法相關議題研析 第五節 產業應用 第一項科學研究內容。

（一）　特種個人資料之定義及立法例之討論

我國參考 1995 年歐盟資料保護指令、德國聯邦個人資料保護法第 13 條及奧地利聯邦個人資料保護法等外國立法例，於 2010 年增訂個資法第 6 條之規定，並將特種個人資料限於病歷、醫療、基因、性生活、健康檢查及犯罪前科等 6 種類別，另以個資法施行細則第 4 條加以補充說明[120]。立法技術上屬於「列舉規定」之形式，即僅以法律明文列舉之內容為限。然而，綜觀其他國家之特種個人資料之定義及範圍，特別在健康、遺傳基因、性生活、種族、宗教或哲學信仰、政治傾向、工會身分、生物特徵識別等資料屬性上，各國雖概念不一，但普遍承認相關概念屬於特種個人資料之範疇（詳見下表之比較表格）。

較需特別說明者有二：其一，美國基於交易安全之目的，承認金融帳戶、簽帳金融卡或信用卡號碼、存取憑證等金融資料亦屬於特種個人資料；而新加坡則未明文規定特種個人資料，但對身分證明號碼等敏感性資料有發布相關諮詢指南。其二，從立法技術上比較，目前多數國家包含我國，均採行列舉規定，而日本及韓國則採「例示規定」的方式，如日本承認「其他對於當事人產生不當差別待遇、偏見及其他不利益者」，而韓國承認「其他對當事人明顯侵害隱私之資料」，並透過行政規則補充說明例示規定。

[120] 立法院公報，第 97 卷第 48 期，頁 128-132（2008）。

表 15 我國與各國有關特種個人資料立法例之比較

要件／國別	明文規範	要件標準	類別 ※各國針對各項類別範圍仍有差異									
			健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會身分	其他
我國	○	列舉	○	○		○	○					
歐盟	○		○	○	○	○	○	○	○	○	○	
德國	○		○	○	○	○	○	○	○	○	○	
英國	○		○	○	○	○	○	○	○	○	○	
瑞士	○		○	○	○	○		○	○	○	○	社會扶助措施
美國 CCPA	○		○	○	○		○	○	○		○	身分號碼、金融資料、地理位置等
美國 UPDPA	○		○	○		○	○	○	○			身分號碼、金融資料、地理位置等
日本	○	例示	○			○		○	○			社會身分等
韓國	○		○				○		○	○	○	思想
新加坡	X	諮詢指南	無規定特種個資，所有個資適用相同規定									身分證明資訊

資料來源：本計畫研究團隊自行整理

（二）　履行法定義務要件之討論

我國為使公務機關或非公務機關蒐集、處理或利用特種個人資料得依法為之，且依相關規定提供適當安全維護措施，爰仿 1995 年歐盟資料保護指令第 8 條及德國聯邦個人資料保護法第 28 條等外國立法例，於 2010 年個人資料保護法修訂第 6 條第 1 項但書第 2 款規定[121]。當蒐集、處理或利用特種個人資料，係屬公務機關執行法定職務或非公務機關履行法定義務必要範圍內，如檢警機關偵辦犯罪，蒐集或利用涉嫌人之犯罪前科資料；醫生發現疑似法定傳染病，蒐集相關醫療資料通報主管機關等，得依本款作為合法要件。

而所謂「法定職務」依個資法施行細則第 10 條之規定，指法律、法律授權之命令、自治條例、法律或自治條例授權之自治規則、法律或中央法規授權之委辦規則。參考國外立法例，GDPR 第 6 條第 3 項第 b 款規定，若援引執行法定職務、履行法定義務作為運用個資之合法要件，該法律內容可能包括規範控管者運用個資之合法性一般條款、個資類型、個資當事人、揭露對象及目的、目的限制、儲存期間等具體規定；且日本、韓國、我國未就該法律或法規命令所需具備之具體程度為相關規定。

（三）　公共利益及保護個人利益要件之討論

相較於一般個人資料，目前我國個資法第 6 條規定並未將公共利益作為蒐集、處理利用特種個人資料之合法要件。然而，參照其他國家之個資法規定，例如歐盟 GDPR 第 9 條第 2 項第 g 款及 UK GDPR 第 9 條第 2 項第 g 款規定，皆承認重大公共利益作為合法要件，但須與資料當事人的權益進行利益衡量；而德國 BDSG 第 22 條第 1 項第 2 款則限於公務機關，得基於國防安全、追訴犯罪、執行刑罰或健康照護或藥品醫材安全；瑞士 DSG 第 31 條第 2 項第 5 款規定，得以研究、規劃或統計之公益目的；美國 UDPDA 第 7 條規定包含公共衛生、公共政策或其他一般公共利益，以及日本個資法第 20

[121] 立法院公報，第 97 卷第 48 期，頁 128-132（2008）。

條第 2 項規定在公共衛生、兒童發展之必要且難以取得同意，得例外允許運用特種個人資料。

表 16 特種個人資料基於公共利益要件之比較表

國別	重大公共利益	國家高權	司法相關	其他情形
我國				
歐盟	◯+利益衡量		◯	◯醫療及社會福利、公共衛生
德國	◯+利益衡量	◯國防安全	◯追訴犯罪、執行刑罰	◯健康照護或藥品醫材安全
英國	◯+利益衡量		◯	◯公共衛生
瑞士				◯研究、規劃或統計
美國 CCPA				
美國 UPDPA			◯司法調查	◯公共衛生、公共政策或其他一般公共利益
日本				◯公共衛生、兒童發展之必要且難以取得同意
韓國				
新加坡				

資料來源：本計畫研究團隊自行整理

我國現行個資法第 6 條並未如一般個人資料之相關規定，即個資法第 16 條第 3 款與第 4 款，以及第 20 條第 1 項第 3 款與第 4 款，設有「保護當事人利益」之相關規範。然而，參考其他國家之規定，例如歐盟 GDPR 第 9 條第 2 項第 c 款規定；英國 UK GDPR 第 9 條第 2 項第 c 款規定；瑞士 DSG 第 34 條第 4 項規定；日本個資法第 20 條第 2 項第 2 款之規定，均有針對生命或身體法益，得在未取得

當事人同意下，逕對特種個人資料進行處理。

比較特別的是，日本相對於上述其他國家之保護利益，將「財產利益」亦納入保護範圍；而美國 UPDPA 第 7 條則規定，在符合當事人期望或有利於當事人，控管者或處理者可以不經當事人同意進行相容性資料作業。另外，各國對於保護個人利益之合法要件，均限於「難以取得當事人同意」之情形，歐盟體系對此採取嚴格標準，須當事人因身體因素無法給予同意或被法律定義為無能力給予同意之情形，始得為之。

表 17 特種個人資料基於保護個人利益要件之比較表

國別		生命	身體	財產	其他說明
我國		N/A			
歐盟	當事人	○	○		限於當事人因身體因素無法給予同意或被法律定義為無能力給予同意之情形
	其他人	○	○		
德國	當事人	○	○		
	其他人	○	○		
英國	當事人	○	○		
	其他人	○	○		
瑞士	當事人	○	○		
	其他人	○	○		
美國 CCPA	當事人				
	其他人				
美國 UPDPA	當事人	符合當事人期望或有利於當事人			
	其他人				
日本	當事人	○	○	○	同上
	其他人	○	○	○	
韓國		N/A			
新加坡		N/A			

資料來源：本計畫研究團隊自行整理

（四）　取自公開資料或一般可得來源要件之討論

而有關個資法第 6 條第 1 項第 3 款「當事人自行公開」或其他「已合法公開」之合法要件，我國個資法於 2010 年修訂時，考量當事人已自行公開或其他合法公開之個人資料，隱私已無被侵害之虞，爰修訂本法第 6 條第 1 項但書第 3 款之規定。依個資法施行細則第 13 條規定，當事人自行公開之個人資料係指當事人自行對不特定人或特定多數人揭露其個人資料；已合法公開之個人資料則包括依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

綜觀多數國家（歐盟、德國、英國、瑞士、美國 UPDPA 及日本）均有「當事人自行公開」之合法要件；但對於「其他已合法公開」之要件，目前僅有日本採納。因此，是否仍有必要保留「其他已合法公開」作為蒐集、處理及利用特種個人資料之合法事由，殊值疑義。然而，前者「當事人自行公開」之合法要件，在現行實務之司法判決，特別在非公務機關基於新聞報導之公益目的，得引用法院公開之判決資訊，蒐集當事人犯罪個人資料，素有爭議[122]。但多數國家在適用此條款時，會就進階處理時的目的相容性作為判斷，特別是歐盟體系對於當事人自行公開之合法要件，限於明顯由當事人自行公開之特種個人資料，且須限於當事人明顯有意公開資料，且進階處理仍須符合原始利用目的之相容性及其公開之情境脈絡。

表 18 特種個人資料基於公開資料或一般可得來源要件之比較表

國別	自行公開	合法公開	其他說明
我國	◯	◯	
歐盟	◯		明顯由當事人自行公開+進階處理之相容性判斷
德國	◯		
英國	◯		

[122] 參照臺灣臺北地方法院 109 年訴字第 2188 號民事判決，以及臺灣高等法院臺中分院 109 年上易字第 458 號刑事判決。

瑞士	◯		
美國 CCPA			
美國 UPDPA	◯		
日本	◯	◯	
韓國			
新加坡			

資料來源：本計畫研究團隊自行整理

參、分析與小結

在個人資料蒐集、處理或利用之合法要件（不含當事人同意）討論上，從大方向而言，主要討論及關注二大議題，分別為個人資料法律概念及立法例的選擇，以及合法要件之相關細節檢討及修訂。前者主要針對特種個人資料目前採列舉規定，而近來引發諸多討論之人臉識別應用、穿戴式裝置等新興科技，蒐集臉部、指掌紋、聲紋等敏感個人資料，目前未列入我國個資法第 6 條第 1 項之特種個資，而基於人權保障之目的，未來可參考日本及韓國透過例示方式，加以適當地補充，以周延地保護個人資料當事人權益的方式，值得我國未來修法之考量。

後者又可細分為一般個人資料在公務機關與非公務機關，以及各種個人資料之合法要件二項議題，而一般個人資料在避免當事人及他人生命身體危險要件，參考比較法之規範，可不限於目的內利用，但建議應有其他限縮適用之要件存在；而正當利益部分，目前我國並無此合法要件，但參考多數國家皆有相關規定，亦值得採納，以促進資料合法之流通。

而不論是一般個人資料或特種個人資料，在合法要件的探討上，皆涉及到「公共利益」要件、「保護個人利益」要件以及「取自公開資料或一般可得來源」要件。公共利益在法理上自屬不確定之法律概念，如未來能參考其他多數國家之立法規範，具體化明確描述公共利益之適用態樣，將有助於降低法律適用之疑義。而保護個人利益部

分，特別是特種個人資料的部分，建議應參考歐盟之相關規定，限於當事人因身體因素無法給予同意，或被法律定義為無能力給予同意之情形，較能對於資料當事人提供周全之隱私保護。最後，有關取自公開資料或一般可得來源之要件，觀諸我國個資法之立法理由，主要參考德國及日本等舊個資法規定，但在一般個人資料部分德國已刪除此一合法要件，而在特種個人資料部分，歐盟國家須以明顯由當事人自行公開，且須符合進階處理之相容性判斷。這些合法要件在適用上相對嚴格，相關條文之實際應用情境，建議我國未來修法時應一併納入考量，適時調整我國個資法之合法要件。

第二項　受託處理者義務

壹、比較法國家

一、歐盟

（一）　資料控管者與受託處理者之概念

依據 GDPR 第 4 條第 7 項規定，所謂「控管者」（controller）係指決定個人資料處理目的及方式的自然人、法人、公務機關、仲介或其他單位；而「受託處理者」（processor）依據 GDPR 第 4 條第 8 項規定，則係指替資料控管者處理個人資料的自然人、法人、公務機關、仲介或其他單位。受託處理者與資料控管者個別為獨立的個體，而委託方式包含委託多位受託處理者，或委託單一受託處理者，再由該受託處理者複委託資料處理業務[123]。

（二）　受託處理者之相關義務

依據 GDPR 第 28 條第 1 項規定，資料控管者應確保受託處理者能夠有效地保證（sufficient guarantees），採取適當技術上與組織上措

[123] EDPB, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (2021), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en, at para 75-76 (last visited Jan. 14).

施並遵守 GDPR 之相關規範要求。EDPB 對於控管者及受託處理者，於 2021 年發布相關指引，建議控管者評估受託處理者之專業知識、信用信賴程度、資源、市場地位及名聲等內容，以決定是否符合委託個人資料之事務[124]。此外，依據 GDPR 第 28 條第 3 項及第 9 項之規定，個人資料之委外契約應以書面（含電子）契約簽訂，且 EDPB 建議契約之內容不得僅將條文內容複製貼上，應針對個案情形撰寫，例如低風險之資料處理則不需高強度保護措施，且雙方應依個案情形撰寫較詳盡的條文內容，細數應如何達到每項要求、安全措施之強度、風險程度、當事人之權利等，且應在契約中同一區段呈現，例如可以附件方式一併呈現[125]。EDPB 建議契約中最少應包含以下項目[126]：

（1）委外資料處理之服務內容：不得概括呈現，應盡量詳細並清楚描述所處理之資料。

（2）資料處理之時間：應載明確切資料處理之時間或是以何標準訂定資料處理的時間。

（3）資料處理之特性：資料處理之方式（錄影、錄音、儲存圖檔）以及資料處理目的。

（4）資料處理之種類：應盡量詳細描述，只敘述個資種類為一般個資或特種個資並不足夠，特種個資至少須記載為哪一種類之特種個資。

（5）當事人之分類：應盡量詳細描述，例如訪客、員工、快遞公司等。

（6）資料控管者之權利義務：資料控管者之義務包含提供須處理之資料、下指令並紀錄、確保受託處理者皆遵守 GDPR 要求、適時監督以及驗證抽查。

資料控管者或受託處理者如果位於歐盟境外且受域外效力規範

124 *id*, at para 97.
125 *id*, at para 103, 112-113.
126 *id*, at para 114.

時，依據 GDPR 第 27 條規定須在歐盟境內指定一位代表，該代表必須位於接受商品、服務、監控之當事人所屬會員國境內，但是如果所處理之資料為非經常性、小規模、以及非特種個資，則不需在歐盟境內指定一位代表。依前言第 80 點規定，資料控管者或受託處理者必須以書面方式授權該代表，個資監管機關有權聯繫該代表。另外，資料處理委外契約中應涵蓋資料控管者監督義務及受託處理者義務相關條款：

（1）依 GDPR 第 28 條第 3 項第 a 款、第 29 條規定，受託處理者只能依資料控管者書面指令處理資料，書面是指以任何文字形式呈現，含電子方式，EDPB 建議將書面指令與契約一起存放[127]。

（2）依 GDPR 第 28 條第 3 項第 b 款規定，受託處理者應確保其雇用之全職、臨時員工盡保密義務，受託處理者應只給予需要接觸個人資料的員工存取權[128]。

（3）依 GDPR 第 28 條第 3 項第 c 款規定，受託處理者應遵守 GDPR 第 32 條安全處理要求，依照風險採取適當措施。如安全處理措施有異動，受託處理者應事先取得資料控管者之同意[129]。

（4）依 GDPR 第 28 條第 2 項、第 28 條第 3 項第 d 款規定，未經資料控管者書面授權同意，受託處理者不得複委託業務給其他處理者，書面授權之形式可較限縮或寬鬆，契約中應載明取得授權同意的程序，寬鬆的書面授權至少應載明受託處理者在變更複委託者時應告知資料控管者，告知後資料控管者有反對權，如未反對則視為同意[130]。複委託必須以契約形式約定之，並要求複委託者遵守與受託處理者相同的權利義

[127] EDPB, *supra* note 123, at para 118.
[128] EDPB, *supra* note 123, at para 123.
[129] EDPB, *supra* note 123, at para 126.
[130] EDPB, *supra* note 123, at para 128.

務。GDPR 第 28 條第 4 項明定，如複委託者有違法之情形，受託處理者對資料控管者負有責任[131]。

（5）依 GDPR 第 28 條第 3 項第 e 款規定，受託處理者應協助資料控管者履行當事人權利，協助程度依個案而定，小則為傳達當事人需求或是讓資料控管者直接取得、管理個人資料，因此契約應載明受託處理者協助之方式[132]。

（6）依 GDPR 第 28 條第 3 項第 f 款、第 32 至 36 條規定，受託處理者應協助資料控管者履行安全處理要求、個資事故要求、資料保護影響評估要求、監管機關諮詢要求，且於契約中載明應遵循的程序或將應填寫之表單作為附件[133]。個人資料事故發生時，受託處理者亦須及時通知資料控管者，EDPB 建議可於契約中明定幾小時內受託處理者須通報資料控管者、資料控管者窗口、通報方式及內容[134]。

（7）GDPR 第 28 條第 3 項第 g 款規定，依資料控管者之選擇，受託處理者得刪除或歸還全部個人資料，並刪除任何複製本。

（8）依 GDPR 第 28 條第 3 項第 h 款規定，受託處理者應提供資料控管者所有資料已證明遵循 GDPR 第 28 條之義務，如受託處理者認為資料控管者之指令違反 GDPR，應立即告知資料控管者。

（9）GDPR 第 30 條規定雙方都須針對資料處理盡紀錄義務，此為資料控管者與受託處理者最重要的義務。

（10） 個資事故發生時，依 GDPR 第 33 條第 2 項規定，受託處理者應於發現事故 72 小時內通報資料控管者，不得無故延遲通報。

此外，隱私監管機關愛爾蘭資料保護委員會（Ireland's Data

131 EDPB, *supra* note 123, at para 129.
132 EDPB, *supra* note 123, at para 130-131.
133 EDPB, *supra* note 123, at para 133.
134 EDPB, *supra* note 123 at para 136.

Protection Commission，DPC）於 2019 年發布指引，強調 GDPR 第 28 條第 3 項要求之強制委外契約條款之重要性[135]。因此如受託處理者不遵從資料控管者的指令處理資料而自行決定資料處理方式，依據 GDPR 第 28 條第 10 項規定，受託處理者即被視為資料控管者；而依據 GDPR 第 82 條當事人可直接向受託處理者請求損害賠償。GDPR 第 82 條第 4 項及第 5 項規定，若涉及多位受託處理者時，包含複委託關係，每一位受託處理者應負獨立且全部之損害賠償責任，但是事後得向其他受託處理者請求補償金額。

二、英國

英國有關資料控管者及受託處理者之規定，主要規範於 UK GDPR 第 4 條第 7 項及 DPA 第 6 條，與 GDPR 規定相同。比較特別的是，在 DPA 第 209 條規定，行政部門視為各自獨立，政府部門間無法簽訂契約時，得以備忘錄形式為之。如資料控管者涉及皇室、蘭開斯特公國（Duchy of Lancaster）或康瓦爾公國（Duchy of Cornwall），則另有特殊規定；雖然，政府部門或皇室及公國成員不會被起訴相關刑事責任，但根據 DPA 第 209 條第 6 項 C 款，為官方服務之資料控管者可能被起訴。

英國有關受託處理者義務主要規範於 UK GDPR 及 DPA 第四章，內容與歐盟 GDPR 相同。除此之外，ICO 也針對此進一步發布「資料控管者和受託處理者指南」。此外，ICO 針對資料控管者和受託處理者間的契約，發布相關標準契約條款以供參酌[136]，相關契約內

[135] DATA PTROTECTION COMMISSION [DPC], *A Practical Guide to Controller-Processor Contracts* (2019), https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190624%20Practical%20Guide%20to%20Controller-Processor%20Contracts.pdf (last visited Jan. 14).

[136] ICO, *What needs to be included in the contract?*, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/#10 (last visited Jan.14,2022)

容之要求與歐盟 EDPB 前述之內容相符，應包含特定內容與條款[137]。

三、德國

德國有關「資料控管者」（Verantwortlicher）與「受託處理者」（Auftragsverarbeiter），主要規定於 BDSG 第 46 條第 7 款與第 8 款，與歐盟 GDPR 之規定相同。而 BDSG 第 62 條第 5 項同樣與 GDPR 規定相同，並要求個人資料委託契約須明訂下列條款，且該契約或其他法律文件必須包含處理對象、處理日期、處理類型、處理目的、資料種類、當事人類型及資料控管者之權利義務：

1. 受託處理者原則僅得依據資料控管者之書面指示處理個人資料，除非受託處理者認為該指示違法時，得例外不遵守資料控管者之意見，但應立即通知資料控管者[138]。

2. 除法律另有規定外，資料控管者應確保受託處理之相關人員負有保密義務；

3. 受託處理者應協助資料控管者遵守當事人權利之相關規定；

4. 若依據法律規定受託處理者不具有儲存資料義務時，則仍應依控管者要求，於委託服務結束後返還或刪除所有個人資料，或提供銷毀之副本資料；

5. 受託處理者應提供資料控管者，依據 GDPR 第 76 條規定之日誌，以作為證明其履行義務之文件；

6. 資料控管者或其委託第三方之驗證得要求由受託處理者履

[137] ICO, Contracts, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/ (last visited Jan.14, 2022)

[138] BDSG 針對遵守資料控管者之指示亦有規範，依據 BDSG 第 52 條第 1 項之規定，凡從屬於控管者或授予權限得近用個人資料之受託處理者，除非法律另有規定外，受託處理者僅得就資料控管者之指示處理個人資料。

行；

7. 在複委託或共同受託處理之情形，受託處理者應遵循控管者對其他受託處理者之相同要求；

8. 受託處理者應採取 BDSG 第 64 條之資料安全要求；

9. 受託處理者應衡量處理類型以及現存資訊，協助資料控管者符合 BDSG 第第 64 條至第 67 條及 69 條規範之義務[139]。

另外，針對受託處理者的義務規範，包括 BDSG 第 64 條第 3 項規定，資料控管者與受託處理者應依據風險評估措施，採取適當技術上與組織上之措施，以確保資料的安全性；以及協助資料控管者維護當事人權利；保存處理之活動紀錄等義務；符合 GDPR 第 35 條條件時應進行資料影響評估；BDSG 第 65 條規定要求受託處理者發現資料侵害事故時，應立即向資料控管者報告；BDSG 第 62 條第 3 項及第 4 項對於複委託或共同處理之管理規範。

比較特別的是，非公務機關依據 GDPR 第 37 條第 1 項之規定，應指定資料保護專員（Datenschutzbeauftragte/en）。此外，BDSG 第 38 條第 1 項規定，除上述情形外，如果資料控管者或受託處理者連續聘用至少 20 名人員，應指定資料保護專員[140]。而受託處理者在委託處理過程中，違反處理目的或方式時，則為其視為資料控管者。

---

[139] 相關規定分別為：資料安全處理的義務、向聯邦專員報告的義務、個資事件通知資料當事人的義務、進行個資保護影響評估，以及參與聽證。

[140] Bundesministerium für Bildung und Forschung [BMBF], *Handreichung Datenschutz* (2020), Aufl. 2, S. 26, https://www.forschungsdaten-bildung.de/files/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf (last visited Jan. 12, 2022).

四、美國

（一）　CCPA 及 CPRA 相關規定

1. 營利事業之控管義務

依據 CCPA 及 CPRA 第 1798.140 條第 d 項之規定，不論是否設立加州境內，在加州境內營業蒐集加州居民消費者個人資料且滿足以下任一條件的營利事業：（1）年營業總額超過 2500 萬美金；（2）每年基於商業目的購買、收受、販售或共享超過 5 萬筆消費者（consumer）、家戶（household）或裝置（devices）之個人資料；或（3）每年 50%以上之營業額來自販售加州消費者之個人資料，皆有 CCPA 之適用。而規範主體包含大型企業以及透過蒐集、共享、販售加州居民個人資料營運之企業、與營利事業共用品牌之控制企業以及被控制企業（controls or is controlled by a business that shares common branding with the business）。而依據 CCPA 及 CPRA 要求營利事業本身（1）根據第 1798.100 條第 a 項、第 1798.110 條第 c 項及第 1798.130 條第 1 項第 5 款第 B 點，應於蒐集前或蒐集時告知當事人蒐集個人資料之類型及目的，未經告知不得蒐集及作其他目的之利用；（2）根據第 1798.81.5 條第 b 項及第 1798.150 條第 a 項第 1 款應施行妥適的資安保護措施；（3）根據第 1798.140 條第 ag 項向營利事業提供服務而處理資料應受書面契約的約束等相關要求。

2. 服務提供者與承包商之遵守義務

依據 CCPA 及 CPRA 第 1798.140 條第 e 項第 5 款以及第 ag 項之規定，當營利事業委由他人為其營業目的提供服務並簽訂書面契約，且向營利事業提供服務的人或實體涉及個人資料處理及接收時，即本法規範之「服務提供者」（service provider）。而服務提供者只能在書面契約特定的營業目的下，保有、使用或揭露個人資料。CCPA 對服務提供者的要求與營利事業不同，服務提供者並無義務回應消費者請求，當事人如逕向提供服務者請求存取或刪除個人資料時，服務提供者得拒絕該請求。

CPRA 第 1798.140 條第 j 項第 1 款之規定新增「承包商」（contractor），其權利義務與服務提供者相當類似，不同之處在於承包商並非資料處理者，而是僅接受個人資料對其揭露，但承包商亦必須於 CCPA 契約中作契約性的保證。

依據 CCPA 及 CPRA 第 1798.145 條第 i 項之規定，服務提供商或承包商違反本法得加以處罰，但營利事業向服務提供商或承包商揭露個人資料時皆符合 CCPA 之規定，且並不知悉或沒有理由相信服務提供商或承包商有意違反規定，則營利事業對服務提供商或承包商的違法情事不負責任，反之亦然。

3. 書面契約之相關規範

營利事業為了營利目的，與服務提供者或承包商簽訂書面契約應符合下列要求：

（1） 依據 CCPA 及 CPRA 第 1798.140 條第 ag 項之規定，要求營利事業與服務提供者之書面契約須明文約定，服務提供者不得於契約明定為營利事業提供服務目的或法規允許之外的目的保留、使用或揭露個人資料。此外，CPRA 第 1798.140 第 ag 項第 1 款規定增訂更詳細的要求：

A. 服務提供者不得販售及分享個人資料；

B. 不得基於契約明定營利目的或法規允許之外的商業目的（commercial purpose）保留、使用或揭露個人資料；

C. 不得於營利事業及服務提供者間直接業務關係之外保留、使用或揭露個人資料；

D. 除法規允許外不得將依書面契約所接收的個人資料與自他人接收之個人資料或透過與消費者直接互動獲得之資料相結合。

（2） 對於與營利事業簽署書面契約接受個人資料揭露者，

CCPA 第 1798.140 條第 w 項要求契約內容須約定其：

A. 不得販售個人資料；

B. 不得於契約明定為營利事業提供服務目的或法規允許之外的商業目的保留、使用或揭露個人資料；

C. 不得於營利事業及簽約者間直接業務關係之外保留、使用或揭露個人資料。

（3） 而針對承包商的定義，CPRA 第 1798.140 條第 j 項第 1 款第 A、B 及 C 點規定亦詳細要求：

A. 承包商不得販售及分享個人資料；

B. 不得基於契約明定營利目的或法規允許之外的商業目的保留、使用或揭露個人資料；

C. 不得於營利事業及承包商間直接業務關係之外保留、使用或揭露個人資料；

D. 除法規允許外不得將依書面契約所接收的個人資料與自他人接收之個人資料或透過與消費者直接互動獲得之資料相結合（4）須有承包商出具其理解並將遵守規範的保證文件；

E. 須約定承包商允許營利事業以某些方式監管承包商合規性的監督條款。

而針對再委託之情形，則依據 CPRA 第 1798.140 條第（j）項第（2）款規定，如有服務提供商及承包商基於營利目的再委託他方處理個人資料，或其後有其他再委託的情形，則服務提供商及承包商應將上述情形告知營利事業，且所有委託行為應有書面契約約定遵守上述 CCPA 及 CPRA 之要求。CCPA 第 1798.192 條並禁止營利事業以任何協議或契約條款，豁免或限制 CCPA 所賦予消費者之權利。

（二）　UPDPA 相關規定

1.　資料控管者與受託處理者之概念說明

依據 UPDPA 第 2 條第（1）、（3）及（21）項之規定，單獨或與他人共同決定個人資料處理目的及手段之「控管者」（controller），並得區分為「蒐集控管者」（collecting controller）及「第三方控管者」（third-party controller），前者指直接從當事人蒐集個人資料的控管者，後者指自另一個控管者取得個人資料或匿名化資料的存取權限，並決定另外處理的目的和方式的控管者。而依 UPDPA 第 2 條第（12）項之規定，為控管者處理個人資料者則屬於「受託處理者」（processor）。

2.　受託處理者之相關義務

（1）與控管者之共通義務

依據 UPDPA 第 10 條之規定，控管者與受託處理者皆須實施維護資料隱私及安全風險的評定，並留存紀錄、定期更新，該評定須評估個人資料保留及處理的機密性和完整性及可能的風險影響、所採取減少風險的措施、以及資料處理的實踐情形符合本法規的程度。

（2）受託處理者之個別義務

依據 UPDPA 第 4 條第（b）項和第 10 條第（b）項之規定，處理者需協助控管者回應當事人要求的個人資料或存取權限、更正資料、避免於控管者要求目的外處理個人資料、施行、維護及更新第 10 條所規定的資料隱私及資安風險的評測，並為處理者依控管者的指示處理當事人的個人資料過程中，故意執行的不相容或禁止的資料行為提供補救措施。

（3）自願性共識標準

除了法條明定對控管者及處理者的義務，UPDPA 第 12 條另有規定，控管者或處理者如採行並遵守「自願性共識標準」（Voluntary

Consensus Standard），則視為遵守 UPDPA 的要求。針對該標準的內容設計，UPDPA 於第 13 條有列出一些非強制性的例示，包括（1）產業的相容性資料作業認定（2）確保當事人同意非相容性資料作業的程序和方法(3)回應當事人取得或更正個人資料請求的常用方法，包括驗證資料身分的機制（4）隱私政策的形式，用以提供當事人一致且公平政策的溝通（5）為控管者或處理者維護的個人資料提供合理安全保護的作業（6）任何其他與遵循本法案有關的政策和做法。而合格的「自願性共識標準」重點在於符合第 15 條所列的要求，包括：該標準的開發須符合第 14 條的程序，最後並須由州檢察長（Attorney General)確認該標準與其他法律合理調和，且不與 UPDPA 第 5 至 10 條（包括當事人要求複本以及更正資料的權利、 隱私政策、相容的資料處理行為、不相容的資料處理行為、禁止的資料處理行為、資料隱私及安全風險評估）相衝突並符合第 14 條的程序後，即可認可該標準。

五、日本

（一）　個人資料處理事業者及受委託人之相關概念

依日本個資法第 16 條第 2 項之規定，針對「個人資料處理事業者」(個人情報取扱事業者)係指將個人資訊資料庫等供事業利用者，但不包括國家機關、地方自治團體、獨立行政法人及地方獨立行政法人等。另《行政機關個人資料保護法》並未有委託相關規定，2021 年修法後無論公務機關或非公務機關均統一適用《個人資料保護法》，惟公務機關仍未適用委託規定之條文。而依同法第 25 條規定，受委託人(委託先)應指受個人資料處理事業者委託處理全部或一部個人資料者。

（二）　個人資料處理事業者應監督之內容

本法並未課予受委託人之相關義務，僅於第 25 條「對受委託人之監督」，規定個人資料處理事業將個人資料之處理全部或一部委託他人時，被委託處理個人資料之安全管理，應對受委託人進行必要且

適當之監督。因此法條解釋上，受託處理者仍應負安全管理措施之義務，且針對受委託人是否位於國內外，並未作不同規範。另依個人資料保護委員會於 2018 年發布之「個人資料保護法指引（通則編）」（個人情報の保護に関する法律についてのガイドライン（通則編））[141]，第 25 條所稱監督義務之必要事項可分為：

1. 選定適當之受託處理者：個人資料處理事業者須選定合適的受託處理者，選定前應先確認受託處理者的個資處理內規，並且有無隱私影響評估與至少需符合第 23 條「安全管理措施」[142]，並已採取必要且適當之措施。

2. 簽訂委託契約：個人資料處理事業必須與受託處理者簽訂契約，若有複委託情形，受託處理者亦應簽訂契約；委託契約之內容應包括處理個人資料所採取之必要且適當安全管理措施，及雙方同意之內容，並使委託方合理掌握受託方之個人資料處理情形。

3. 掌握受託處理者對於個人資料處理之情形：為掌握受託處理者處理個人資料之情形，個人資料處理事業應定期對受託處理者進行檢查及風險評估。

針對複委託之情形，受託處理者應將複委託之對象、複委託之業務內容、複委託者處理個人資料之方法等，向委託方進行事前報告及取得同意。而委託方對於複委託者仍應透過受託處理者或必要時自行定期實施檢查，確認複委託者是否已採取第 23 條安全管理措施。如複委託者再為複委託情形，則適用相同規定。綜上，如發生個資事故時，原則上係以個人資料處理事業者負責，其是否對受委託人已盡

141 〈個人情報の保護に関する法律についてのガイドライン（通則編）〉，日本個人情報保護委員會，https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/#page_top（最後瀏覽日：2021/06/12）。

142 依本法第 23 條規定，個人資料處理事業為防止其處理之個人資料洩漏、滅失或毀損，及其他為個人資料之安全管理，應採取必要且適當之措施。

必要且適當之監督，若是，則個資事故應由受委託人負責；若否，則個人資料保護委員會得依第 148 條對個人資料處理事業者進行勸告及命令，若仍未改善，則個人資料保護委員會得依第 179 條對個人資料處理事業者裁罰。

六、韓國

（一）　委託者及受託者之相關概念

依據PIPA第26條第3項第2款與第3款之規定，所謂「委託者」（위탁자）係指委託他方為個人資料處理業務之個人資料控管者，而受託處理該個人資料業者為「受託者」（수탁자）。

（二）　受託者之相關義務

韓國對於個資蒐集主體及受託處理者的要求，須遵循 PIPA 第 26 條。委託處理個人資料業務之限制臚列如下：

1. 個人資料處理者委託第三方處理個人資料業務時，其書面揭露內容應包含下列各款：

（1）　履行委託事務目的外，禁止處理個資之相關事項；

（2）　保護個人資料之技術性、管理性等適當安全維護措施；

（3）　其他依個資法施行細則[143]安全管理個人資料規定之事項。

2. 委託者應使個資當事人可隨時確認該委託業務內容及受託者[144]。

---

[143] 依據新修正之個資法施行細則第 28 條第 2 項之規定，委託第三方處理個人資料之適當安全保護措施應包含：委託的項目、複委託的內容及限制、限制蒐集的個資種類，以及監督受託者管理狀況。

[144] 委託者應於其入口網站揭示委託內容及受託者，若實務不可行，仍應至少將委託內容公告在受委託方工作場所顯眼處；若委託者為是公務機關應於公報

3. 委託者有委託宣傳或銷售等業務時，應依施行細則告知個資當事人委託業務之內容及受託者；當委託業務之內容及受託者有所變更時亦同。

4. 委託者應對受託者施以教育訓練、檢查處理狀況等方式監督受託者是否以安全方式處理個資，以避免個資當事人之個人資料有遺失、竊取、洩漏、變造及毀損等情事。

5. 受託者利用或對第三方提供之個人資料，不得逾越個人資料處理者委託之業務範圍。

6. 受託者於處理與受託業務相關之個人資料過程中，因違反 PIPA 而發生損害賠償責任時，視為個人資料處理者。

7. PIPA 第 15 條至第 25 條（個資的蒐集、處理、利用的規定及限制）、第 27 條至第 31 條（假名資料處理的規定及個資的安全管理措施）、第 33 條至第 38 條（個資當事人權利行使）及第 59 條（禁止之行為）[145]，於受託者準用。

除此之外，依據同條規定，委託者應使當事人可隨時確認該委託業務內容以及受託者為何人。若有委託情形，應以文書訂明委託之目的、禁止事項、適當安全維護措施；若涉及商品宣傳，則應履行告知義務，當被委託業務內容及受託者有變更時亦同。委託者應對受託者盡教育訓練、檢查及監督之責，以避免個人資料事故的發生。而在複委託的情形，在一般情形，只要屬合乎特定目的外用途提供第三人，嗣後該第三人發生個人資料外洩事件，原資料提供者無須與該第三人共同承擔法律責任。惟原提供者與第三人若屬委託者與受託者之

上揭露委託業務及受託方；若為非公務機關，則應於一般出版品於委託者所在地公告周知；於媒體上（期刊、報紙、公關雜誌等等）公告，每年至少揭露兩次；委託者與受託者間應簽訂服務協議並提供一份副本予當事人。

[145] 根據 PIPA 第 59 條，禁止行為包含：以虛假或其他不正手段或方式取得個人資料或得到關於處理同意之行為；洩漏業務上所知之個資或無權限卻使他人提供個資之行為；無正當權限或逾越許可權限而毀損、滅失、變更、偽造、或洩漏他人個資的情形。

關係，則受託者若發生個資事故，以致個人資料外洩，委託者亦須承擔責任。

比較特別的是，若委託者為公務機關，PIPA 施行細則規定應於公報或官方媒體揭露委託資訊並公告周知。且根據 PIPA 第 75 條第 4 項規定，違反第 26 條第 1 項未揭露委託業務之書面內容且未包含同項各款所定者，以及違反第 26 條第 2 項未揭露委託業務之內容及受託者，將課予 1 千萬以下韓圜。

（三）　針對影像處理之特殊規範

隨著科技日新月異以及數位犯罪的猖獗，PIPA 在第 25 條修訂對於影像處理設備[146]的設置及運作的特別規定，除非法令中有具體准許之情形、為犯罪預防及搜查所必要、安全及火災預防所必要、交通管制所必要、交通資料之蒐集及分析之必要，否則不論何人均不得在公開場所設置或操作影像資料處理設備。

而針對影像處理者委外的特殊規定在 PIPA 第 25 條第 8 項，影像資料處理設備的操作者得將有關設置或操作影像資料處理設備的相關事務委託第三方辦理。但於公務機關將設置或操作影像資料處理業務委託於第三方時，其程序及條件應依據 PIPA 施行細則規定。根據 PIPA 施行細則第 26 條，公務機關若將影像處理業務的設置及操作委外，應以書面形式說明以下內容，並應將委託者的資訊及聯絡方式公告：

1. 委託業務的內容
2. 複委託的限制
3. 委託業務的適當安全維護措施，包含對於影像個資的管理權限

[146] 所謂「影像處理設備」係指在特定空間設置並持續拍攝影像，或將該影像透過有線、無線網路傳送之裝置。

4. 保留及存放影像個資的指示

5. 若有個人資料事故，委託者與受託者違反契約義務的損害賠償責任分配

七、新加坡

（一）　組織與資料中介者之概念說明

依據 PDPA 第 2 條規定，處理個人資料之主體區分為組織（organisation）及資料中介機構（data intermediary），組織泛指非公務機關之自然人、法人團體以及非法人團體，無論該組織是否依據新加坡法律設立，或在境內是否設有實體營業據點；而資料中介機構係指非組織員工並為組織處理個人資料之另一組織。

（二）　資料中介者之相關義務

資料中介機構根據以書面形式證明或訂立之契約，代表另一組織為其目的處理個人資料。依據 PDPA 第 3 編至第 6 編規定（除了第 24 條保護義務及第 25 條保存限制義務），以及第 6A 編有關個資外洩通知義務（除了第 26C(3)(a)條及第 26E 條）不適用於資料中介機構，資料中介機構僅在 PDPA 規定下負擔保護義務、保存限制義務以及資料中介機構之個人資料外洩通知義務。若資料中介機構逾越組織授權範圍而利用或揭露其擁有或控制的個人資料，必須遵守 PDPA 所規定的所有保護義務[147]。

1. 保護義務及保存限制義務：資料中介機構有義務保護其擁有或控制的個人資料，以防止未經授權之存取、蒐集、使用，揭露、複製、修改或處置、遺失任何儲存個人資料之媒介或裝置等類似風險。資料中介機構應考量一切情形以確保合理且適當安全維護措施，以確保及時且有效因應資料外洩事故

147 PDPC, *GUIDE TO MANAGING DATA INTERMEDIARIES,* https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Intermediaries--2020.pdf?la=en (last visited Jan. 15, 2022).

發生。此外，當資料中介機構因委託關係結束而無權限存取個人資料時，該資料中介機構應停止保存個人資料，將個人資料退還組織、銷毀或是將個人資料匿名化。

2. 資料中介機構之個人資料外洩通知義務：當資料中介機構有理由確信發生個資外洩事故，必須立即通知組織，組織必須在接獲通知後評估該事故是否屬於應通報之情形。若資料中介機構是代表公務機關並為其目的處理個人資料，在有理由確信已發生個資外洩事故時，必須立即通知公務機關且不得無故拖延。

除此之外，組織應在契約中清楚訂立資料中介機構將代表其執行並為其目的所展開個人資料處理行為的工作範圍，並進行適當盡職調查以確保資料中介機構能夠確實遵守 PDPA 相關保護義務等規定。PDPC 為了協助組織管理資料中介機構以確保符合 PDPA 規定，透過指引說明資料中介機構管理生命週期（Data Intermediary Management Lifecycle），其內容包含：資料治理及風險評估、資料保護政策與實踐方式、定期管理與查核以及委託結束管理[148]。雖為組織委託資料中介機構處理個人資料時所應考量的重要因素，但同時也屬於中介處理者應踐行之相關要求義務。

貳、我國規定

一、個資法上委託關係之規範及概念

我國有關受託處理個人資料之規定，主要規範於個資法第 4 條、個資法施行細則第 7 條及第 8 條。而現行條文對於「委託機關」或「受託者」並無明確的法律定義，對於委託機關與受託者間之關係亦同；按法務部 103 年 4 月 11 日法律字第 10303504420 號函認為，既依個資法第 4 條規定委託法人、團體或自然人蒐集、處理或利用個人資料時，則受託者自非為個人資料蒐集之主體，有關受委託為個人

[148] *id*. at 9.

資料之蒐集、處理或利用者，並非個資法上的主體，仍以委託機關為權責歸屬機關；因此，受託者係「委託機關手足之延伸」之關係。

二、受託者視為委託機關

依據個資法第 4 條規定，受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於個資法之適用範圍內，視同委託機關。換言之，法人、團體或個人辦理公務機關或非公務機關所委託業務涉及處理個人資料，則該受託處理個人資料之法人、團體或個人，視同委託機關，並以委託機關為權責歸屬機關，並由委託機關負賠償責任。如委託機關屬於公務機關，依個資法第 28 條規定負賠償責任，並依個資法第 31 條適用國家賠償法之規定；而如委託機關屬於非公務機關，依個資法第 29 條規定負賠償責任，並依個資法第 31 條適用民法之規定（詳見法務部 87 年 9 月 29 日法律司字第 033900 號函，以及法務部 103 年 11 月 18 日法律字第 10303511950 號函等）。

三、受託者依委託機關應適用之規定

個資法施行細則第 7 條規定「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」對於適用之具體規定、適用範圍或義務主體並無詳細敘明。參照法務部 102 年 3 月 12 日法律字第 10100250980 號函見解，如委託機關依據個資法第 8 條第 1 項規定，向當事人蒐集個人資料時，負有明確告知當事人本條事項義務時，則除非有同條第 2 項免告知情形之一者，否則委託機關或受託者均有告知義務。

除此之外，參考法務部民國 103 年 6 月 25 日法律字第 10300570190 號函意見，國內從事電子商務零售業者於履約及提供售後服務過程中，如委託境外協力廠商代為蒐集、處理及利用客戶個人資料，該受託境外協力廠商即視為委託機關，即受託機關如於委託機關原合法蒐集特定目的及要件下，已得蒐集、處理及特定目的內利用個人資料，則無需再經當事人書面同意，惟應確保委託處理個人資料安全管理；另資料備份儲存於協力廠商資料維護中心，除有法定所列

得免為告知情形外，應踐行告知義務。

四、委託機關之監督義務

最後，有關委託機關對於受託者之監督義務，則規範於個資法施行細則第 8 條，同條第 1 項規定「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。」、第 2 項「前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。」、同條第 3 項「第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。」以及同條第 4 項「受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。」

參、分析與小結

一、比較法之分析

（一）　委託、委託機關與受託者之相關定義

依據我國個資法第 4 條、個資法細則第 7 條以及個資法細則第 8 條之規定，對於個資法上之「委託」、「委託機關」或「受託者」缺乏明確的概念定義。雖然依照法務部 105 年法律字第 10303504420 號函釋內容，如依個資法第 4 條規定，受委託為個人資料之蒐集、處理或利用者，仍以委託機關為權責歸屬機關，受託者係委託機關手足之延伸，而委託機關若將已蒐集之個人資料交由受託者執行業務時，受託者應協助委託機關處理或利用該個人資料。但對於何謂委託、委

託機關或受託人仍無明確之規範。

觀察比較法上其他國家在個資委託之規範定義（詳見下表），可歸納出三種定義方式，第一種係以委託目的及方式為核心，例如歐盟、英國、德國、美國及新加坡將決定個資處理目的及方式者，定義為資料控管者、營利事業體或組織，而為資料控管者處理個資者為受託處理者或資料中介者；第二種則係日本，以個人資訊資料庫等供事業利用之個人資料處理事業者為資料控管者，而受個人資料處理事業委託處理全部或一部個人資料者，為受託處理者；第三種則是韓國，以委託他方處理個資業務者為資料控管者，而受託處理者係受託處理個資業務之人。上開歐盟、英國、德國、美國、日本、韓國及新加坡之比較法規範，得作為未來我國明訂委託機關與受託人概念定義之參考。

表 19 個資法上委託關係之法律定義與適用主體

		委託人	受託人			
		定義		適用主體		
				自然人	法人	團體
我國		N/A（委託蒐集、處理、利用個資）		O	O	O
歐盟		決定個資處理目的及方式	替資料控管者處理個資	O	O	O
德國						
英國						
美國	CCPA CPRA	蒐集、決定個資處理目的及方式的營利事業	替資料控管者於營利目的內處理或接收個資	O	O	O
	UDPDA	決定個資處理目的及方式	替資料控管者處理個資	O	O	O
日本		將個人資訊資料庫等供事業利用	受個人資料處理事業委託個	O	O	X

	者	人資料之全部或部分處理者			
韓國	委託他方處理個資業務者	受託處理個資業務者	O	O	X
新加坡	決定個資處理目的及方式	代表組織並為其目的處理個資	O	O	O

資料來源：本計畫研究團隊自行整理

（二）　個資法上的責任義務

承前所述，我國現行有關委託法律關係之責任義務分配，依據個資法第 4 條規定「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」以及個資法細則第 7 條規定「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」，對於義務主體應為委託機關或受託人或二者皆是，不無疑問。特別當涉及當事人權利行使時，應以委託機關、受託人、或應同時向委託機關與受託人請求，或得擇一請求即可，亦有同樣適用上之問題。

從比較法來看，比較特別的是，除了我國之外，歐盟、英國、美國 CCPA、日本、韓國及新加坡等國家，對於個人資料委託契約要求應以書面或電子方式簽訂契約，屬於要式契約之性質而非口頭之諾成契約。此外，針對該個人資料委託契約，歐盟、英國、德國、美國 CCPA、日本、韓國及新加坡皆於個資法上明訂應清楚載明特定條款之強制要求，例如受託者採取之適當安全管理措施、權利義務分配或複委託及共同受託處理等情形。

另觀察歐盟、德國、英國、美國、日本、韓國及新加坡，針對資料控管者與受託處理者共同須遵守之義務，包括保密義務、適當安全措施之確保資訊安全義務、資料保護影響評估之做成，以及對於要求雙方負有保存義務（資料控管者應保存控管者聯絡資訊、處理目的、當事人類別及資料屬性以及技術上與組織上的安全措施等資訊；而

受託處理者應保存其處理之活動紀錄，其保存內容應包含處理者的聯絡資訊、處理的類型、傳輸接收者之適當保護書面文件，以及技術上與組織上的安全措施等資訊）。

而且另外針對受託處理者之遵守指示義務，以及複委託之事前同意要求、共同處理或更換處理者之通知義務，以及複受託處理者未履行之代履行責任，歐盟、德國、英國、美國、日本、韓國及新加坡，均明確於個資法加以規範。另外，在協助資料控管者遵守當事人權利及規範要求之義務，僅日本未加以明訂，其餘歐盟、德國、英國、美國、韓國及新加坡，均有規定。而停止利用個人資料、刪除個人資料或返還個人資料予控管者之義務，則係歐盟、德國、英國、韓國及新加坡，有相關明確之規定。

表 20 個資法上委託關係之責任義務規範

		合法處理	要式契約	遵守指示	複委託要求	保密義務	當事人權利	資訊安全	協力義務	資料保護影響評估	諮詢義務	事故通知	事故通報	返還義務	保存義務
我國		委		受	委	委/受		委＋受				受	委/受		委
歐盟		控	O	處	處	控＋處	控	控＋處	處	控、處	控	控、處	控	處	控＋處
德國															
英國															
美國	CCPA CPRA	控	O	處	處	控＋處	控	控＋處	處	控＋處		處			
	UDPDA	控		處		控＋處	控	控＋處	處	控＋處					
日本		控	O	處	處		控	控＋處		控＋處		控＋處	控＋處		控＋處
韓國		控	O	處	處	控＋處	控	控＋處	處	控＋處	控	控＋處	控＋處	處	控＋處
新加坡		控	O	處	處	控＋處	控	控＋處	處	控	控	控、處	控	處	控＋處

＋：個資法明文規範二者皆有義務
、：個資法條文個別規範

資料來源：本計畫研究團隊自行整理

（三）　個資法上的法律效果歸屬

承前述討論，若法律規範上對於責任義務之主體規範不明時，可能使效果歸屬產生同樣問題。尤其，我國現行有關委託法律關係上之效果歸屬，依據個資法第 4 條以及個資法細則第 7 條之規定，對於效果歸屬之主體應為委託機關或受託人或二者皆是，缺乏明確規定；此外，現行規範對於共同委託或複委託（再委託）之情形，亦無明確之規範。

雖然，法務部 87 年法律字第 033900 號函釋、102 年法律字第 10200018090 號函釋，以及 103 年法律字第 10303511950 號函釋，明確表示在委託機關所委託之特定目的範圍內，受委託蒐集、處理或利用範圍內所為行為，均視同委託機關之行為，責任效果應以「委託機關」作為歸屬主體。然而，觀察歐盟、德國、英國、美國、日本、韓國及新加坡等其他國家，於個資法上明確規定，如受託處理者於委託目的與方式外，所為之處理個人資料之行為，則視為資料控管者之地位，應由受託處理者為主要損害賠償的課責主體，而資料控管者之監督義務則屬於損害賠償之比例分配。

另外，在複委託之情形亦同，複受託處理者於委託目的與方式外，所為之處理個人資料之行為，則視為資料控管者之地位，即不以資料控管者作為唯一效果歸屬之主體。並且對於複委託關係有複受託處理人未為履行時，歐盟、英國、德國、美國、韓國及新加坡等個資法明文規範，應由受託處理人代為履行複受託處理人之義務，而日本係以契約約定為主。

表 21 個資法上委託關係之效果歸屬

		受託人		共同處理的情形	複委託的情形	
		指示內	違反指示		未履行	違反規定
歐盟		控管者	處理人	就左列個別處理人而定	處理人代履行	複處理人
德國						
英國						
美國	CCPA CPRA	營利事業	處理人（服務提供商及承包商）		處理人代履行	複處理人
	UDPDA	控管者	處理人			
日本		控管者	處理人		依契約約定	複處理人
韓國		控管者	處理人		處理人代履行	複處理人
新加坡		控管者	處理人		處理人代履行	處理人
我國		委託機關		委託機關	N/A	委託機關

資料來源：本計畫研究團隊自行整理

二、小結

我國個資法針對個人資料之委託蒐集、處理或利用之相關規範，相較於比較法上其他國家之規定，僅有第 4 條明定受委託蒐集、處理或利用個人資料者，於個資法之適用範圍內，視同委託機關；並以個資法細則第 7 條及第 8 條分別規定受託者之適用責任義務與委託機關之監督義務，作為規範個資法上委託關係之主要規定。然而，在進入資料、數位經濟時代後，資料利用的樣態漸趨複雜，許多資料利用樣態似乎並非單純的委託與被委託關係（例如 A 賣場欲蒐集客戶資料進行分析，以擬定行銷策略；而 B 資料統計公司希望藉由與 A 賣場合作，蒐集、處理與利用 A 賣場客戶資料訓練其所設計的精準

商品推薦應用程序或完善其資料統計軟體，則雙方對客戶資料之蒐集、處理、利用，已非單純 A 賣場委託 B 公司之關係)。歐盟為處理前述漸趨複雜的個人資料蒐集、處理、利用樣態，引入「共同控管者」概念，要求「共同決定資料處理目的或方法」的不同資料控管者，必須約定彼此對法定義務的責任安排。建議參考歐盟、德國、英國、美國、日本、韓國及新加坡等國家之個資法規定，應於我國個資法明確化委託機關、受託者與個資法上委託關係之法律概念，方得協助釐清個資法上之委託關係，並且應考量共同委託機關、共同受託者或複委託等複雜之法律關係適用。

此外，個資法細則第 7 條規定受託者依委託機關應適用之規定為之，但相較其他國家之規範，不僅明示個資法上委託契約屬於要式契約，更於個資法上明列應載明之強制條款、複委託情形以及其他應遵守之義務要求規範等。依據司法院釋字第 432 號解釋，所謂「法律明確性」原則係指法律文義苟非難以理解、受規範者所得預見，且可經由司法審查加以確認。且依據司法院釋字第 522 號及第 680 號解釋，所謂「授權明確性」係指法律授權之目的、範圍及內容須明確。其審查內容可能包含法律用語、法律概念、指示性規定內容以及法律效果等。其目的是使受規範者知悉法律禁止事項，避免有違反而受處罰風險，且同時控制國家權力行使的合理性與可預測性，以落實法治國原則及法安定性。因此，為使受規範者能夠清楚地預見其法規所課責之義務及義務違反之賠償或處罰責任，故建議有關受託者之責任義務規範，應於個資法上明文規範或以個資法細則詳列，以明確遵守相關法令所賦予之義務，並落實個人資料保護之立法要求。

最後，有關責任效果之歸屬問題，從現行個資法第 4 條及相關函釋之見解，在委託機關所委託範圍內，不論是否逾越委託機關之委託範圍，受委託蒐集、處理或利用範圍內所為行為，均視同委託機關之行為，責任效果主要以「委託機關」作為歸屬主體，而複委託之情形亦同。然而，觀察比較法上多數國家之個資法規定，多以受託處理者於委託目的與方式外處理時，即逾越資料控管者之委託或指示時，則所為之處理個人資料之行為，視為資料控管者之地位，應由受託處

理者為主要損害賠償的責任主體，複委託之情形亦同。因此，現行我國實務對於個資法上委託關係，對於委託機關之責任過苛，建議若仍就個案實際之委託內容與範圍，依責任分配法理進行適當之課責，在受託處理者明顯違反資料控管者指示、未經資料控管者之複委託，或違反資料控管者複委託之指示等情形，則應由受託處理者或複受託處理者承擔相關責任為宜。

第五節　產業應用

第一項 科學研究

壹、比較法國家

一、歐盟

（一）　科學研究之定義及適用範圍

雖然 GDPR 條文對於「科學研究」（scientific research）並未定義，但 GDPR 前言第 159 點明定科學研究應以廣義方式詮釋（interpreted in a broad manner），科技發展及成果、基礎研究、應用研究、私人贊助研究、以公共利益為目的進行的公衛研究、及以營利為目的的研究都屬科學研究，科學研究即是任何以發掘新知識為目標、以促進某領域發展為目標的活動[149]。GDPR 前言第 157 點不只限於與科學相關的研究，亦包含與人文相關的研究；但仍必須依照各專業領域的研究方法執行、符合倫理標準以及遵循最佳實務典範[150]。

此外，有關「基於建檔目的」而處理個人資料之情形，GDPR 定義為永久儲存資料，通常該資料用於歷史研究的前置作業，並於

---

[149] Rossana Ducato, *Data protection, scientific research, and the role of information*, COMPUTER LAW & SECURITY REVIEW 37, 1, at 3 (2020); EDPB, *supra* note 68, at para 9-10.

[150] Ducato, *supra* note 149, at 3; ARTICLE 29 DATA PROTECTION WORKING PARTY [WP29], *Guidelines on consent under Regulation 2016/679* (2018), https://ec.europa.eu/newsroom/article29/items/623051, at 27-28, (last visited Oct. 29, 2021).

GDPR 前言第 158 點明定，不論公務機關或私人凡基於公共利益建檔得適用本點。而在「歷史研究」部分，則依 GDPR 前言第 160 點指出歷史研究包含地理研究[151]。

（二）　科學研究之適用條件

依 GDPR 第 9 條第 2 項第 j 款規定，基於歐盟法或歐盟成員國國內法，為達到公共利益建檔目的（archiving purposes in the public interest）、科學或歷史研究目的（scientific or historical research purposes）或統計目的（statistical purposes）時，且手段與目的間符合比例原則要求，例外允許處理特種個人資料。除此之外，基於尊重資料保護之本質，處理時應依 GDPR 第 89 條第 1 項規定適合的保護措施，採取特定的、適當安全維護措施（safeguards）及資料最小化（data minimisation）原則等措施，以保護當事人的基本權利及利益。

（三）　科學研究之特殊彈性規範

為促進社會進步及鼓勵產業研究，GDPR 針對基於公益目的而建檔、科學或歷史研究、統計目的，提供特殊彈性的處理規範，其試圖在保障自然人基本權利、商業自由、以及社會對新知識的期待，這三項領域中找出適當的平衡[152]。因此，在 GDPR 架構下，如欲以科學研究目的處理資料，應採取 GDPR 第 89 條第 1 項適當保護措施前提下，方得適用下列特殊彈性，包含 GDPR 第二章資料保護原則中，有針對科學研究訂定例外條款（exceptions）；GDPR 第三章當事人權利，有針對科學研究訂定特別規範條款（derogations）[153]。

1.　承認當事人之廣泛同意

原則上依據 GDPR 第 7 條之規定，對於當事人之同意有明確之規範內容，包含明確告知蒐集之特定目的、取得明示且自主性的同意

---

[151] Ducato, *supra* note 149, at 2.
[152] Ducato, *supra* note 149, at 4-5.
[153] Ducato, *supra* note 149, at 5.

等要求；惟基於科學研究目的而處理個人資料的情形，則參照 GDPR 前言第 33 點內容，基於科學研究目的所為之個人資料處理，於資料蒐集當時不可能完整指明該處理之目的時，則在符合公認之道德標準時，應允許當事人僅就科學研究之特定範圍為同意之表示。或使當事人有機會就特定研究範圍、預期目的之部分研究計畫表示同意。

2. 推定進階處理之新舊目的相容

GDPR 為鼓勵產業進行科學研究並應用其成果，調整因科學研究目的之處理，使控管者所需遵守的資料保護原則較寬鬆，例如 GDPR 第 5 條第 1 項第 b 款規定，原則限於蒐集目的內處理個人資料，但若係基於科學研究為處理目的時，二次處理該資料推定新舊目的為相容，則有 GDPR 第 6 條第 4 項進階處理規定之適用。舉例而言，當事人去醫院檢查是否確診新冠肺炎，之後其健康資料被利用於疫苗相關的科學研究，仍屬於進階處理之合法範圍[154]，其目的是促進合法取得之研究資料方便再利用，放寬法律要求[155]。但仍應注意新舊目的相容性檢查項目，應考量包含舊目的與新目的之連結、蒐集時的脈絡、個資的性質、新目的處理之可能後果及安全保護措施之落實。

3. 放寬儲存期間之限制

依據 GDPR 第 5 條第 1 項第 e 款規定，原則當資料蒐集目的消失時，資料控管者所儲存之資料應銷毀，方符合限制儲存原則（storage limitation）之要求；惟若基於科學研究目的而處理個人資料時，即使無繼續儲存資料之必要，仍允許延長個人資料之儲存時間。這項例外條款對科學研究甚為重要，因為研究案結束後雖當初蒐集個人資料之研究目的消失，但為了確認研究成果仍有可能未來再進行相關處理行為[156]。不過，歐洲資料保護監督機關（European Data Protection Supervisor, EDPS）於 2020 年「關於資料保護與科學研究

154 EDPB, supra note 149, at para 13.
155 Ducato, *supra* note 149, at 5.
156 Ducato, *supra* note 149, at 5.

之初步意見」中表示，GDPR 第 5 條第 1 項第 e 款所訂定的例外條款，僅允許資料儲存較長的時間並非永久保留[157]。

4. 採取適當保護措施即得處理特種個人資料

承前所述，GDPR 第 9 條第 1 項規定原則禁止特種個人資料之處理，但 GDPR 第 9 條第 2 項第 j 款與第 89 條第 1 項規定例外情形，即基於科學研究目的，得允許控管者在採取適當保護措施後處理特種個人資料。

5. 適當限制當事人權利之行使

為使資料控管者得有效地基於科學研究目的而處理個人資料，針對當事人之權利予以限制，包含 GDPR 第 14 條被告知權（right to be informed）、第 17 條刪除權，以及第 89 條第 2 項允許歐盟成員國自立國內法針對當事人之近用權、更正權、限制處理權、拒絕權另行規定。

二、英國

英國有關科學研究採廣義之定義，規範於 UK GDPR 前言第 157 點、第 158 點與第 159 點，可包含科技發展及成果、基礎研究、應用研究、私人贊助研究、以公共利益為目的進行的公衛研究、及以營利為目的的研究，與 GDPR 之規範內容相同。除此之外，針對基於公共利益之建檔目的、科學或歷史研究目的或統計目的，而處理個人資料之適用條件與放寬限制等規定，依據 UK GDPR 第 9 條第 2 項第 j 款、UK GDPR 第 5 條第 1 項第 b 款、第 14 條第 5 項第 b 款、第 89 條第 1 項、第 6 條第 4 項，以及 UK GDPR 前言第 33 點與第 39 點等規定，與歐盟 GDPR 內容相同。

---

[157] Ducato, *supra* note 149, at 5 (2020); European Data Protection Supervisor [EDPS], A *Preliminary Opinion on data protection and scientific research* (2020), https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf, at 23, (last visited Oct. 29, 2021).

比較特別的是，DPA 第 19 條第 3 項有規定相關限制，「針對特定當事人的措施或決策之處理，不符合 GDPR 第 89 條第 1 項之要求。但處理目的為必要（包含經批准之醫學研究目的），不受此限。」而所謂「經核准的醫學研究」，依 DPA 第 19 條第 1 項及第 4 項之規定，係指由衛生研究機構（Health Research Authority）依據《護理法》（Care Act 2014）第 2 章第 3 部分認可或設立之研究倫理委員會；或由國務大臣、蘇格蘭部長、威爾士部長或北愛爾蘭部門；國民保健署（National Health Service，簡稱 NHS）相關機構[158]；英國研究與創新機構或依科學技術法（Science and Technology Act 1965）目的設立之研究委員會；依《所得稅（收入和養老金）法》（Income Tax (Earnings and Pensions) Act 2003）第 4A 章第 7 部分之研究機構。在上述機構核准，同意醫學研究之處理目的，即使未遵守 DPA 第 19 條 3 項前段之限制，亦得例外處理個人資料。

三、德國

（一）　科學研究之定義及特殊規定

BDSG 針對「科學研究」並無具體規範說明，但根據德國聯邦教育及研究部（Bundesministerium für Bildung und Forschung, BMBF）委託研究並於 2020 年 6 月發布第 2 版之「資料保護手冊指南」（Handreichung Datenschutz）文件，係指社會科學、行為科學及經濟科學領域，實證研究時所涉及的相關個人資料[159]。其中應注意的是，依據 BDSG 第 2 條針對公務機關及非公務機關之規範定義，凡涉及

---

[158] NHS 機構是指英格蘭的 NHS 信託或 NHS 基金會信託；威爾士的 NHS 信託或地方衛生委員會；根據《國家衛生服務（蘇格蘭）法》（National Health Service (Scotland) Act 1978）第 2 條組成之衛生委員會或特殊衛生委員會；蘇格蘭衛生服務公共服務機構，或《健康和社會關懷（改革）法》（Health and Social Care (Reform) Act (Northern Ireland) 2009）第 1 條第 5 項第 a 至 e 款之北愛爾蘭健康和社會保健機構。

[159] Rat für Sozial- und Wirtschaftsdaten (RatSWD), Handreichung Datenschutz (2020), Aufl. 2, Berlin, S.7, https://www.konsortswd.de/wp-content/uploads/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf (last visited Oct. 29, 2021).

依法組成之公法組織、基金及協會，或受國家高權監督之行政部門、機構或協會，皆屬於 BDSG 所訂「公務機關」之概念範圍。由於大學屬於依法令設立實施教育之機構，而科學研究機構如係受行政機關委託執行相關研究計畫，屬於執行國家公共任務時，則多數情形應適用 BDSG「公務機關」合法處理之相關規定。

而德國針對基於公共利益之建檔目的、科學或歷史研究目的或統計目的，而處理個人資料之適用條件規定，與歐盟 GDPR 內容相同。但比較特別的是，依據 BDSG 第 1 條第 2 項之規定，如其他聯邦法律另有規定，例如「藥事法[160]」（Arzneimittelgesetz, AMG）、「基因診斷法[161]」（Gendiagnostikgesetz, GenDG）及「移植法[162]」（Transplantationsgesetz, TPG）等規定者，已針對研究部分另有規定，則優先於 BDSG 適用。

（二）　科學研究之特殊放寬規定

針對基於公共利益之建檔目的、科學或歷史研究目的或統計目的，而處理個人資料之放寬限制，原則上與 GDPR 規定大抵相同。但適當安全措施部分，有二點值得說明：其一，依據 BDSG 第 27 條第 3 項規定基於科學目的、歷史目的或研究目的（並不包含統計目的者），除上開適當及具體措施外，應將個人資料匿名化，但存在當事人正當利益衝突時，則不在此限。在個人資料匿名化前，有關人別或事物關係而特定或可得特定當事人（BDSG 第 3 條）的詳細內容（Einzelangabe），其標記（Merkmale）應該被分開儲存，只有其符合研究目的或統計目的要求時，才允許將標記有關之詳細內容加以彙整之。其二，另外，依據 BDSG 第 50 條規定，不論建檔、科學或統計等形式目的範圍內，如果涉及公共利益且規劃合於當事人正當利

[160] 全稱為：藥品銷售法（Gesetz über den Verkehr mit Arzneimitteln）。

[161] 全稱為：人類基因診斷法律（Gesetz über genetische Untersuchungen bei Menschen）。

[162] 全稱為：器官及組織之捐贈、切除及移植法律（Gesetz über die Spende, Entnahme und Übertragung von Organen und Geweben）。

益之保障，則允許處理個人資料。但此種保障建議儘可能採行，像是使用匿名化之資料、採取針對未經授權第三人的預防措施，或空間上及組織上單獨專門地分開處理等為宜。

而在「進階處理」的彈性規定，則依據 GDPR 第 9 條第 2 項例外合法處理特殊種類個人資料，開放由歐盟法或成員國法律訂定及補充規定；對此，德國社會法法典（Sozialgesetzbuch, SGB）第 10 編社會行政程序與社會資料保護，依 SGB X 第 67b 條第 3 項規定，出於研究目的（Forschungszwecke）者得針對特定研究項目或科學研究領域，取得資料當事人的廣泛同意，以補充 GDPR 第 9 條第 2 項第 a 款之規定。不過，若係非直接從資料當事人蒐集之個人資料，則依據 SGB X 第 67a 條第 2 項規定，應衡量資料當事人正當利益是否受到損害。

另外，在「公開個人資料」的部分，依據 BDSG 第 27 條第 4 項之規定，只有在當事人同意下，或為呈現時代「歷史事件」的研究成果所不可或缺時，則資料控管者得公開之。其考量是基於科學研究、歷史研究或統計目的處理個人資料，往往容易在資料分析及研究成果之中，透過資料庫或期刊發表的方式，將涉及個人資料的研究成果予以公布（公開），只要資料能夠特定或可得特定當事人，特別是質化研究容易連結到當事人的特徵，其一經公布則不特定多數人得以公開閱覽，對於資料當事人將產生重大且不可逆的影響；因此限於上述二種情形時，始得公開當事人個人資料。

四、美國

（一）　HIPAA 之相關規定

美國 HIPAA 對於特種個人資料，除取得個人授權同意、事先告知並給予選擇同意與否機會，或符合 HIPAA 所定無須取得個人同意的情形，否則不得利用與揭露之。不過，在 HIPAA「個人可辨識健

康資料隱私規則[163]」（Standard for Privacy of Individually Identifiable Health Information，下稱「隱私規則」）規定內，依據聯邦法規第164.501 條規定，所謂「研究」（research）旨在為開發或有助於知識普及之系統性調查，包含研究開發、測試與評估。但依據聯邦法規第164.512 條第 i 項之規定，以研究用途為目的者，須經過研究倫理審查委員會（Institutional Review Board, IRB）之審查，或是其他相類似之隱私委員會（privacy board）之同意的情形時，例外得無須得當事人同意而為資料之使用。同時，受規範機關（構）仍須落實「電子保護健康資料之安全標準規則[164]」（Security Standards for the Protection of Electronic Protected Health Information）規定，有關第 164.308 條管理安全措施（administrative safeguards）、第 164.310 條物理上保護措施（physical safeguards）與第 164.312 條技術上保護措施（technical safeguards）等相關規定。

（二）　CCPA 之相關規定

依據 CCPA 第 1798.140 條第 ab 項之規定，所謂「研究」係指目的是在發展或促進公共或科學知識之科學分析、系統研究與觀察（包含基礎研究與應用研究），並遵守或以其他方式符合所有相關適用的道德與隱私法律，包含但不限於在公共衛生領域為公共利益所進行之研究。然而，透過企業服務或設備所蒐集消費者個人資料進行之研究，應符合下列 8 項要件：

1. 與蒐集個人資料的商業目的相符；
2. 隨後進行假名化、去識別化或匯總化，使企業不能合理識別、涉及、描述、直接或間接關聯特定消費者；
3. 受技術保護措施的規範，除研究必要外，禁止重新識別資料

[163] Privacy of Individually Identifiable Health Information, 45 C.F.R §§164.500-164.534 (2013).

[164] Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. §§164.302-164.318 (2013).

可能涉及的消費者；

4. 受業務流程禁止重新識別資料的規範，除非研究所必要；

5. 受業務流程規範，防止無意洩漏被識別資料；

6. 防止任何重新識別的企圖；

7. 僅用於蒐集個人資料背景相關之研究目的；

8. 由進行研究之企業為額外之安全控制，限制對研究資料的存取，僅執行研究目的必要之人才能存取資料。

另外，依 CCPA 第 1798.145 條第 c 項之規定，CCPA 相關規定排除適用《醫療資料保密法》（the Confidentiality of Medical Information Act）與 HIPAA 之資料，即該等資料應特別適用前述法律，而無 CCPA 之適用。同時該條也排除臨床試驗或其他生物醫學研究所蒐集的個人資料，但該等資料須符合「美國聯邦人體保護政策」（the Federal Policy for the Protection of Human Subjects）、國際醫藥法規協會（International Council for Harmonisation）發布良好臨床實踐指南或美國食品與藥物管理局（Food and Drug Administration, FDA）的人體保護要求，但不得以本項不允許的方式出售或分享這些資料，如果有不一致之處，應告知參與者用途並取得同意。

（三）　UPDPA 之相關規定

一般而言，依據 UPDPA 第 7 條第 b 項相容性資料作業規定，該資料之處理符合當事人期望或有利於當事人，在研究上常適用之要件包含：（1）對建立假名化資料或去識別化資料是合理必要的；（2）允許基於產品或服務的研究與開發進行一般研究（generalized research）[165]之分析，所謂「一般研究」係指利用個人資料發現與公共衛生、公共政策或其他一般公共利益有關的事項，不包含利用個人

資料對特定的當事人進行預測或決定；或（3）其他可確定為相容性資料作業之目的。在符合上開相容性資料作業，控管者或處理者可以在不經當事人同意進行相關個人資料之處理。除此之外，依據 UPDPA 第 9 條第（a）項第（4）款規定，倘未能落實合理的資料安全措施，包含管理上、技術上與物理上保護措施，則可能會被認定構成禁止性資料作業處理，而禁止為相關資料處理。同時，依據 UPDPA 第 10 條第（a）項之規定，資料控管者應落實資料隱私與安全風險評估。不過，有關人體受試研究者資料之處理或保存，依據 UPDPA 第 3 條第（c）項之規定，無本法之適用。

五、日本

（一）　學術研究之定義及適用對象

日本舊的個資法在立法時，基於學術研究自由為憲法保障之基本權，原則上由研究團體自律，避免公權力之介入，故於個資法第 76 條第 1 項第 3 款及第 3 項規定，大學及其他以學術研究為目的之機關或團體，或屬於上開大學等之人員，為供學術研究之目的者，不受個資法之限制；而應由各該大學或機關訂立個資之蒐集處理規範[166]。

惟新修正之個資法有關學術研究一律除外適用之規定，修正為根據情況適用除外規定。根據此次修正，第 16 條第 8 項對於本章所稱「學術研究機關等」，係指大學及其他以學術研究為目的之機關或團體，或所屬人員。所謂「大學及其他以學術研究爲目的之機關或團體」是指私立大學、公益法人等研究所以學術研究爲主要目的活動的機關或「學會」，所謂「所屬人員」係指私立大學的教職人員、公益

[166] 鑑於大學自治等學術研究機關的自主性，原則上有必要尊重學術研究機關的自主性判斷。為此，學術研究機關等為利用個人資料進行研究，單獨或共同制定或公佈適當實施的自主規範時，該自主規範的內容應從保護個人權利利益的觀點出發，其處理符合相關自主規範時，個人資料保護委員會根據新法第 149 條第 1 項對此將予以尊重。但其按照自主規範處理個人資料，仍應限於未侵害當事人權利利益風險之情形，原則上個人資料保護委員會依新法第 148 條第 1 項仍得行使其監督權限。

法人等研究所的研究人員、學會會員等。再者，民間團體附屬的研究機關等的研究活動，在該機關以學術研究爲主要目的之情形，也該當於「學術研究機關等」。另一方面，當機關單純以產品開發爲目的時，不該當於「以學術研究爲目的之機關或團體」，但在產品開發及學術研究之目的併存時，應根據主要目的進行判斷。

（二）　學術研究之相關放寬規定

新法修正有關學術研究機關等基於學術研究目的處理個人資料，有個資法之適用，但可就下列特定情形，適用放寬變更目的、取用特種個人資料與提供予第三人之限制，以下分別說明之：

1. 放寬變更利用目的之限制

依日本個資法第 18 條第 3 項第 5 款之規定，當學術研究機關基於學術研究目的有處理個人資料之必要，且未有不當侵害個人權利利益之風險時；復同項第 6 款個人資料處理事業者向學術研究機關等提供個人資料，並且該學術研究機關等基於學術研究目的有處理該個人資料之必要時（包括處理該個人資料的一部分目的爲學術研究目的時，但可能侵害個人權利利益的情況則除外），不受本法第 18 條第 1 項及第 2 項有關限制利用目的之規定，即事前未經當事人同意，得超出原利用目的之範圍處理個人資料。

2. 鬆綁取得敏感性個人資料之限制

依日本個資法第 20 條第 2 項第 5 款之規定，當學術研究機關等基於學術研究目的有處理敏感性個人資料之必要時，且未有不當侵害個人權利利益風險時，該學術研究機關得不經當事人同意，取得敏感性個人資料。復同項第 6 款規定，當個人資料處理事業者基於學術研究目的從與該個人資料處理事業者共同進行學術研究的學術研究機關等取得該敏感性個人資料的情形（包括取得該敏感性個人資料之目的中一部分係為學術研究目的之情形，惟應排除具有不當侵害個人權利利益風險之情形），事先無需取得當事人同意，即可取得

敏感性個人資料。

3. 取消個人資料提供予第三者之限制

依日本個資法第 27 條第 1 項第 5 款之規定，學術研究機關等因學術研究成果的公佈或教授之必要提供個人資料而不得已時（個人權利利益可能受到不當侵害的情形除外），得不經當事人同意，向第三方提供個人資料。復同項第 6 款規定，學術研究機關等基於學術研究目的，提供個人資料予該學術研究機關等共同進行學術研究的第三者（不論是否為學術研究機關等）的情形（包括提供該個人資料的一部分目的爲學術研究目的，惟應排除可能不當侵害個人權利利益之情形），得不經當事人同意，向第三者提供個人資料。又同項第 7 款規定，學術研究機關等自第三者接收個人資料的情形，當該學術研究機關等基於學術研究目的有處理該個人資料之必要時，得不經當事人同意向第三者提供。

（三）　學術研究機關等應遵守之義務

依日本個資法第 59 條之規定，學術研究機關等以學術研究目的處理個人資料的情形，關於該個人資料的處理，在遵守該法律的同時，仍應承擔相關義務如安全管理措施、申訴處理等、爲了確保個人資料適當處理自行採取必要措施，且致力於公布該措施的內容。在個人資料之利用、取得及提供方面仍應符合第 17 條利用目的之特定、第 19 條禁止不當利用、第 20 條第 1 項適當取得、第 21 條利用目的之通知以及第 22 條確保資料內容正確性之規定，學術研究機關等與其他個人資料處理事業者適用相同之規範。

另外，個人資料的安全管理措施相關規範（第 23 條至第 26 條）、保有個人資料的揭露與更正等及停止利用等請求相關規範（第 33 條至第 40 條）、假名加工資料處理事業者等之義務（第 4 章第 3 節）、匿名加工資料處理事業者等之義務（第 4 章第 4 節）以及民間團體促進個人資料保護的規定（第 4 章第 5 節），學術研究機關與其他個人資料處理事業者適用相同之規範。

六、韓國

（一）　科學研究之背景與定義

韓國 PIPA 於 2020 年修法時參考歐盟 GDPR 引進「假名化」的概念，使個人資料處理者在兼顧資料商業運用與維護個人資料自主性的前提下，允許其得利用個人資料進行統計編製、科學研究或保存公益紀錄等特殊目的，促進資料於產業上的應用，為韓國數位發展及資料共享提供良好的發展環境，尤其是放寬無須個資當事人同意之假名資料，開放運用在科學研究領域，將有助推進新技術及科學研究的發展，進而推動韓國政府政策，發展物聯網、人工智慧與雲端等新興產業科技。

依據 PIPA 在第 2 條第 8 款之規定，所謂「科學研究」（과학적 연구）係指技術的開發與實證、基礎研究、應用研究及民間投資研究等使用科學方法的研究。

（二）　科學研究之適用條件與限制

為促進資料的運用及分析，PIPA 第 28 條之 2 規定，例外放寬無須取得資料當事人的同意，得將該資料充分運用於統計編製、科學研究及保存公益紀錄等領域，增訂得透過總統指定的專門機關將假名資料予以連結；但若欲對第三方提供時，應注意不得包含可識別特定個人的資料，若在處理過程中產生可識別特定個人的資料亦應立即停止並銷毀。除此之外，同法第 28 條之 3 特別規定假名資料的適用限制：

1. 為了結合不同個資處理者基於統計編製、科學研究及保存公益紀錄等目的處理的假名資料，應由保護委員會或相關中央行政機關首長指定之專門機關執行。

2. 個資處理者欲將該資料對外輸出，應以假名方式或依第 58 條之 2 以合理之時間、費用、技術也無法識別個資的方法處理資料後，取得專門機關負責人的核准方可為之。

3. 專門機關的指定與取消指定之標準、程序、管理、監督，與輸出暨批准基準、程序等必要事項，須依施行令定之[167]。

如欲連結不同個人資料處理者因統計編製、學術研究、保存公益紀錄等特定使用目的下所處理之假名資料，應由政府指定之專門機關來執行，且須事先經過專門機關的負責人核准後，該連結資料始得對外輸出。而有關假名資料的適當安全管理措施的要求，應符合 PIPA 第 28 條之 4 至第 28 條之 6 之相關規範要求[168]。

七、新加坡

（一）　產業應用之相關合法事由

根據 PDPA 第 13 條規定，組織在未經個人同意或視為同意（deemed consent）之情況下，原則上禁止蒐集、處理或揭露個人資料，除非符合下列事由之一者，方得蒐集、處理或揭露個人資料：

1. 基於促進業務改進之目的

組織可能利用現有客戶個資進行數據分析及市場研究，以利於開展業務活動前，獲得市場先機之洞察力並了解其現有客戶。這些是為行銷目的所進行之準備行為，而非直接向個人發送行銷資訊，因此為了促進商業發展訂有提供未經同意利用或揭露個資之例外規定[169]。依據 PDPA 附件一第五編及附件二第二編第二部分規定「促進業務改進之目的」，若不以單獨識別個人之形式利用所蒐集個資，將無法合理實現以下目的之一，且確保於一般通常智識之人認為是適當情況下，允許組織得未經同意下蒐集個資：

---

[167] PIPA 第 28 條之 3 所指的專門機構規定在韓國個人資料保護施行令（Enforcement Decree）於第 29 條之 2。如機構有至少三名具備處理假名化技術相當經驗之全職人員、相關機器設備、適當安全政策、達一定財務資本及近三年未有 PIPA 第 66 條所列之重大違法事由。

[168] 詳見第二項假名化及匿名化之內容說明。

[169] PDPC, *supra* note 58, at 69.

（1） 改善或加強所提供之商品或服務，或開發新的商品或服務；

（2） 改善或發展新興商業模式；

（3） 瞭解客戶喜好；

（4） 客製化商品或服務所必要之目的。

2. 基於研究、歷史或統計研究目的

若組織為了進行更廣泛之研發活動，但這些研發可能不會立即應用於其產品、服務、業務營運或市場銷售。可適用的對象包括：科學技術研發之企業實驗室、藝術及社會科學研究之高等教育機構，以及進行市場分析之研究組織[170]。依據 PDPA 附件二第三部分規定，將個資用於「研究目的」（包括歷史或統計研究），在符合以下所有情況，得未經同意利用或揭露個資，以最大程度地提高企業研究利益並減少蒐集及利用個資的風險：

（1）不以單獨識別個人之形式利用個資，將無法合理實現研究目的；

（2）組織徵求個人同意揭露其個資為不切實際（impracticable）的作法：徵求個人同意將導致額外成本或嚴重延宕研發時程而致研究不可行之程度，評估「不切實際」之因素例如：沒有固定數量的受試者、徵求同意將影響研究有效性等。

（3）將個資用於研究目的有明顯之公共利益；

（4）研究結果將不會用於做出任何影響個人之決定；

---

170 PDPC, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*, at 8-10, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (last visited Nov.7,2021).

（5）該組織以無法識別個人之形式公布結果。

3. 視為同意而利用或揭露個人資料

若組織欲超出原始蒐集目的進行次要目的（relevant purposes）之利用或揭露個人資料，又無法適用法定例外規定（例如促進業務改進之目的或研究目的），依據 PDPA 第 15 條及第 15A 條，規定三種不同視為同意之形式：一是透過行為視為同意；二為依據契約需求視為同意；三則是以告知方式視為同意[171]。但組織必須在蒐集、利用或揭露個資前，符合 PDPA 第 15A 條第 4 項第 a 款規定，進行評估以消除或減輕不利影響[172]。以及符合 PDPA 第 15A 條第 4 項第 b 款之規定，組織必須充分告知個人注意以下事項：組織蒐集、利用或揭露個資之用途；該蒐集、利用或揭露個資之目的；提供個人選擇退出之合理期間及方式[173]。

（二） 資料共享政策之特殊規定

為因應國家政策與產業需求，PDPC 依據 PDPA 第 62 條所賦予之豁免權（exemption），允許個人或組織可在遵循 PDPC 所制定之指南[174]，協助企業、組織遵守 PDPA 的同時，提供組織內部與組織間之個資共用，進行組織內部及組織之間的資料共享（Data Sharing）。

1. 資料共享之適用條件

資料共享是指組織向一個以上的組織利用或揭露個資，可分為

---

171 *id*, at 42-50.

172 所謂「不利影響」是指對於個人任何身體傷害、騷擾、嚴重恐慌或痛苦。

173 組織必須為個人提供合理的選擇退出期間，在期間屆滿後才符合視為同意之要件；選擇退出期間之考慮因素包括：與個人互動之方式及頻率、使用管道是否直接與個人接觸（例如：透過電子郵件提供退出之網路連結）等，當選擇退出期間屆滿，個人仍可撤回同意。

174 PDPC, *Guide To Data Sharing*, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf (last visited Nov.7,2021).

在同一組織內或關係組織間共享：共享包含向一或多組織為利用、揭露或後續蒐集個資；與資料中介機構共享（依契約約定資料留存與保護義務）：在組織內共享個人已同意利用之個資，組織還應制定內部政策，防止濫用，並避免未經授權的處理、利用與揭露；與一個或多個組織共享（在不同私部門間、公私部門間）：還應考慮共享的預期目的，以及共享可能產生的潛在利益與風險。若組織在未經同意的情況下共享個資，必須確保符合 PDPA 的相關例外或豁免之規定。

（1）同一組織內或關係組織間共用

組織可以出於個人已同意或被視為已同意的目的，在組織內共享個資。例如：組織的客戶關係部門可能會與其財務部門共享個資，以管理客戶交易業務。組織應制定內部政策以防止個資濫用，例如：設定存取限制以防止未經授權的存取、利用及揭露。組織應考量資料共享的預期目的，以及共享可能給個人帶來的潛在利益及風險。若組織預計在未經同意的情況下共享個資，則必須確保符合 PDPA 相關例外規定，例如：在任何調查或訴訟必要情況下，允許未經同意揭露個資。

（2）與資料仲介機構共用

組織可以與其資料仲介機構共享個資，以代表其處理個資。組織應與資料仲介機構簽訂書面契約，要求資料仲介機構根據組織的指示處理個資。為了簡化業務委託決策，組織無需向個人徵求明確同意向其資料仲介機構揭露個資。然而，未經個人同意資料仲介機構不得將個資用於其他目的。根據書面契約代表組織處理個資的資料仲介機構，僅受到 PDPA 有關保護及保存個資之相關規定所拘束，而委託資料仲介機構的組織，對於資料仲介機構代表其處理的個資，在 PDPA 的規範下仍具有處理個資之所有義務。

（3）與一個或多個組織共用

在決定是否與其他組織共享個資時，該組織應考慮共享的預期

目的以及共享可能給個人帶來的潛在利益和風險。主要考慮因素例如：共享目的、是否適當、共享個資之類型、與預期目的相關性、於預期目的下，匿名資料具備個資替代性、共享是否需要獲得同意、是否有例外、如無須同意，是否需要通知共享目的、以及共享是否涉及跨境傳輸等。

2. 資料共享安排機制

在 PDPA 的要求下，組織通常應徵求同意或適用 PDPA 例外規定，在未經同意的情況下才可共享數據。然而，在某些情況下，數據共享不太可能對個人產生任何不利影響，或者所需保護之正當利益及公共利益（或其一部分），大於對於個人任何不利影響。為了因應此類資料共享需求，PDPC 依照個案給予組織免除 PDPA 部分規範，由 PDPC 於 2018 年設立的沙盒計畫：「資料共享安排」機制（Data Sharing Arrangements，下稱 DSA），如組織所進行的共用模式是在特定群體並範圍具體明確，同時不會造成個人有負面影響等情事，可在不須經個人同意下進行資料共用。組織只要遵循法律、達到一定資料技術應用品質與實施資安與個資保護措施下，向 PDPC 申請通過即可進行 DSA 之個人與商業資料之共用，申請標準如下：

（1）首先，根據 DSA 進行共享的個資，必須在指定時段內與指定的組織進行共享，若需要再另外增加其他組織則必須再次向 PDPC 提出申請。

（2）其次，DSA 所共享的個資必須用於明確且具體的特定目的。例如：為了社會研究目的而在 DSA 共享個資，將可能認定為範圍過於廣泛。

（3）第三，DSA 不得對個人產生任何不利影響，或者基於正當利益，對公共利益（或其一部分）大於對於個人的任何可預見不利影響：

A. 告知及選擇退出機制：共享目的不太可能對個人產生

任何不利影響，或是共享不是為了行銷之目的。

B. 正當利益：為該目的徵求同意是不適當的，或是公共利益（或其一部分），大於對於個人任何不利影響

在 DSA 運作下，組織將被要求進行資料保護影響評估，以評估資料共享的預期風險及對個人的影響，並實施必要措施來減輕及解決這些風險。根據具體情況，可能會施加以下條款及條件：

（1）將資料共享的目的告知個人，並在資料共享之前提供合理選擇退出期間；

（2）在任何期間提出選擇退出的請求，或撤回同意均為有效；

（3）透過資料保護政策揭露並說明所依據的正當利益。

八、菲律賓

依據 DPA 2012 第 4 條第 d 款之規定，基於新聞、藝術、文學或研究目的而處理個人資料，並不適用本法之規定。而所謂「研究」（Research）依照菲律賓的個資專責獨立機關 NPC 隱私政策辦公室於 2021 年 7 月發布之「2021-023 號諮詢意見」，係指為發展或促進可歸納的知識（包含理論、原則、關係）所進行的活動，或使用科學方法觀察、推理、分析和累積任何資訊的活動[175]。

另外，依據 DPA 第 19 條與 IRRDPA 第 37 條之規定，研究包含科學研究（scientific research）與統計研究（statistical research），但不限於此，凡為追求公共利益且符合特定法規與專業道德倫理規則，皆屬於研究涵蓋範圍。然而，由於以研究為目的而處理個人資料之行為，可直接排除 DPA 的適用；因此，依據 IRRDPA 第 49 條第 e 款之規定，須要經過 NPC 審查始有本條之適用。

---

[175] NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2021-023 2-3, July 5, 2021, https://www.privacy.gov.ph/wp-content/uploads/2021/07/Redacted-Advisory-Opinion-No.-2021-023.pdf (last visited Nov. 4, 2021).

貳、我國規定

我國有關學術研究之相關條文，主要規定於合法事由之中，因科學研究而蒐集、處理及利用個人資料之規定，包含個資法第 6 條第 1 項第 4 款「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」、第 16 條第 5 款「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」、第 19 條第 1 項第 4 款「學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」以及第 20 條第 1 項第 5 款「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」

就個人資料的性質、蒐集、處理及利用之目的，以及合法事由之構成要件，可區分為下列表格內容，但有關「保護措施」之相關討論，詳見第二項假名化及匿名化之討論，以及有關「彈性規定」涉及當事人權利限制的部分，則詳見第六節當事人權利之第三項權利限制規定說明內容。

表 22 我國個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之整理

合法要件	**一般個資**		**特種個資**
	目的內	**目的外**	
適用主體	學術研究機構	公務機關或學術研究機構	
合法事由	基於公共利益為統計或學術研究而有必要		基於醫療、衛生或犯罪預防之目的，而為統計或學術研究有必要
保護措施	資料經提供者處理後/經蒐集者依其揭露方式無從識別特定之當事人		

彈性規定	間接蒐集得免為處理或利用前之告知義務

資料來源：本計畫研究團隊自行整理

參、分析與小結

一、比較法之分析

（一）　有關學術研究條款之相關定義討論

我國個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之規定，主要以「學術研究」作為條文用語；然而，綜觀各國個資法上之規定，並不僅以學術領域之研究，始得作為個資法上合法運用之事由。主要可分為三類：「研究」、「科學研究」及「學術研究」之規範用語。規定「研究」之國家，包含美國、新加坡及菲律賓；而歐盟、英國、德國及韓國則以「科學研究」作為個資法規範規定；而我國及日本則係以「學術研究」作為條文用語。

而上述三種個資法上用語是否存在差異，須進一步探究研究、科學研究及學術研究之實質上內容而定。參照法務部 104 年 7 月 2 日法律字第 10403508020 號函釋，所謂「學術研究」，係指針對有系統而較專門之學問中的特定主題，作深入且有系統的探討或研查，以發現事實，形成理論並付諸應用；因均屬抽象之法律概念，故尚難遽定其範圍及認定標準，仍宜依具體個案分別認定之。而司法院釋字第 380 號解釋協同意見書，借用學術自由之論述過程，對於研究與學術研究有較深入之討論，特別是憲法第 11 條對於學術自由之制度性保障，內容包含研究自由、講學自由及學習自由等事項，其中「研究」包含研究動機之形成，計畫之提出，研究人員之組成，預算之籌措分配，研究成果之發表等事項；而「科學研究」則係包含自然科學與社會科學領域之研究事項；最後，有關「學術研究」係者使學者能夠獲

得充分研究為主要內涵[176]。顯見，就三者概念比較上研究指涉的內涵大於科學研究及學術研究，而科學研究適用範圍又比學術研究內涵廣泛。

除此之外，歐盟體系的國家在 GDPR 前言第 159 點之「科學研究」係指包含科技發展及成果展示、基礎理論研究、應用研究及私人贊助研究等，但須依照各專業領域的研究方法執行、符合倫理標準等要求。且美國 CCPA 亦強調「研究」之目的在發展及促進公共或科學知識之科學分析、系統研究與觀察，並應遵守所有相關適用的道德與隱私法律。二者對於相關概念皆有要求應遵守一定研究方法、研究倫理標準等規範，方屬於個資法上之科學研究或研究之適用範圍。

（二）　因學術研究條款而蒐集、處理或利用個資合法要件之探討

依據我國個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之規定，非公務機關就一般個人資料之特定目的內蒐集或處理限於「學術研究機構」，而非公務機關或公務機關就一般個人資料之特定目的外，以及特種個人資料之蒐集、處理或利用，則限於「公務機關或學術研究機構」，始得為之。從我國個資法規定，其適用主體與前述「學術研究」有互為重要關聯，將研究之合法要件與「學術研究」之概念聯繫，使適用主體限於學術研究單位。但比較其他國家個資法有關研究或科學研究之適用主體規定，歐盟、英國、德國、美國、韓國、新加坡等國家，均未限定研究或科學研究須限於公務機關或學術研究機構之條件。僅有我國和日本採取「學術研究」為合法要件用語，始將適用主體限於學術研究機構或單位。

除此之外，有關合法事由，我國第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之規定限於基於「公共利益」為目

[176] 參考司法院釋字 380 號解釋理由書，以及同號解釋大法官林永謀及楊慧英協同意見書。

的而為統計或學術研究而有必要，始得為之。但觀察歐盟、英國及德國之規定，符合其個人資料之屬性及各該合法事由，得處理個人資料；另觀察美國、日本、韓國、新加坡等國家，基於研究目的或科學研究之目的，即得作為合法事由，而無須限於特定目的之研究行為。是以，我國個資法學術研究限於公共利益為目的，始得合法蒐集、處理或利用個人資料，可能會使非公共利益之研究性質者，難以適用本條款之合法要件，例如基於商業利益或私人利益之研究情形等。

此外，在個資法第 6 條第 1 項第 4 款規範相較於前述公共利益，有關特種個人資料則更限縮，僅得基於「醫療、衛生或犯罪預防目的」之學術研究，始得為之。考究我國個資法之立法沿革，於 2015 年修法，個資法第 6 條第 1 項第 4 款規定「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」並刪除第 2 項授權辦法之規定，即刪除程序控管之相關規範，並於修法理由指明基於資料之合理利用，鬆綁以促進學術研究發展，並由公務機關自行制訂行政規則。就此部分，參考英國、德國或美國之個資法規範，有提供特殊適當之保護措施，殊值參考。

表 23 我國與各國有關研究/科學研究/學術研究合法要件之比較

國家	適用主體	合法事由（排除當事人同意）	管理措施	其他
我國	公務機關、學術研究機構	基於公共利益/醫療/衛生/犯罪預防目的+為統計或學術研究有必要	資料經提供者處理後/經蒐集者依其揭露方式無從識別特定之當事人	特種個資另有人體研究法、人體試驗及人體生物資料庫管理規定
歐盟	無限制	— 公共利益 — 執行職務所必要行使	對資料當事人之權利和自由	
英國				— 禁止對當事人造

			公權力所必要 — 追求正當利益所必要+利益衡量	提供適當保護措施，並應採取技術+組織上之措施+遵守最小化利用原則	成重大危害/痛苦之處理 — 醫學研究應經相關委員會核准
德國*					特種個資有特殊利益衡量
美國	**UPDPA****	無限制	符合當事人期望/有利當事人+相容性作業資料判斷	落實合理資料安全措施+資料隱私與安全風險評估	醫療資料適用HIPAA；臨床實驗或其他生物醫學研究之個資，應從其特別規定
	CCPA		基於研究之目的	落實明列之適當安全措施	
	HIPAA	健康計畫/健康照顧清算中心/健康資訊之健康照顧提供者	— 事前告知+選擇同意 — 經研究倫理/隱私委員會審查	管理安全+物理+技術上保護措施，應符合「電子保護健康資料之安全標準規則」	
日本		大學及其他以學術研究為目的之機構/團體/所屬人員	以學術研究為目的之活動	採取必要適當之安全管理措施、對從業人員或受委託人之適當監督	醫療個資另有「次世代醫療基盤法」加以規範
韓國		無限制	基於科學研究之目的	應進行假名化之處理	欲連結假名化資料，應取得指定之

				專門機關許可
新加坡	無限制	符合「視為同意」之情形	評估以消除或減輕不利影響+充分告知	
		基於促進業務改進之目的	須合理實現目的+一般人認為符合適當蒐集個資之情形	不以單獨識別個人形式將無法合理實現目的
		基於研究之目的	須合理實現目的+不切實際+公共利益+不影響個人+無法識別個人	
菲律賓	無限制	基於科學/統計研究之目的	應落實明訂之管理措施	特種個資應符合專業倫理規則
*：針對特種個資另有嚴格適當且具體之措施規定 **：僅 UPDPA 要求不得對特定個人進行預測/決定				

資料來源：本計畫研究團隊自行整理

（三） 有關學術研究而蒐集、處理或利用個資之特殊彈性規範

目前針對學術研究之彈性措施分別為：目的外利用及免為告知義務。依據個資法第 16 條第 5 款及第 20 條第 1 項第 5 款規定，公務機關及非公務機關得基於研究目的而為目的外利用。此外，依據個資法第 9 條第 2 項第 5 款之規定，公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之一般個人資料，如果係基於公共利益為統計或學術研究之目的而有必要，且該資料經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限，得於處理或

利用前免為告知個人資料來源及第 8 條第 1 項第 1 款至第 5 款所列事項。有關特種個人資料之免告知義務，則係依第 6 條第 2 項準用第 9 條第 2 項第 5 款之規定。

觀察歐盟、英國及德國之個資法規定，針對科學研究之彈性規定，包含允許就科學研究之特定範圍內取得同意、進階處理不視為與原始目的不相容、可延長一定儲存期間等彈性措施；而德國針對取得當事人同意或公開屬於歷史事件不可或缺時，以及新加坡若已去識別至無法辨別資料當事人時，則可公開當事人之個人資料等特殊規定；以及新加坡如遵守 PDPC 發布之資料共享政策與指南，向 PDPC 提出 DSA 之個人與商業資料共用申請，得於遵守 PDPA 規範下，提供組織內部與組織間之個資共用及資料共享。就此而言，綜觀比較法上其他國家之作法，我國目前針對學術研究之彈性措施，僅有目的外利用與免除告知義務，稍嫌過少，未來修法建議可適度地參考其他國家予以調整。

表 24 我國與各國針對研究/科學研究/學術研究彈性措施之比較

國家	儲存時間延長	免除告知	公開研究成果	其他特殊規定
我國		間接蒐集免告知義務		
歐盟	可延長儲存期間	提供資料之時間/精力，對科學研究造成影響,得免告知義務		
英國				
德國*			— 取得同意 — 歷史事件不可或缺	
美國				
日本			學術研究成果公布/教授不得已時+不侵害個人權利或利益	
韓國				
新加坡		—基於促進業務改進目的 —基於研究目的	必須以無法識別個人之形式公布結果	遵守資料共享政策，得豁免 PDPA 規定
菲律賓	得延長儲存期間			
*：僅德國規定識別特定/可得特定之標記可以不用分開儲存				

資料來源：本計畫研究團隊自行整理

二、小結

綜合上述分析討論之內容，結構上明顯可見學術研究之概念定義與內涵，將影響本款合法要件之適用問題，即適用主體及合法事由等法律要件，可能影響產業基於研究或科學研究之目的，而發展資料經濟之利用可汲性。目前除了菲律賓明顯規定基於研究目的而處理個人資料，排除於個資法之適用範圍外，可清楚地區分為二大類型：如屬於歐盟、英國、德國、美國、韓國或新加坡等國家，定義為「研究或科學研究」者，則其適用主體上將不限制為特定主體，而在合法

事由上得基於該研究或科學研究目的，即可為之，而無需限於特定公共利益之目的；但歐盟國家與美國針對研究或科學研究之概念，係限於一定研究方法、研究倫理與隱私法規等範圍。另一類則係我國與日本皆以「學術研究」作為規範用語，並限於特定主體始得適用本款合法事由，但相較於日本之規定，我國之一般個人資料限於公共利益目的，而特種個人資料限於醫療、衛生或犯罪預防之目的。

綜上所述，若未來我修法調整學術研究之相關條文，除需體系性考量是否配合目的內與目的外利用、公務機關或非公務機關，以及是否區分蒐集、處理或利用等框架性問題調整外，參考多數國家之規定與作法，就現有個資法之制度，除調整個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款等合法要件之規定，應一併修改相關規範用語，以便放寬適用本款之適用主體，亦得考慮刪除合法事由之特定目的限制，但有關特種個人資料之額外保護措施，可考慮以特種個人資料程序性控管規定加以保障，或另由特別法或授權目的事業主管機關以命令，加以規範為宜。

最後，有關學術研究之彈性措施，目前若以學術研究而為蒐集、處理或利用個人資料時，可目的外利用或免為告知義務，但相較於比較法上其他國家之規定，現行彈性措施仍有調整空間，而考量研究業務範疇涉及科學技術發展、產業創新研發及社會生活之提升，若能適度地提供資料流通或彈性放寬研究等特殊規定，將有助於資料經濟之運用與發展。

第二項　假名化及匿名化

壹、比較法國家

一、歐盟

（一）　假名化之規範

1. 定義及效果

假名化（pseudonymisation）作為去識別技術，係將得識別個人之資料以人工識別碼、別名、假名取代[177]。因此假名化資料仍與當事人有隱形連結，得間接識別自然人，仍有 GDPR 之適用。依 GDPR 第 4 條第 5 項明定假名化為資料經處理後，非與其他資料比對無法識別特定個人，並應將其他資料分開保管且採用技術上或組織上適當措施防止資料識別之風險。依 GDPR 第 25 條第 1 項表示資料假名化係技術及組織上安全措施之一，又依 GDPR 第 32 條第 1 項第 a 款明定假名化為風險管理技術之一。當假名化資料發生事故時，依 GDPR 第 34 條第 3 項第 a 款規定，控管者得免除通知當事人之義務。

2. 相關規範

GDPR 前言第 28 點表明 GDPR 視假名化為風險管理的技術，個人資料假名化後可有效降低當事人所承受的風險並幫助資料控管者及處理者遵循 GDPR。由於 GDPR 將假名化視為風險管理技術，針對假名化之加工方式，第 29 條資料保護工作小組 2014 年發布意見列舉之技術包括：（1）加密（Encryption），係使用祕密金鑰（secret key）加密個人資料，擁有祕密金鑰的使用者可還原資料以識別自然人，用於解密的祕密金鑰即是 GDPR 第 4 條第 5 項規定下所稱之「其他資料」。（2）雜湊函數（Hash Functions），係以人工代碼取代可識

[177] Chris Achatz and Susan Hubbard, *US vs. EU Guidelines for De-Identification, Anonymization, and Pseudonymization*, JOURNAL OF INTERNET LAW, 20(11), 1, at 1 (2017).

別個人的識別碼[178]。（3）記號化（Tokenization），係將個人資料與一組記號（token）代替，記號係隨機產生與個人資料並無關連[179]。

而針對假名化資料之管理雖未明文規範，惟歐盟網路安全局（European Union Agency for Cybersecurity, ENISA）於最佳實務典範報告提出以下建議[180]：（1）原始資料應與假名化資料分開於不同的檔案夾存放。（2）假名化資料應存放於安全的媒體，避免存放於硬碟、系統等。（3）組織應建立管理制度或章程，對於存取權限進行高強度管理，且存取紀錄應以 log 紀錄為之。（4）原始資料應進行加密，加密後之金鑰管理及存放亦須留意。

（二）　匿名化之規範

1.　定義及效果

GDPR 前言第 26 點將匿名化（anonymisation）資料定義為無法直接識別或間接識別個人之資料，由於不屬於個人資料，因此不適用 GDPR。匿名化技術所進行去識別化之程度遠高於假名化，係將任何得識別當事人之資料去除，並使當事人再也無法被識別。

2.　相關規範

同樣地，GDPR 亦將匿名化視為風險管理技術之一，針對假名化之加工方式，第 29 條資料保護工作小組於 2014 年發布意見所列舉之技術包括：（1）雜訊加入（Noise Addition），係指將得識別個人之識別碼以概括方式表述，如將身高以實際身高加減 10 公分做紀錄[181]。

---

178 *id*, at 4.

179 NERDWALLET, *Credit Card Tokenization: What It Is, How It Works* (2021), https://www.nerdwallet.com/article/credit-cards/credit-card-tokenization-explained (last visited Dec. 3, 2021).

180 EUROPEAN UNION AGENCY FOR CYBERSECURITY, *Pseudonymisation techniques and best practices: Recommendations on shaping technology according to data protection and privacy provisions* (2019), https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices, at para 5.5, (last visited Dec. 3, 2021).

181 ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 05/2014 on*

（2）排列變更（Permutation），係指變更排列得識別個人之識別碼以達到匿名化，如將原始資料以表格呈現，變更排列方式使其無法與當事人連結[182]。（3）資料聚集與 K 匿名（Aggregation/K-Anonymity），主要運用於表單形式之資料，目的係將得識別之個人資料概括化，使資料交叉比對後無法識別特定自然人[183]。

二、英國

（一）　假名化之規範

1.　定義及效果

英國 UK GDPR 第 4 條第 5 款有關假名化之定義，沿用歐盟 GDPR 規定。由於假名化資料經與其他資料比對，仍得識別特定自然人，故應適用 UK GDPR 之規範。依 UK GDPR 第 25 條第 1 項，假名化技術得作為幫助控管者實踐 UK GDPR 義務之方式，又依 UK GDPR 第 32 條第 1 項第 a 款作為風險管理技術之一。若假名化資料發生個資事故時，由於難以識別特定個人，依 UK GDPR 第 34 條第 3 項第 a 款規定，控管者得免除通知當事人之義務。

2.　相關規範

根據 UK GDPR 前言第 29 點，為鼓勵控管者於個人資料處理過程中應用假名化技術，同一控管者，若已採取必要之技術性及組織性措施，以確保處理過程遵守 UK GDPR，且已將得識別特定當事人之其他資料分開存放，則得將該資料用於一般分析，惟須註明該被授權人之身分。另針對重新識別定義為違法行為，並明訂於 DPA 第 171 條第 1 項，若個人故意或過失將假名化資料，在未經控管者於其法律責任範圍內同意，進行重新識別之行為，屬於違法行為；同條第 5

Anonymisation Techniques(2014),https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf, at 12, (last visited Dec. 3, 2021).

182 *id*, at 13-14.

183 *id*, at 16.

項規範因故意或過失而處理重新識別之資料，亦屬於違法。除有 DPA 第 171 條第 2 項至第 8 項及第 172 條之阻卻違法事由，如犯罪偵查、當事人同意、行為人合理相信該行為合法、或用於新聞及公共利益等目的。

（二）　匿名化之規範

1. 定義及效果

依 UK GDPR 前言第 26 點，匿名化技術所進行的去識別化，則定義為將資料中可識別當事人之資料去除，並採取技術性措施，使該當事人無法再被識別。其定義乃沿用歐盟 GDPR 規定，因匿名化資料不涉及已識別或得識別自然人之資料，其已非屬於 UK GDPR 欲保護之個人資料範圍，故無 UK GDPR 之適用。另英國 ICO 於 2021 年 5 月發布「匿名化、假名化和隱私增強技術指南」（anonymisation, pseudonymisation and privacy enhancing technologies guidance）之草案，提及匿名化資料應視為資料轉譯後之結果，故亦無 DPA 之適用。

2. 相關規範

ICO 於「匿名化、假名化和隱私增強技術指南」之草案認為有效之匿名化，應使資料與已識別或可得識別之個人無關，或以無法識別個人之方式呈現。惟其強調匿名化有效之判斷將隨著技術、時間推移而變化，難以確保存在完美之匿名化技術，必須就每個案例單獨評估具體情形作為判斷，因此未規定匿名化之加工方式。

而針對匿名化資料之管理規範，ICO 於 2012 年發布之「匿名化：資料管理風險守則」（Anonymisation: managing data protection risk code of practice），建議組織進行匿名化流程時應注意授權及監督責任、員工培訓、識別可能需匿名化之程序、新指南或判例法之知識管理、相關行業組織、隱私影響評估、透明度、審查匿名程序後果、事故後對當事人損害之回復。另建議可透過高級資訊風險負責人（Senior Information Risk Owner, SIRO）制度，由具有足夠資歷、管

理流程技術經驗及法律背景者擔任 SIRO，負責組織之關鍵決策，並提供公司組織匿名化相關資訊[184]。此外，針對匿名化資料之重新識別行為，如同前述有關假名化資料禁止重新識別之規定，亦屬違法，除有阻卻違法事由之外，不得重新識別匿名化資料。

三、德國

（一）　假名化之規範

1. 定義及效果

德國有關假名化除適用 GDPR 規範外，依 BDSG 第 46 條第 5 款規定，所謂「假名化」（Pseudonymisierung）資料為非與其他資料比對，無法識別特定個人。此外，針對假名化資料應與其他資料分開保管，並採取技術及組織上措施，以避免被重新識別之風險。

2. 相關規範

德國 BDSG 針對程序面並無特別規定，惟依 GDPR 第 25 條第 1 項及 BDSG 第 7 條第 1 項規定，資料控管者應在決定個人資料處理方式或進行處理時，採取適當預防措施（angemessene Vorkehrungen）。該預防措施必須依 GDPR 第 35 條及 BDSG 第 67 條之資料保護影響評估（Datenschutz-Folgenabschätzung）而認為適當且有效落實資料保護原則，如資料最小化原則（Datensparsamkeit），與應確保遵守法律要求及保護當事人權利。惟控管者得考量現有技術、實施成本與處理之類型、範圍、情況及目的，對於當事人權利及自由處理相關風險之不同發生概率、嚴重程度，決定所採行之適當預防措施。另依 BDSG 第 64 條第 2 項規定，該假名化措施應能夠確保：（1）與處理個人資料有關連的系統及服務，具備機密性、完整性、可用性及彈性要求（2）在發生物理或技術事故時，個人資料的可用性及近用性得被快

[184] ICO, *Anonymisation: managing data protection risk code of practice*, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf (last visited Dec.7, 2021)

速地回復。

（二）　匿名化之規範

德國有關匿名化亦適用 GDPR 之規範。另依 BDSG 第 27 條第 3 項、第 50 條及第 71 條第 1 項規定，並不排除以匿名化方式，作為個人資料之適當及具體措施。至於匿名化是否具有「識別性」之判斷標準，該判斷標準應考量所有合理使用方法及客觀因素，因此匿名性資料將隨著當時技術發展而有所改變，故控管者及處理者即便將個人資料匿名化，仍應隨時檢查個人資料去識別化之程度，以符合當時匿名化之要求[185]。

四、美國

（一）　UPDPA

依 UPDPA 第 2 條第 5 款有關去識別化資料（Deidentified data）之定義，係指已刪除所有直接識別符（如姓名、地址、電子郵件地址、可識別照片、電話號碼與社會安全號碼）之個人資料，並可以合理確保未經允許或者不具備特殊存取權限之人無法透過相關資料識別特定當事人。另同條第 14 款對於假名化資料（Pseudonymized data）之定義，係指不包含直接識別符之個人資料，且無法合理與當事人之身分相關連，或無法被維護以允許與當事人進行個人化溝通或處理，如不含直接識別符之網路協議位址（internet protocol address）、瀏覽器、硬體或軟體識別代碼（a browser, software, or hardware identification code）、永久單一代碼（a persistent unique code）或特定設備有關的其他資料。另外，依據 UPDPA 第 9 條第 a 項及 b 項規定，控管者不得從事禁止性資料作業，當有重新識別或導致重新識別假名化資料或去識別化資料以蒐集或建立個人資料之行為，原則上將被視為禁止性資料作業。

---

185 Taeger/ Gabel, a.a.O (Fn. 84), Rn. 47-48.

（二）　CCPA

依 CCPA 與 CPRA 第 1798.140 條第 v 項第 3 款規定，個人資料不包含經去識別化（deidentified）或匯總化（aggregate）的資料。依 CCPA 與 CPRA 第 1798.140 條第 b 項與第 m 項規定，去識別化係指不能合理用於推斷有關特定消費者或以其他方式連結至特定消費者的資料。而匯總化的消費者資料係指與消費者群體或類別有關的資訊，其中個人消費者身分已被刪除，且沒有連結或合理連結任何消費者或家庭。至於假名化資料則依 CPRA 第 1798.140 條第 aa 項規定，係指在不使用其他資料的情形下，以不再連結特定消費者的方式處理個人資料，前提是其他資料單獨保存並確保採取資料無法識別或可識別消費者的技術上與組織上措施。

針對企業有關去識別化義務，依據 CCPA 與 CPRA 第 1798.140 條第 m 項規定包括：（1）採取所有合理措施確保資料不會與消費者或家庭相關連；（2）公開承諾以去識別化方式維護與利用資料，並且不會嘗試重新識別資料；(3)根據契約，任何資料接受者將遵循 CCPA 有關去識別化規範。而消費者個人資料經去識別化後得允許基於研究目的利用，並應依 CCPA 第 1798.140 條第 ab 項遵循相關規範，包括：（1）與蒐集個人資料之商業目的相符；（2）隨後進行假名化、去識別化或匯總化，使企業不能合理識別、涉及、描述、直接或間接關聯特定消費者；（3）除研究必要，禁止重新識別資料；（4）防止資料洩漏；（5）防止任何重新識別之企圖；（6）僅用於蒐集個人資料背景相關之研究目的；（7）由進行研究之企業進行存取權限控管，僅執行研究目的必要之人始得存取資料。另依 CCPA 第 1798.148 條第 a 項規定明文禁止任何人對去識別化資料重新識別，除非符合公共衛生目的或依據聯邦法進行之研究，始得例外允許之。

（三）　HIPAA

依 HIPAA「個人可辨識健康資料隱私規則」第 164.502 條第 d 項，個人健康資料經去識別化處理時，受規範機關即可將此去識別化

之健康資料進行其他目的之使用。同時依「電子保護健康資料之安全標準規則」第 164.514 條第 a 項，有關去識別化之受保護健康資料（de-identification of protected health information），係指無法識別特定個人，且無合理依據相信其可用於識別特定個人之健康資料。HIPAA 規範個人健康資料原則上不得利用或揭露，惟透過去識別化（deidentified），則得例外無須取得當事人同意為之。

而 HIPAA 有關去識別化之方式包括：（1）「專家核決」（Expert Determination），係指由在統計學、科學之原則及方法上具備適當知識及廣泛接受經驗之專家，以適當原則及方法認定資料接受方不論單獨利用或與其他合理可得之資料一併使用，均僅有極小風險可識別特定個人，並以書面說明其方法及分析結果；（2）安全港條款（Safe Harbor），係指依「個人可辨識健康資料隱私規則」第 164.514 條第 b 項第 2 款第 i 點，去除 18 項識別因子（identifiers）[186]，且受規範主體不論單獨使用或合併其他資訊，均無「實際具體知識」（actual knowledge）得識別健康資料之特定個人時，始達到去識別化之程度。

五、日本

（一）　假名化之規範

1. 定義及效果

日本有關假名化資料規定於個資法第 2 條第 5 項，係指個人資料經加工處理後，非與其他資料比對無法識別特定個人之資料。另針對假名化資料處理事業規定於第 16 條第 5 項，係指針對包含假名化資料之資訊集合物，為使特定假名化資料經由電腦檢索等行為，從而

[186] 18 項識別因子包含姓名、地理資訊、所有與個人直接連結的資料要素、電話號碼、傳真號碼、電子郵件信箱、社會安全號碼、醫療紀錄號碼、健康照護計畫受益人號碼、帳戶號碼、證書號碼、車輛識別與序列編號（包含汽車牌照號碼）、設備識別及序列編號、網頁網址、通訊協定位置編號、生物識別因子（包含指紋與聲紋）、全臉照片與其他可比較影像以及任何其他獨特可識別之號碼、特徵或編號。

構築為體系化資訊，由政令所訂之事業，使特定假名化資料易於檢索並成為體系化資訊。假名化之效果依第 41 條第 9 項規定，考量假名化資料本身不具識別性，如發生資料洩漏亦已相當程度降低個人權益受侵害之風險，故不適用第 17 條第 2 項變更利用目的之限制、第 26 條洩漏報告義務、第 32 條有關保有個人資料事項之公告義務、第 33 條揭露義務、第 34 條訂正義務第 35 條停止利用或刪除義務及第 36 條至第 39 條程序規定。

2. 管理規範

日本針對假名化之加工方式訂有一般通用性規定，依個資法第 2 條第 5 項第 1 款應刪除第 2 條第 1 項第 1 款個人資料中之姓名、出生年月日及其他得以識別特定個人之記述；復依同項第 2 款規定，應刪除個人資料中包含個人識別符號者。假名化之加工標準依第 2 條第 5 項應達到「非與其他資料比對，無法識別特定個人」之程度，又依個人資料保護法施行規則第 18 條之 7 第 1 項規定為刪除或替換個人資料中可以識別特定個人之全部或部分記述；第 2 項為刪除或替換所有個人識別符號；第 3 項為刪除或替換可能因非法使用所造成財產損失之記述。

而假名化之管理規定，依第 41 條第 3 項規定，事業非依法令不得將假名化資料作目的外利用；同條第 4 項規定於作成假名化資料時，事業有公告利用目的之義務，且不得以向當事人通知方式代替之；同條第 6 項規定，事業非依法令不得向第三方提供個人資料；第 7 項禁止以識別個人作為比對目的；第 8 項禁止利用聯絡資訊，包括住址及電話、傳真機或其他電子通訊方式。又依第 42 條第 1 項規定，事業非經法令允許不得向第三方提供假名化資料；第 3 項禁止事業以識別目的取得原始資料。

另依第 42 條第 3 項有關假名化資料之安全管理措施規定，事業於作成假名化資料或取得假名化資料及原始資料時，為防止資料洩漏必須採取安全管理措施。復依個人資料保護法施行規則第 18 條之

8 有關原始資料之安全管理措施標準，第 1 項規定應明確化原始資料等（包括原始資料與加工方法之資訊）處理者之權限及責任；第 2 項為應制定有關原始資料等處理之規範，依其進行適當處理，並評估處理情形且根據結果採取必要改善措施；第 3 項為防止非法權限者近用原始資料，應採取必要適當措施，如完善組織體制、進行員工教育、掌握原始資料等處理情形並進行評估與改善，防止措施則包括避免攜帶電子設備或廢棄機器及電子設備、避免使用資訊系統等時發生原始資料洩漏；而對於近用原始資料之存取權限則包括近用者身分識別與認證等方式。

（二）　匿名化之規範

1. 定義及效果

日本有關匿名化資料規定於個資法第 2 條第 6 項，係指個人資料經加工後為無法識別特定個人之資料，且無法復原者。有關匿名化資料處理事業者依第 16 條第 6 項，係指針對包含匿名化資料之資訊集合物，為使特定匿名化資料經由電腦檢索等行為，成為體系化資訊並易於檢索，由政令所訂之事業。而個人資料經匿名化後，得不經當事人同意，提供予第三人或進行目的外利用。

2. 相關規範

有關匿名化之加工方式訂有一般通用性規定，依第 2 條第 6 項第 1 款應刪除或替換第 2 條第 1 項第 1 款個人資料中之姓名、出生年月日及其他得以識別特定個人之記述；復依同項第 2 款規定，應刪除或替換個人資料中包含個人識別符號者[187]。為確保匿名化資料無法還原，依第 43 條第 1 項規定個人資料處理事業應依循個人資料

[187] 其規範得分為：(1)須對應「記述型」及「符號型」個資進行不同之加工方法；(2)須依「無法有規則性之方法得以復原」原個資之方法進行加工；(3)對「記述型個資」為刪除包含於個資中一部分之記述，而對「符號型個資」則為全部刪除。

保護委員會所制定之規範基準進行匿名化處理作業[188]。依個人資料保護法施行規則第 19 條揭示匿名加工標準包括：第 1 項規定為刪除或替換個人資料中可以識別特定個人之全部或部分記述；第 2 項為刪除或替換所有個人識別符號；第 3 項刪除或替換連接個人資料與相應個人資料採取措施獲得資訊的符號；第 4 項刪除或替換特異記述等；第 5 項除前各項所揭示措施以外，尚須考慮個人資料中所包含的記述等與構成個人資料資料庫中包含該當個人資料之間的差異及資料庫的性質，根據其結果採取適當措施。上述僅為所有業界共通適用之最低限度加工標準方法，業者非得僅選擇其一而須均遵守。

有關匿名化資料之管理規定，依第 43 條第 2 項個人資料處理事業應遵循個人資料保護委員會所制定之規範基準，採取必要安全管理措施[189]。依同條第 6 項相關安全管理措施必須包含針對個人資料匿名化所提出之申訴對應處理機制，及確保匿名化資料適當處理之其他必要措施[190]。依第 46 條安全管理措施規定，匿名化資料處理事業自身應致力採取對匿名化資料之安全管理上必要且適當措施、有關匿名化資料處理之申訴及其他為確保匿名化資料之適當處理必要措施，且須公告該措施之內容。又依個人資料保護法施行規則第 20 條進一步規定，有關安全管理措施標準包括：第 1 項規定應明確規範有關加工方法等資訊之處理者權限及責任；第 2 項規定應整備有關加工方法等資訊之處理規範，依其規範適當處理，並對其處理狀況

188 依第 43 條第 1 項授權個人資料保護委員會以法規命令性質之施行規則訂立加工標準。

189 依第 43 條第 2 項規定，個資處理事業在作成匿名加工資料時，對自原個資所刪除之部分資料，採取之加工程序、程式等有關加工方法之資料，應明確其管理責任人、訂立管理規程等安全管理措施以防止其洩漏。

190 依本法第 43 條第 6 項，個資處理事業應於作成匿名加工資料時，努力針對該當匿名加工資料之安全管理採取必要且適當之措施；對於該當匿名加工資料之作成，及在處理有關申訴之處理及其他確保該當匿名加工資料之處理事宜上採取必要措施，且應將該當措施之內容予以公告。此義務並非具有強制力之法定義務而是努力義務，從而此項之安全管理措施，個資處理事業得依其事業性質、該當匿名加工資料之性質、數量、處理狀況等進行合理且適當之安全管理、及建置申訴處理等措施。

進行評價且進行改善；第 3 項規定爲防止不具正當權限之人近用，應採取必要適當措施。

而有關匿名化資料處理事業之義務，依第 43 條第 5 項規定其不得採用與其他資料對照識別，並依第 45 條規定匿名化資料處理事業進行匿名化時，若擬識別當事人，應透過其所須刪除之原始資料中具識別性之資訊或個人識別符號，或依第 43 條第 1 項所規定之匿名化加工方式取得，不得將該匿名化資料與其他資料對照辨識[191]。同時應依同條第 3 項規定，公佈匿名化資料中所包含之個人資料類別，並依個人資料保護法施行規則第 21 條於作成匿名化後不得延遲，而利用網路或其他適切方法為之[192]。另有關提供匿名化資料予第三人之規範，依第 43 條第 4 項及第 44 條規定，個人資料處理事業應依循個人資料保護委員會所制定之規範基準，事先公布匿名化資料中所包含之個人資料類別及其提供之方式，同時針對該第三人須明示其所提供之資料屬於匿名化資料。依個人資料保護法施行規則第 22 條、第 23 條公布得利用網路或其他適切方式為之，而明示方式則得利用電子郵件或書面交付等其他適切方式為之。

3. 日本次世代醫療基盤法

日本為推動健康、醫療領域研發及產業發展，制定次世代醫療基盤法以管理醫療資料匿名化業者，使他人能安心利用經匿名化處理

---

191 此項立法係因：1.本法規定個資處理事業在進行匿名加工時，並未要求其將原個資刪除，故須立法阻斷其組合比對復原原個資之可能；2.本法僅要求匿名加工資料依一般人及一般事業之能力、技術等基準，為無法識別特定人且無法回復原狀，並未排除技術面上所有可能性，因此個資處理事業可能利用其他資料或高度之資訊技術，進行當事人之再識別或回復原狀，對安全性保障存有威脅，故特別以本項明文禁止個資處理事業進行匿名加工資料之再識別行為，以課予法律義務之方式，擔保匿名加工資料之安全性。

192 例如原包含有「姓名、出生年月日、性別、購買履歷」之個資，經匿名加工後為「出生年、性別、購買履歷」者時，匿名加工資料包含之上開三個項目，應予以公告。此係因匿名加工資料作成過程中，並無當事人得參與之機制，立於個資法之透明化原則，應讓當事人知悉並能確認自己個資被加工後之狀態。

之醫療個人資料，並設置認定機構，以確認業者是否符合一定標準及具備相當之匿名化技術，始得進行醫療資料匿名化作業等。本法所稱匿名化醫療資料依第 2 條第 3 項規定，係指經法令所定程序與標準進行匿名化，已無法識別特定個人且無法回復原狀之醫療資料。而有關匿名化醫療資料作成事業依第 2 條第 4 項規定，係指有助於醫療領域之研究開發，而處理及加工於醫療資料以作成匿名化醫療資料之事業。因此經匿名化之醫療資料，即可提供予產業、政府或學界進行加值運用。

匿名化應由政府認定之匿名化醫療資料事業辦理[193]，而匿名化醫療資料事業依本法第 8 條應具備相關申請資格、符合法定要件並經主管機關認定，始取得合法對醫療資料進行匿名化之資格；相關申請資格包含醫療資料之整理方法、匿名加工方法，以及資訊安全管理措施上應達到政府要求的標準，並承諾遵守認定匿名化醫療資料事業之義務，如本法第 17 條遵守利用目的限制、第 18 條禁止重新識別、第 19 條刪除無利用必要之資料、第 20 條安全管理措施、第 21 條從業人員之監督、第 24 條委託對象之監督、第 33 條資料正確性之確認義務等。如未符合上述規定，則主管機關得依第 15 條撤銷認定。

在保障醫療資料當事人權利部分，本法要求在醫療機構、網站公告，以及在當事人就診時，對當事人進行告知其醫療資料將經匿名化處理後提供利用且得隨時請求停止提供，故以事前充分告知加上當事人得行使事後退出權之方式，提供當事人在匿名化前，有機會得自主決定是否提供醫療資料供匿名化處理後利用，以維持保障醫療資料當事人權利之要求。

---

193 依本法第 28 條規定，受認定匿名加工醫療資料作成事業之委託進行處理醫療資料等或匿名加工醫療資料之事業（限於法人），得依申請，經主管機關大臣認定其得適當且確實執行該當事業。

六、韓國

（一）　定義及效果

為使個人資料之概念更具體，PIPA 明確區分個人資料、假名化資料、匿名化資料。雖然 PIPA 未明文規範匿名化資料，惟依 PIPA 第 58 條之 2 規定，「以合理之時間、費用、技術予以評估，當透過其他資料也無法識別特定個人時，即不適用本法」。故 PIPA 排除匿名化資料之適用，主要針對假名化有較為詳盡之規範。依 PIPA 第 2 條第 1 項第 3 款規定，假名化資料係指個人資料（包含透過姓名、住民登錄號碼及藉由影像得直接或間接識別個人之資料）經假名處理後，非使用或結合其他供還原識別之其他資訊，無法識別特定個人之資料。由於個人資料假名化處理後仍具有間接識別性，因此仍為 PIPA 保護之個人資料範圍。個人資料經假名化後，得用於統計編製、科學研究及公益紀錄保存等目的處理。另外假名化資料依第 28 條之 7 規定，得排除第 20 條、第 21 條、第 27 條、第 34 條第 1 項、第 35 條至第 37 條、第 39 條之 3、第 39 條之 4、第 39 條之 6 至第 39 條之 8 等規定之適用，如間接蒐集之應告知事項、保存期限屆期之銷毀、處理者讓渡全部或一部經營業務或合併所需傳輸個人資料之限制、資料洩漏之通知、當事人行使權利（請求閱覽、更正、刪除、撤回同意）及其個人資料被利用之通知等。

（二）　管理規範

有關假名化之加工方式訂有一般通用性規定，藉由刪除或替代個人資料之部分、全部，達到非與其他資料比對時，無法識別特定個人之程度。而有關假名化之管理規定，依第 28 條之 4、第 28 條之 5、第 28 條之 6 規定，假名化處理過程須採行指定的安全措施，並進行相關紀錄的編製及保管，並且禁止再續探究特定個人背景。有關安全措施依第 28 條之 4 規定，組織應設置技術、管理及物理上必要安全措施，將額外可還原辨識特定個人之資料分別管理，以防止遺失、竊取、洩漏、變造及毀損等情事；在處理假名化資料時，並應填

載目的且保存相關文件管理紀錄。

而假名化之義務依第 28 條之 2 之規定，即使基於統計編製、科學研究及保存公益紀錄等目的利用假名化資料，若有將假名化資料結合之需求，應由個人資料保護委員會或相關中央行政機關首長指定之專門機關執行；若將專門機關結合之資料對外傳輸，應依第 58 條之 2 規定處理後，取得專門機關負責人之批准，並依照專門機關所指定之標準、程序、管理、監督，始得為之。另外，任何人均不得以識別特定個人為目的處理假名化資料，如處理過程中得以識別特定個人時，應立即中止並將該資料返還、銷毀。

七、新加坡

（一）　定義及效果

PDPA 未針對假名化或匿名化予以規範。惟 PDPC 所發布之「PDPA 特定議題指南」（Advisory Guidelines On The Personal Data Protection Act For Selected Topics）及「資料匿名化基本技術指南」（Guide To Basic Data Anonymisation Techniques），說明有關匿名化及匿名資料之定義，以及組織選擇匿名化技術所應考量之因素，提供組織針對內部營運狀況進行判斷處理。

依 PDPA 特定議題指南解釋匿名化，係指將個人資料轉換為無法用於識別任何特定個人之過程，且無論其是否可逆轉回復為原始資料。換言之，匿名化係透過技術將原始個人資料轉化為匿名化資料之過程，而匿名化資料則係指經過匿名化技術，並針對特定個人重新識別風險進行評估之資料。由於匿名化資料並非個人資料，排除 PDPA 第 3 編至第 6A 編資料保護規定之適用。另依 PDPA 第 25 條規定，若保存個人資料已不再符合蒐集目的，或基於法律、商業目的所保存之個人資料已無必要性，組織必須停止保存或刪除時，得將個人資料匿名化以符合 PDPA 要求。

（二）　管理規範

如同歐盟將匿名化視為風險管理控制措施，作為防止資料洩漏及安全漏洞的保護措施，因此並未有相關管理規定。有關匿名化技術，PDPC 認為應依個案選擇採用最合適組織運用之技術，依 PDPA 特定議題指南例示以下常用之匿名化技術，並提供如何運用各項技術之範例說明[194]：（1）假名化，係利用其他方法替換個人識別符號，用編造數值替代身分辨識資訊，當原有資料經過適當處理且不可重複之方式進行時，達到不可逆轉之假名化，另依「資料匿名化基本技術指南」[195]說明假名化有無逆轉之差異性（2）資料彙集（Aggregation），係指將資料集記錄轉換為總合值以總數呈現，不顯示可識別特定個人的任何單一資訊（3）取代（Replacement），為計算平均值或透過子集方式取代原有資料（4）資料抑制（Data suppression），係指當匿名資料集無需某一屬性時，此技術應於匿名化過程的起始階段使用，以降低特定個人可辨識度（5）資料重組或概括化（Data recoding or generalisation），為將類別分組或分為更廣泛類別，意圖降低資料準確性（6）資料清洗（Data shuffling），為將相同類型資訊進行混合或替換，使資料相似但與原始資料無關（7）遮蔽（Masking），以使用一個不變的符號（如「*」或「X」）對資料字符進行修改，通常為部分遮蔽，僅替換資料之特定字符，或刪除部分細節同時保留資料原始呈現。

而針對資料是否匿名化之參考因素包括：（1）資料性質與類型，即組織需考量資料性質以判斷需刪除多少識別資訊，使其不再具識別性。此外，具有特殊資料之樣本資料集可能無法達到匿名效果，仍有重新識別之風險，組織必須謹慎管理以確保資料集達成有效匿名

---

194 PDPC, *ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS*, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (last visited Dec. 9, 2021).

195 PDPC, *GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES*, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf (last visited Dec. 9, 2021).

化處理（2）對特定個人潛在影響，即組織應考慮重新識別個人身分對特定個人有無任何潛在負面影響，若屬於具高度敏感性個人資料，縱使組織評估識別風險低，仍應謹慎考慮是否合適。

由於 PDPA 特定議題指南強調組織於進行匿名化之前，應針對重新識別風險進行評估，考量資料集是否存在得識別特定個人之可能性包括[196]：（1）影響重新識別風險之因素，包括揭露程度、匿名化程度、其他相關資訊可用性及接收方重新識別之能力及動機等（2）評估重新識別風險之測試，組織得運用「有心侵入者測試」（motivated intruder test）判斷匿名化資料是否得透過動機、一般能力、公開資源（如網際網路等）重新識別特定個人（3）重新識別風險之管理，組織應確保資料確實匿名化，亦可考量採取其他適當措施降低重新識別風險，如透過具有法律拘束力之協議或政策、技術或物理措施。若組織欲重新識別特定個人，須取得當事人同意[197]。否則依 PDPA 第 9B 編有關未經授權重新識別匿名化資料之規定，將有相關處罰規定。

八、菲律賓

（一）　定義及效果

DPA 及 IRRDPA，均未針對假名化或匿名化予以特別規定。惟 NPC 轄管之隱私政策辦公室於 2017 年發布之第 2017-001 號諮詢意見，表示「匿名化資料」為個人資料經匿名化處理，不再具有識別性，因此非屬於 DPA 及 IRRDPA 之個人資料，當事人亦無法依 DPA 和 IRRDPA 規定對匿名化資料請求刪除[198]。又 NPC 於 2017 年發布之第 2017-23 號諮詢意見，表示依據 DPA 和 IRRDPA 規定，當個人資料被永久或暫時地轉換為非個人資料時，則例外允許延長資料之保存

196 *id.*
197 PDPC, *supra* note 195.
198 NPC, *PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-001 4*, Jan. 5, 2017, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-001.pdf (last visited Dec. 3, 2021).

期間，其中「永久轉換為非個人資料」即指匿名化資料，「暫時地轉換為非個人資料」則為假名化資料[199]。因此匿名化資料應無 DPA 及 IRRDPA 適用，而由於假名化資料仍有間接識別性，屬於個人資料，故應適用 DPA 及 IRRDPA 之規範。

（二）　管理規範

NPC 於 2018 年發布第 2018-068 號諮詢意見中，表示匿名化程度須依個案分析判斷[200]，如單純刪除部分識別符號，並不足以確保任何人均無法重新識別特定個人[201]。而 NPC 於 2017 年發布之第 2017-31 號諮詢意見，則表示將個人資料以電子金鑰加密後進行傳輸，僅能透過電子金鑰開啟以重新識別當事人，因此屬於假名化技術，仍應符合 DPA 及 IRRDPA 之規定[202]。

關於匿名化資料之管理規範，NPC 於第 2017-31 號諮詢意見表示處理程序，得依照 ISO/IEC 29100 所訂之標準化作業流程辦理，控管者得取得 ISO/IEC 29100 認證作為有妥善管理之佐證[203]。又依 NPC 於 2019 年發布之第 2019-032 號諮詢意見，須事先將匿名化處理之詳細流程向當事人告知[204]。另依 NPC 於 2019 年發布之第 2019-036 號諮詢意見，針對匿名化資料的共享及委託第三人處理，仍宜由雙方

---

199 NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-23 8, June 21, 2017, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-023.pdf (last visited Dec. 3, 2021).

200 NPC, *PRIVACY POLICY OFFICEADVISORY OPINION NO. 2018-068 3*, Nov. 20, 2018, www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/v1[Redacted]%20Advisory%20Opinion%20No.%202018-068.pdf (last visited Dec. 3, 2021).

201 *id.* at 2-3.

202 NPC, *PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-31 4*, June 28, 2017, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-031.pdf (last visited Dec. 3, 2021).

203 *id.*

204 NPC, *PRIVACY POLICY OFFICEADVISORY OPINION NO. 2019-032 2*, Sep. 12, 2019, www.privacy.gov.ph/wp-content/files/attachments/advopn/2019/AdOps_2019-032.pdf (last visited Dec. 3, 2021).

訂定資料共享協議，以便確認權利義務關係[205]。

貳、我國規定

去識別化依照資料加工程度所呈現之狀況，區分為「匿名化」、「假名化」。「去識別化」並非我國個資法之法律用語，將個人資料去識別化之行為應定性為個資法第 2 條第 4 款之「處理」行為（參照法務部 107 年法律字第 10703512280 號函），至於去識別化後之結果為「匿名化」或「假名化」，亦非我國個資法之法律用語。我國個資法涉及個人資料去識別化行為之規定，於個資法第 6 條第 1 項第 4 款、第 9 條第 2 項第 4 款、第 16 條但書第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項但書第 5 款均有「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」之規定，作為學術研究之合法要件。

蒐集去識別化資料依個資法第 9 條第 2 項第 4 款規定，得免為向當事人告知個人資料來源及第 8 條所列事項。參照法務部 103 年法律字第 10303513040 號函有認為「如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自無個資法之適用」。此一見解結合個資法施行細則第 3 條及第 17 條規定，得推敲去識別化為「針對所保有的個人資料，運用代碼、匿名、隱藏部分資料或其他相類之技術，將個人可識別資訊予以去除，而達到無從直接識別特定之個人，並且也無法透過與其他資料對照、組合、連結等相類方式，進而識別出特定之個人。」，此種解釋較相近於匿名化之概念。復參照最高行政法院 106 年判字第 54 號判決認為「無從識別特定個人」係以「完全切斷資料內容與特定主體間之連結線索」程度為判準，若資料收受者掌握還原資料與主體間連結之能力，則不符合去識別化

---

[205] NPC, *PRIVACY POLICY OFFICEADVISORY OPINION NO. 2019-036 4*, July 3, 2019, www.privacy.gov.ph/wp-content/files/attachments/advopn/2019/v1[Redacted]%20Advisory%20Opinion%20No.%202019-036.pdf (last visited Dec. 3, 2021).

標準。

我國個資法未明文規範去識別化之管理措施，惟經濟部標準檢驗局已公布國家標準 CNS29100-2「資訊技術－安全技術－個人資訊去識別化過程管理系統」以及 CNS29191「資訊技術-安全技術-部分匿名及部分去連結鑒別之要求事項」，並委由財團法人台灣電子檢驗中心進行驗證，且研訂「個人資料去識別化過程驗證要求及控制措施」，作為去識別化具體要求及控制措施之參考。參照法務部 105 年 1 月公務機關利用去識別化資料之合理風險控制及法律責任之研析報告，認為驗證功能得協助證明機關並無違反個資法之主觀故意或過失，並已採行適當安全維護措施，且個人資料遭到違法蒐集或利用，並非因機關違反個資法所致。又倘資料接收者嗣後運用特殊罕見之技術或方法進行重新識別而取得個人資料，仍須符合個人資料蒐集、處理或利用之要件，如有違反則係違法之蒐集行為。

參、分析與小結

一、 比較法之分析

（一） 有關匿名化之相關規範探討

1. 法律效果及定義

綜觀各國法制，多數國家認為個人資料經匿名化後，已不具可識別性，故非屬個人資料，因此排除個資法之適用。惟歐盟強調資料匿名化仍應考量合理運用，包括所有客觀因素、識別所耗費之成本及時間、當時技術及科技發展。而日本則允許依一定程序予以匿名加工後之資料，得不經當事人同意作目的外利用或提供予第三人。

針對匿名化之定義，目前歐盟、英國、德國、美國及日本均有明文規定，而新加坡、菲律賓則透過主管機關解釋。經綜整各國有關匿名化之定義，係指「個人資料經加工處理須達到以合理手段均無法識別特定個人之程度，且無法復原者」，故主要可分為「處理」、「合理性」、「無法識別」、「無法復原」四個要件。

另所謂「無從識別特定個人」之判斷標準，日本有採「一般人基準說」，以一般人為基準，判斷其有無「其他資訊」作組合、比對之可能；或採「提供人基準說」，認為「其他資訊」不應僅限於一般人容易獲得之資料，在具體事件上於判斷組合、比對之可能性時，雖僅為一定範疇之關係人可能知悉、保有之其他資訊，亦應納入考慮。英國及新加坡則採「有心侵入者測試」，當非具有專業電腦知識或技術之侵入者有動機嘗試時，是否可能成功地再識別。若未能達到標準，則並非法律上之匿名化。

表 25 各國有關匿名化之要件

	名稱	處理	合理性	無法識別	無法復原
我國	去識別化	O		O	
歐盟	匿名化	O	O	O	O
德國	匿名化	O	O	O	O
英國	匿名化	O	O	O	O
美國 UPDPA	去識別化	O	O	O	
美國 CCPA	去識別化	O	O	O	
美國 HIPAA	去識別化	O	O	O	
日本	匿名化	O		O	O
韓國	匿名化	O	O	O	
新加坡	匿名化	O		O	
菲律賓	匿名化	O		O	O

資料來源：本計畫研究團隊自行整理

2. 管理規定

首先針對匿名化之加工方式，歐盟第 29 條資料保護工作小組曾指出，無論對資料控管者或接收者而言，若不刪除原始資料，無論資料經何種程度之處理，皆排除構成匿名資料之可能，且須達到盡一切現今合理可能之手段，均無法回復原狀之程度。惟歐盟強調技術中

立，考量因各種資料屬性不一，不同資料有不同的應用領域與利用可能性，對個人隱私的侵害程度不盡相同，故難以概念式地制定加工方式。日本則考量匿名化之加工方式涉及技術面問題，在法制設計上先由法律確立原則性加工方式及一般通用性標準，再由個人資料保護委員會訂定法規命令揭示具體之加工方式。

其次，針對匿名化資料之管理措施，由於歐盟將匿名化視為風險管理技術，故未規定匿名化之管理措施。美國、日本則明定於個資法，英國、新加坡、菲律賓則透過主管機關解釋。觀察各國規定，管理措施主要可分為授權及監督責任、風險評估、制定處理規範及防止事故等類型。此外，日本另要求應建立申訴對應處理機制，以提供當事人救濟之管道。

表 26 各國有關匿名化之管理措施

		授權及監督責任	風險評估	制定處理規範	防止事故	其他
歐盟			O			
德國			O			
英國		O	O	O	O	員工培訓
美國	UPDPA					
	CCPA				O	
	HIPAA					
日本		O		O	O	申訴機制
韓國						
新加坡			O			
菲律賓						ISO 29100

資料來源：本計畫研究團隊自行整理

最後，有關匿名化資料之義務要求，考量由於經匿名化之資料仍可能會因情境變化而得以重新識別特定個人，故多數國家均課予禁

止重新識別之義務；美國 CCPA 規定去識別化資料須限於特定目的利用，且企業應公開承諾或以契約方式遵守去識別化程序；日本則由於強調匿名化過程之透明性，故要求須公告其事業名稱、施作對象之個人資料類型、匿名化項目及利用目的，並向第三方明示所提供為匿名化資料。

表 27 各國有關匿名化之義務要求

		禁止重新識別	特定目的利用	其他
歐盟		O		
德國		O		
英國		O		
美國	UPDPA	O		公開承諾、契約
	CCPA	O	O（研究）	
	HIPAA			
日本		O		公告義務、向第三方明示
韓國				
新加坡		O		
菲律賓				

資料來源：本計畫研究團隊自行整理

（二）　有關假名化之相關規範探討

1. 法律效果及定義

綜觀各國法制，由於個人資料假名化仍可能與其他資料比對而得識別特定個人，屬於間接識別之個人資料，故仍應適用於個資法。因此針對個人資料經假名化之法律效果，有採利用目的得放寬如美國、日本；有採個人資料發生事故時得免除通知義務如歐盟、英國、德國、日本、韓國；有採排除當事人行使權利如歐盟、美國、日本、韓國；或排除個資法適用如菲律賓；尚有採免除保存期限銷毀義務如

韓國。

針對假名化之定義，目前歐盟、英國、德國、美國、日本、韓國均有明文規定，新加坡、菲律賓則透過主管機關解釋，其中新加坡將假名化例示為匿名化加工方式之一，故概念未特別區分。經綜整各國有關假名化之定義，係指「個人資料經加工後，非與其他資料比對無法識別特定個人」，由於不同匿名化要求去識別化達到無法復原之程度，故主要可分為「處理」、「無其他資料」、「無法識別」三個要件。

表 28 各國有關假名化之要件

		處理	無其他資料	無法識別
歐盟		O	O	O
德國		O	O	O
英國		O	O	O
美國	UPDPA	O		O
	CCPA	O		O
	HIPAA			
日本		O	O	O
韓國		O	O	O
新加坡				
菲律賓		O		

資料來源：本計畫研究團隊自行整理

2. 管理規定

首先針對假名化之加工方式，歐盟第 29 條資料保護工作小組例示假名化得使用加密、雜湊函數、記號化之加工方式，惟強調技術中立，故未明文予以規定。而日本、韓國考量假名化之加工方式涉及技術面問題，故在法制設計上確立原則性加工方式及一般通用性標準，規定應刪除或替換個人資料中之記述或符號，日本另要求應刪除或替換可能因非法使用所造成財產損失之記述。其他國家則係透過主

管機關解釋，提供假名化加工方式之例示說明。

其次，針對假名化資料之管理措施，目前歐盟、美國、日本、韓國均有明定於個資法，要求應對假名化資料採行適當之安全管理措施。觀察各國規定，多數國家均要求假名化資料應與原始資料分別管理，應明確資料控管者權限及責任、建立管理制度及改善評估、防止無權近用等措施。另外韓國要求個人資料進行假名化程序時，應依規定填載目的，並保存相關文件管理紀錄。

表 29 各國有關假名化之管理措施

		資料分別管理	授權及監督責任	建立管理制度	防止事故	其他
歐盟		O		O		原始資料須加密
德國		O		O		
英國		O		O		
美國	UPDPA					
	CCPA	O				
	HIPAA					
日本			O	O	O	
韓國		O			O	保存紀錄
新加坡						
菲律賓						

資料來源：本計畫研究團隊自行整理

最後有關假名化資料之義務要求，歐盟認為假名化資料屬於間接識別之個人資料，因此仍適用個人資料之相同規定。惟考量假名化資料仍有間接識別之風險，故多數國家均課予禁止重新識別之義務；美國、韓國則限制假名化資料須於特定目的內利用；日本由於強調假名化資料係為供事業內部分析用途，故禁止目的外利用或提供予第三方，並禁止利用聯絡資訊，且仍課予須將利用目的公告之義務。

表 30 各國有關假名化之義務要求

		禁止重新識別	特定目的利用	其他
歐盟				
德國				
英國		O		
美國	UPDPA	O		
	CCPA	O	O（研究）	
	HIPAA			
日本		O		禁止目的外利用或提供第三方、公告義務、禁止利用聯絡資訊
韓國			O（科學研究）	
新加坡				
菲律賓				

資料來源：本計畫研究團隊自行整理

二、 小結

綜上所述，去識別化結果依照資料加工程度所呈現之狀況，區分為「匿名化」、「假名化」。綜觀各國法制，歐盟、德國、英國將匿名化、假名化視為資料處理之適當保護措施，鼓勵產業應用該措施，惟強調技術中立，故不以法律干預；美國、日本、韓國為供產業應用去識別化資料，針對去識別化訂有經常性可被使用之匿名化加工方式的相關規定（泛用性規定），使產業得以遵循。而新加坡將假名化例示為匿名化加工方式之一，故無假名化之相關規範；菲律賓則建議以 ISO/IEC 29100 標準處理。

由於去識別化在大數據時代有其重要性，匿名化及假名化應採用何種標準作業流程，有效評估並控制被再識別之風險為此議題核心。考量匿名化資料隨著時間及科技發展，使特定個人身分被重新識

別之風險大幅提升，因此應建立假名化制度，作為企業得利用資料之方式之一。不論匿名化或假名化，均應建立一套管理制度，包含一般通用性之加工方式、安全管理措施及禁止義務，使控管者得以遵循相關規定。至於匿名化或假名化之法律效果，由於難以確保對當事人毫無風險，故是否得以排除個資法之適用仍有疑慮，惟得透過一定程序之驗證後，使資料得排除特定法規限制，而原則上仍應受到個資法之適度規範。

第六節　當事人權利

第一項 資料可攜權

壹、比較法國家

一、歐盟

（一）　有關資料可攜權之規範

GDPR 第 20 條第 1 項賦予當事人具有資料可攜之權利（right to data portability），亦即當事人應有權利從資料控管者取得與其相關的個人資料，並在不受原資料控管者阻礙下，得以將該資料傳輸予其他資料控管者。又同條第 2 項延伸此權利之範圍，即當技術允許時，當事人有權要求原資料控管者直接將其個人資料傳輸予其他資料控管者。由於可攜權亦旨在促進資料控管者間資料無阻礙傳輸，故當事人所接收的個人資料，在形式上應具備結構性、通用性及機器可讀性（structured, commonly used and machine-readable format）。

有關可攜權之行使要件，依 GDPR 第 20 條第 1 項規定，僅限於當事人同意或履行契約為合法處理要件時，且以自動化模式處理資料為必要。依照 GDPR 前言第 68 點強調，除同意與履行契約之情形外，以其他合法處理要件處理資料則並無可攜權之適用，且可攜權亦不適用於資料控管者處理公共事務之情形。惟可攜權並非絕對之權利，依 GDPR 第 20 條第 3 項規定可攜權之行使不得優先於刪除權，並於符合公共利益執行職務或委託資料控管者行使公權力而有必要

者，例外限制不得行使可攜權。又同條第 4 項規定可攜權之行使不得影響他人權利與自由，以避免可攜權之行使對第三方造成傷害。

（二）　產業應用

2021 年 EC 會議及工作坊討論 GDPR 從 2018 年正式施行以來有關可攜權之實施情形，其優點包含促進產品創新、促進市場公平競爭、增加以資料所賺取的商業利益、當事人可選擇將資料與小型公司分享防止資料被大型科技巨頭掌握[206]；並彙整出六種常見實施可攜權的障礙[207]，（1）資料並未以機器可讀性之格式傳輸；（2）在技術方面及資訊安全風險上極難提供資料；（3）透過資料夾所提供之資料不實用或不完整；（4）資料之提供超過法定期限；（5）當事人行使可攜權的經驗落差大，許多企業會向當事人索取更多資訊，欲使當事人放棄繼續行使可攜權；（6）企業認為當事人可攜權之請求極為繁瑣，有些企業直接向當事人提出刪除帳號的方案，而非確實行使可攜權。

目前歐盟主要落實可攜權於數位金融，以促進開放銀行之發展，並於 2018 年實施《支付服務指令 2》（Payment Services Directive, PSD2）。PSD2 規定當當事人提出請求時，強制要求所有歐盟銀行必須傳輸當事人之金融資料予第三方服務業者（third party providers），或者經當事人認證及同意後，由第三方服務業者負擔傳輸之成本費用[208]。因此 PSD2 係使消費者得將資料以數位化方式傳輸於銀行與第三方服務業者之間，且銀行必須採用適當的技術措施確保消費者可

206　EUROPEAN COMMISSION [EC], *JRC Conference and Workshop Report, Unfolding opportunities form the use of APIs in Europe* (2021), https://publications.jrc.ec.europa.eu/repository/handle/JRC124758, at para 2.1.2 (last visited March 16, 2022).

207　*id*. at para 2.1.2.

208　DEUTSCHE BANK, *PSD 2, open banking and the value of personal data* (2018), https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000471102/PSD_2%2C_open_banking_and_the_value_of_personal_data.pdf?undefined&realload=2pyvxUlrP29v~ns0a~dqPkVc0prVE/hRiuLLPpnfPruj4W6MNlPtoAzjc/bZpOMh, at 1　(last visited March 16, 2022).

以行使其資料主權，將資料傳輸行為附加經濟價值[209]。

二、英國

（一）　有關資料可攜權之規範

英國沿用歐盟 GDPR 對可攜權之規定，依 UK GDPR 第 20 條第 1 項，資料可攜權係指當事人有權以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並有權將之傳輸給其他控管者，且不受控管者之妨礙。又依同條第 2 項規定，當技術許可時，當事人亦有權使個人資料由一控管者直接傳輸予其他控管者。而可攜權之行使要件，其一為控管者取得個人資料的方式須基於當事人之同意或依契約之方式；其二為控管者須以自動化方式處理資料之情況。但可攜權於例外情形得予以限制，依同條第 3 項規定可攜權之行使不得優先於刪除權（被遺忘權），又同條第 4 項規定可攜權之行使不得影響他人之權利自由。另 DPA 2018 亦配合 UK GDPR 可攜權之規定，針對可攜權之限制於 DPA 2018 附件二[210]第 28 條第 1 項及第 2 項規定，當行使權利可能阻止或嚴重損害公共利益目的實現時，基於公共利益之存檔目的所處理之個人資料將無法行使該權利。

（二）　產業應用

英國商業創新技術部（Department for Business, Innovation & Skills；BIS）於 2011 年宣布進行自願性的「midata 計畫」[211]，係政府與重點企業及消費者團體所共同展開的一項計畫，旨在讓消費者能夠以可攜式及電子格式近用其個人資料，並助於消費者了解自身消費行為及模式，以做出更明智且合適的消費決策[212]。2014 年對於

209　*id*. at 3-4.

210　Data Protection Act 2018 SCHEDULE 2, LEGISLATION.GOV.UK, https://www.legislation.gov.uk/ukpga/2018/12/schedule/2 (last visited Mar. 21, 2022).

211　The midata vision of consumer empowerment, GOV.UK, https://www.gov.uk/government/news/the-midata-vision-of-consumer-empowerment (last visited Mar. 16, 2022).

212　DEPARTMENT FOR BUSINESS INNOVATION & SKILLS[BIS], *midata*

能源、個人經常性帳戶、信用卡、手機等領域的進展發表本計畫的檢視報告，要求銀行、能源公司及電信業提供消費者更高的資料近用權利[213]。又 2020 年英國數位文化傳媒及體育部（Department for Digital, Culture, Media & Sport；DCMS）發佈國家資料戰略（National Data Strategy），將智慧資料（Smart Data）視為重點舉措，即根據客戶要求得與授權第三方供應商安全共享客戶資料[214]。另目前英國對開放銀行採取強制管制模式，2016 年競爭與市場管理局（Competition and Markets Authority；CMA）設立「開放銀行推動小組」（Open Banking Implementation Enitity；OBIE），並發布《開放銀行標準》（Open Banking Standard）對所有帳戶提供者（ASPSPs）開放，並已在 90%的英國支付帳戶市場實施[215]。

三、德國

（一）　有關資料可攜權之規範

德國 BDSG 亦同英國沿用 GDPR 對可攜權之規定，即在符合法定要件時，當事人得自由地選擇是否攜帶其資料予特定業者，以便於在不同服務供應業者之間轉換服務。在德國聯邦資料保護暨資訊自由機關（Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI）於 2020 年發布之「GDPR—BDSG 之內容與解釋」（DSGVO – BDSG Texte und Erläuterungen）手冊，表示可攜權對於特定領域之傳統業者非常重要，例如銀行業者或保險業者等，

---

company briefing pack (2012), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/34747/12-983-midata-company-briefing-pack.pdf (last visited Mar. 16, 2022).

213 BIS, *Review of the midata voluntary programme* (2014), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf (last visited Mar. 16, 2022).

214 Policy paper National Data Strategy, GOV.UK, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy (last visited Mar. 21, 2022).

215 Welcome to the Open Banking Standard, OPEN BANKING, https://standards.openbanking.org.uk/ (last visited Mar. 16, 2022).

由於過去受限於高密度監管要求，應以封閉方式傳遞或處理個人資料，但可攜權得在符合一定條件下打破相關封閉式的資料流通限制[216]。又 2018 年德國聯邦資訊技術安全局（Bundesamt für Sicherheit in der Informationstechnik, BSI）發布之「保持安全：加密作為安全數位化的基礎」（Mit Sicherheit: Verschlüsselung als Grundlage für eine sichere Digitalisierung）提及，在依據 GDPR 第 6 條第 1 項第 a 款經取得當事人之同意，或同項第 b 款履行契約之情形，在自動化程序處理個人資料之條件下，除有損害他人自由及權利、為履行公共利益目的之任務，或法律賦予 BSI 得排除可攜權之情形外，當事人得行使資料可攜的權利，要求業者以通用、機器可讀取之格式，提供予當事人指定之第三方[217]。

（二）　產業應用

2017 年德國聯邦內政部（Bundesministerium des Innern, BMI）發布「在資料安全下新的同意方法—技術、法律及經濟挑戰」（Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen），指出為安全且合法地處理個人資料，得透過系統提供使用者自主管理的介面，以便其隨時更改、修正或拒絕同意，亦助於使用者行使撤銷權或資料可攜的權利[218]。以德國數位金融服務供應商而言，其透過清楚明列接收個人資料之類別，包

---

216 Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [BfDI], *Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterung* (2020), S. 60-61, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf;jsessionid=CF855B1389AB879E987D57A3812BEF42.intranet241?__blob=publicationFile&v=9 (last visited Mar. 1, 2022).

217 Bundesamt für Sicherheit in der Informationstechnik [BSI], *Mit Sicherheit: Verschlüsselung als Grundlage für eine sichere Digitalisierung* (2018), S. 62, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_02.pdf?__blob=publicationFile&v=1 (last visited Mar. 1, 2022).

218 Bundesministerium des Innern [BMI], *Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen* (2017), S.4.13, https://pdffox.com/download/neue-wege-bei-der-einwilligung-im-datenschutz-pdf-free.html (last visited Mar. 1, 2022).

含保險公司、中介商、金融數位服務母公司、信貸及投資公司、律師、會計師、聯邦金融監督局（Bundesanstalt für Finanzdienstleistungsaufsicht, BaFin）以及社會保險機構（Sozialversicherungsträger）等單位，透過一一列舉方式來取得當事人的同意；如當事人欲行使可攜權將個人資料傳遞予特定第三方，則其根據當事人要求，將個人資料透過結構化、通用格式及機器可讀取之形式提供予當事人[219]。

四、美國

（一）　有關資料可攜權之規範

CCPA 第 1798.100 條第 d 項有關資料「知的權利」（right to know）已包括可攜權之內涵。該規定要求當營利事業被經驗證的消費者請求提供其個人資料時，應以可攜之電子形式提供，且如技術許可，則應以通用形式使消費者可無障礙將資料傳輸至其他實體。而後 CPRA 第 1798.130 條第 a 項第 3 款第 B（iii）點增加消費者在不同營利事業間的資料便攜性：當營利事業提供消費者其特定個人資料時，必須在對消費者而言易懂、技術可行的前提下，以結構性、通用性、機器可讀性之形式提供。因此 CPRA 對於可攜權之行使要件有二，其一係消費者須為加州居民；其二係消費者須經過身分驗證，依 CPRA 第 1798.130 條第 ak 項係指由消費者、消費者代表其未成年子女、經消費者授權之代理人或消費者之監護人提出之請求，並由營利事業以商業上合理方式，或檢察長依 CPRA 第 1798.185 條第 a 項第 7 款採用之相關規定，驗證確實為營利事業蒐集個人資料來源之消費者。而 UPDPA 於第 5 條知的權利僅賦予當事人得請求製給複製本，並未包含可攜權之規定。

219　Finanz-service.digital, https://www.finanz-service.digital/dateneinwilligungserklaerung/ (last visited Mar. 1, 2022).

（二）　產業應用

CCPA 及 CPRA 的可攜權係一般性規定，並無對特定產業予以規範。而美國聯邦法律層級方面雖無可攜權之規定，但《公平信用報告法》（Fair Credit Reporting Act, FCRA）對涉及消費者信用的金融機構（Credit Reporting Agencies, CRAs）提供及使用信用資料、消費者信用報告（consumer report），依 FCRA 第 610 條規定，揭露須以書面為之，或經消費者授權以書面以外形式提供。另在醫療領域，HIPAA 針對電子化醫療資訊之標準格式、交換機制及資料保護進行規範，依 HIPAA 第 164.524 條第 c 項第 2 款規定，經個人要求，受規範機構必須以個人要求之形式提供其受保護的健康資料(Protected health information, PHI)，如不能輕易產製該形式之 PHI，仍須以雙方同意的機器可讀形式提供。

五、日本

（一）　有關資料可攜權之規範

日本個人資料保護委員會於 2019 年 4 月 25 日公布之「個人資料保護法 關於所謂的三年一次修正」（個人情報保護法 いわゆる 3 年ごと見直しに係る 検討の中間整理）[220]，討論日本個資法第 33 條開示請求權具有之可攜性（ポータビリティ），類似 GDPR 之可攜權。依第 33 條第 1 項規定，當事人對個人資料處理事業得依照個人資料保護委員會所訂定之規則，請求公開保有得識別該當當事人個人資料之電磁紀錄。同條第 2 項規定，如依照當事人要求之方式提供電磁紀錄有所需費用過高等困難，則亦得交付書面；除非有侵害當事人或第三人生命、身體、財產或其他權利利益之虞的情形，及顯然對該當個人資訊處理事業正常執行業務產生障礙或有違反其他法令之情

[220] 個人情報保護法 いわゆる 3 年ごと見直しに係る 検討の中間整理，個人情報保護委員会，平成 31 年 4 月 25 日，https://www.ppc.go.jp/files/pdf/press_betten1.pdf（最後瀏覽日：2022 年 3 月 1 日），頁 12 以下。

形，始得拒絕。

（二）　產業應用

日本在數位金融方面有實施資料銀行，乃是為了促進當事人參與其資料的流動、強化當事人對其個人資料的掌控所生的制度。資料銀行係由政府機關認定，需符合一定要求始能通過其認定，以利消費者能夠安心地使用該等服務[221]。再者，另有實施 my portal 制度，即利用日本的 my number 卡作為身分驗證，即可線上辦理相關行政事務，並得確認健保醫療資訊等，且亦可設定與外部網站（如民間企業網站等）連線，向其提供當事人在 my portal 的相關資訊[222]。此外，日本總務省針對電話號碼訂有「手機・PHS 號碼可攜權實施之指引」（携帯電話・PHS の番号ポータビリティの実施に関するガイドライン）[223]，助於消費者更換其手機電信業者時，得順利地將原本的電話號碼移轉至其他手機業者。

六、韓國

（一）　有關資料可攜權之規範

由於現行韓國個資法並未明文規範當事人具有資料可攜權，惟考量新興技術的發展、強化數位時代的公民隱私權，並提升韓國公民作為當事人的權利，於 2021 年 9 月 28 日提出「個人資料保護法修正草案」[224]（下稱「修正草案」），目前仍在國會審議中。於修正草案

221　総務省，情報信託機能の認定スキームの在り方に関する検討会，情報信託機能の認定に係る指針 Ver2.1，令和 3 年 8 月，https://www.soumu.go.jp/main_content/000764120.pdf（最後瀏覽日：2022 年 3 月 15 日）。

222　マイポータル，https://myna.go.jp/（最後瀏覽日：2022 年 3 月 15 日）。

223　総務省，携帯電話・PHS の番号ポータビリティの実施に関するガイドライン，令和 2 年 12 月 18 日最終改正，https://www.soumu.go.jp/main_content/000775806.pdf（最後瀏覽日：2022 年 3 月 15 日）。

224　디지털 시대 「개인정보 보호법」 개정안

第 35 條之 2 明定可攜權，乃為確保當事人對其個人資料的自主權，當事人可要求資料控管者將其個人資料傳輸給當事人或其他個人資料控管者、個人資料管理專門機構。而可攜權之適用範圍僅限於取得當事人同意或依契約為合法處理要件的情形，當當事人要求傳輸時，以合理的時間、成本及技術可行的情況下，資料必須以具備結構性、通用性、機器可讀性之形式傳輸，且不得侵害他人權利或利益。

（二）　產業應用

韓國於「信用資料使用及保護法」（Use and Protection of Credit Information Act, Credit Information Act）先引入「資料可攜權」的概念[225]，提供金融消費者得移轉個人信用資料的權利，作為韓國政府發展「My Data」的基石。又於 2018 年 6 月第四屆工業革命網絡國家論壇通過「資料產業振興戰略」[226]，推出「My Data 試行計畫」，聚焦金融、醫療、電信等領域，並於同年 7 月宣布「MyData 發展計畫」，首先將適用範圍限縮在個人資料信用管理業務[227]，期望透過金融業施行「MyData」經驗作為其他行業參考範例。又個人資料管理業務採行許可制度，除設有最低資本額限制及責任保險要求，加入「MyData」試辦的企業尚需具備個人資料保護制度，以確保制度順利推行。

국회제출，個人資料保護委員會，https://www.pipc.go.kr/（最後瀏覽日：2022 年 3 月 15 日）。

225 신용정보의 이용 및 보호에 관한 법률，https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&query=CREDIT%20INFORMATION%20USE%20AND%20PROTECTION%20ACT#liBgcolor0（最後瀏覽日：2022 年 3 月 15 日）。

226 데이터 산업 활성화 전략，https://www.4th-ir.go.kr/article/detail/277?boardName=internalData&category=relation（最後瀏覽日：2022 年 3 月 15 日）。

227 個人資料信用管理業務包含信用資料查詢，以及信用資料、帳戶管理及第三方諮詢與代管業務。

七、新加坡

（一）　有關資料可攜權之規範

PDPA 修正後新增資料可攜之規範，強化消費者對其個人資料的自主權，惟目前尚需待相關條例公布後始生效，且考量資料可攜為較新概念，故預計將採階段性實施。依據 PDPA 第 26H 條第 1 項之規定，資料可攜係指個人得向組織提出資料移轉請求，請求組織將資料移轉至其指定之個人或其他接收組織。有關資料可攜之行使要件，依第 26F 條規定，僅適用於組織收到資料移轉請求時，應以電子形式提供資料；及組織於收到資料移轉請求時，應於期限內蒐集或建立適用資料之情形。另在 PDPA 附表 12 提及資料可攜之例外規定，若組織合理預期資料傳輸將可能造成當事人以外之個人安全或身心健康之威脅或嚴重傷害、違反國家利益；或是接收資料傳輸之組織屬於被規定為排除接收組織之類別；或經 PDPC 指示組織不得傳輸資料。

（二）　產業應用

新加坡金融管理局（Monetary Authority of Singapore, MAS）及智慧國家暨數位政府集團（Smart Nation and Digital Government Group, SNDGG）於 2020 年 12 月 7 日啟動「新加坡金融資料交換」（Singapore Financial Data Exchange, SGFinDex）制度，使民眾得將其金融資訊整合，以便進行更有效之理財規劃。SGFinDex 係根據「金融計畫數位服務」（Financial Planning Digital Services , FPDS）而生，作為全球第一個使用國家數位身分（Singapore's National Digital Identity，又稱 SingPass）與集中管理的線上同意系統的公共數位基礎設施，由公共部門與新加坡銀行協會及七家參與銀行共同合作開發，使個人得透過應用程式存取在不同政府機構及金融機構持有的金融資訊。

八、澳洲

（一）　有關資料可攜權之規範

澳洲於2019年8月1日通過《2019年消費者資料權法》(Treasury Laws Amendment（Consumer Data Right）Act 2019)，增訂「消費者資料權」(Consumer Data Right, CDR）相關規定，賦予消費者資料權具有聯邦層級之法律地位，並建立消費者權利資料可攜制度。依本法第56條第AA項係使受指定行業的消費者得安全、效率且便利以請求揭露其消費者資料予消費者自身或適格者(Accredited person)，並使任何人均能有效且方便得近用該指定行業內關於商品或服務之資料，進而建立創新、多元選擇與良性競爭的消費環境。依同條第AC項規定財政部長得在「澳洲競爭與消費者委員會」(Australian Competition and Consumer Commission, ACCC）及「澳洲資訊委員公署」(Office of the Australian Information Commissioner, OAIC）的協助下，指定國內特定行業適用CDR相關規定。關於行使CDR之主體依同條第EA項包含個人與法人團體（bodies corporate)，依同條第AI項第3款規定係因產品或服務之提供而可透過消費者資料識別或可合理識別該特定人或與該特定人有關聯之人（例如家庭成員)。而消費者資料依同條第AI項第1款規定，係指經財政部長依法指定行業的資料種類及其衍生資料，又依《2020年消費者資料權規則》（Competition and Consumer（Consumer Data Right）Rules 2020）第3.2條規定包含客戶資料、帳戶及交易資料。

依本規則敘明三種請求消費者資料之方式：(1)「商品資料請求」(Product Data Reguests)，依本規則第2章係指任何人均得要求資料控管者揭露由其所提供之CDR商品資料，並須以機器可讀形式（Machine-readable Form）提供予資料請求人，且不得對資料之使用附加任何條件或限制；(2)「CDR消費者請求其消費者資料」(Consumer Data Requests Made by CDR Consumers)，依本規則第3章係指消費者得要求資料控管者揭露與其有關之CDR資料，並應提供特定線上服務管道供消費者可直接請求，且應以一般人可讀形式

（Human-readable Form）提供予資料請求人；(3)「消費者授權他人請求消費者資料」(Consumer Data Requests Made on Behalf of CDR Consumer)，依本規則第 4 章規定消費者得授權適格者要求資料控管者揭露 CDR 資料，並應以機器可讀形式提供予適格者；該請求應遵循「最少資料蒐集原則」(Data Minimization Principle)，亦即僅蒐集或使用為提供服務或商品所必須之 CDR 資料。OAIC 於《隱私保護措施指引》(Privacy Safeguard Guidelines) 表示，取得消費者的明確同意是適格者蒐集、利用消費者資料的唯一法律基礎[228]。依本規則第 4.12 條規定，同意應符合自願、明示、知情之要件，並基於特定目的，而同意之效力最多僅持續 12 個月，且依本規則第 4.13 條消費者得隨時撤回其同意。另關於認證制度，除依本法第 56 條第 CA 項第 1 款規定，ACCC 於《消費者資料權認證指引》(Consumer Data Right accreditation guidelines) 亦表示，在 CDR 體系下任何人均須經 ACCC 認證，包括資訊安全相關措施、爭端解決程序與保險等項目是否通過認證，始得於消費者同意後自資料控管者接收資料[229]。

（二）　產業應用

澳洲首先指定與民生經濟密切相關之銀行業試行「開放銀行」[230]制度，第一階段自 2020 年 7 月起，由澳洲市占率高達 75%[231]以上之四大銀行優先試行[232]；第二階段於 2020 年 11 月新增得請求抵押貸款及個人貸款之消費者資料；第三階段於 2021 年 7 月起實行在其他

---

[228] Office of the Australian Information Commissioner [OAIC], CDR Privacy Safeguard Guidelines, Chapter C, at 3.

[229] Australian Competition and Consumer Commission [ACCC], Consumer Data Right accreditation guidelines, at 4.

[230] 開放銀行主係指銀行資料透過應用程式介面（Application Programming Interface, API），在兩個或多個非關聯方之間共享，藉以增進金融市場功能。

[231] Australian Government Productivity Commission (ACCC), Competition in the Australian Financial System- Productivity Commission Inquiry Report, at 5.

[232] 消費者得要求澳洲國民銀行（National Australia Bank, NAB）、澳洲聯邦銀行（Commonwealth Bank of Australia, CBA）、澳盛銀行（Australia and New Zealand Banking Group Limited, ANZ）、西太平洋銀行（Westpac Banking, WBK），與適格之資料接受者共享該名消費者之信用卡、簽帳金融卡、存款帳戶及交易帳戶等消費者資料。

銀行[233]，並預計將自銀行業逐步推廣至能源與電信業[234]，而此項消費者資料權立法將使消費者能夠更容易接觸與掌握資料，降低消費者在產品與服務之間進行比較及轉換的障礙，同時能夠促使服務提供者間的競爭，為消費者帶來更具創新性的產品及服務。

貳、我國規定

我國個資法第 3 條賦予當事人就其個人資料得行使之權利有第 1 款「查詢或請求閱覽」及第 2 款「請求製給複製本」；又第 10 條規定「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益」。

實務有認為「本法第 3 條規定當事人查詢或請求閱覽、請求製給複製本係保障個人資料當事人對其個人資料之使用有知悉與控制權。當事人依本法第 3 條、第 10 條及第 11 條所得行使之權利，除有第 10 條或第 11 條所定之除外情形，自得依本法規定行使之。」（參照法務部 101 年 6 月 22 日法律字第 10103104090 號函釋、法務部 102 年 3 月 12 日法律字第 10100271950 號函釋）；又有認為「本法明文保障當事人對於保有其個人資料之公務機關或非公務機關，有查詢、請求閱覽或製給複製本之權利，係司法院釋字第 603 號解釋所揭示人民對其個人資料之使用有知悉與控制權之具體展現。」（參照法務部 102 年 7 月 4 日法律字第 10200118830 號函釋），然而所謂資料可攜權應具有取得及移轉之特性，且至少得請求以電子形式向當事人或第三方傳輸。惟目前尚難從我國個資法有關當事人權利之法條文義及相關實務見解推論當事人賦有得請求資料可攜之權

---

233 Consumer Data Right timeline update, ACCC, https://www.accc.gov.au/media-release/consumer-data-timeline-update (last visited Mar. 9, 2022).

234 預計於 2022 年 11 月起澳洲能源市場營運商、AGL Energy Group、Origin Energy Group 及 Energy Australia Group 持有的客戶資料得開始共享消費者資料。

利。

參、分析與小結

一、 比較法之分析

（一） 資料可攜權之形式

綜觀各國法制，多數國家對於資料可攜權之定義，係指當事人應有權要求以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並在不受原控管者阻礙下，有權將資料傳輸給其他控管者；而部分國家僅規定控管者提供電子形式及當事人得請求控管者將資料向其或第三方傳輸之權利，即認為屬資料可攜權。而日本之開示請求權雖賦予當事人，有權得向控管者請求以電磁紀錄方式提供個人資料，惟如同我國個資法之查詢或閱覽及複製請求權，僅限於向當事人傳輸之情形，並不具備移轉第三人及可攜之性質，故亦非等同於 GDPR 之資料可攜權。

表 31 各國有關資料可攜權之形式要件

		明文	形式			傳輸對象
			結構性	通用性	機器可讀性	
歐盟		O	O	O	O	當事人、第三方
英國		O	O	O	O	當事人、第三方
德國		O	O	O	O	當事人、第三方
美國	CCPA	O	O	O	O	當事人、第三方
	UPDPA	X	無規定			
日本		▲	X	X	O（電子形式）	當事人
韓國		O	O	O	O	當事人、第三方
新加坡		O	X	O	O	當事人、第三方
澳洲 CDR		O	O	X	O	當事人、第三方

資料來源：本計畫研究團隊自行整理

（二）　資料可攜權之規範

目前有明文承認資料可攜權之國家，對於資料可攜權之主要規範，分別對於資料可攜權之行使要件及例外限制予以不同程度之管制模式，得區分為三種立法例。

首先以歐盟 GDPR 體系國家（例如德國）、英國、韓國、新加坡之立法體例，對於資料可攜權之規範主要包括：（1）資料可攜權之請求範圍須為與當事人相關之個人資料，且係由當事人有意識且積極提供之資料，若控管者透過內部分析方法或演算系統，所衍生之資訊或模型等資料，則未包含在內；（2）資料可攜權之行使僅限於以同意或履行契約為合法處理要件的情形，且以自動化程序處理資料為必要，以其他合法處理要件處理資料則無資料可攜權之適用，亦不適用於資料控管者處理公共事務之情形；（3）針對資料可攜權之限制規定，包括不得妨礙刪除權之行使、行使時不得損害他人自由及權利、該權利不適用於符合公共利益執行職務或資料控管者受託行使公權力而為必要處理之情形。

其次，澳洲 CDR 則強調消費者資料權之行使要件僅限於同意，且接收方須取得澳洲競爭與消費者委員會之認證以符合適格性要求，包括隱私、資訊安全、爭端解決程序及保險等項目。

其三，美國 CCPA 乃一般性承認當事人具有知的權利，即包括資料可攜之權利，僅須經身分驗證為消費者本人或有權代表之人即可行使該權利。

另外在其他專業領域之資料可攜權制度，由於資料可攜權除了於一般性之個資法規定以外，澳洲 CDR 屬於競爭法領域之特別規定，並分別指定於金融、電信、能源業分階段逐步實施。亦有在金融領域實施開放銀行制度而另定特別法，如歐盟的支付服務指令（PSD2）、美國公平信用報告法（FCRA）；或是透過相關政策推動，如英國 midata、德國 LETsmart、日本資料銀行、韓國 My Data、新加坡之金融資料交換（SGFinDex），皆仍會輔以配套制度。資料可攜權

雖旨在強化當事人對其個人資料之掌控能力，並賦予當事人對其個人資料之運用有選擇權利；然於產業實務運作上，仍存在像是資料標準化機制之建置、自動化資料傳輸之管道等，在技術、資安、成本等各方面之挑戰，難以實現其資料可攜之目的。

二、 小結

綜上所述，由於我國個資法之當事人查詢或請求閱覽、製給複製本之權利，並未要求應以電子形式提供個人資料予當事人，亦未賦予當事人得將資料作移轉，甚或得請求原控管者將資料傳輸予其他控管者之權利，因此難謂有可攜之概念，故我國個資法尚未保障當事人具有資料可攜之權利。

參酌多數國家對於資料可攜權之規範，首先在形式要件上，資料應具備結構性、通用性及機器可讀性，且傳輸對象應包含當事人及第三方，始得達到可攜之目的。其次，在資料可攜權之行使要件上，歐盟 GDPR 體系強調應以當事人同意或履行契約作為合法處理要件，且以自動化程序處理為必要；澳洲 CDR 則強調消費者資料權應限於當事人同意，且接收方須取得適格性認證；美國 CCPA 則採一般性承認當事人均得行使資料可攜權。其三，對於例外情形得限制當事人行使資料可攜權之規定，歐盟 GDPR 體系以公共利益、他人自由及權利等類型為主；相對地，澳洲 CDR、美國 CCPA 則未作例外限制，對於符合行使要件之情形，即一般性承認當事人得行使資料可攜權。最後，由於資料可攜權應用領域廣泛，除了透過個資法作一般性規定外，亦有國家透過另定特別法或相關政策推動資料可攜制度，為避免實施上對於產業造成過大衝擊，亦可採取相應之配套制度。

第二項 被遺忘權

壹、比較法國家

一、歐盟

（一）　背景與定義

2014 年歐盟法院於 *Google Spain v AEPD and Costeja* 案首次承認被遺忘權，雖係針對 1995 年個人資料保護指令進行詮釋，但仍對 GDPR 產生莫大影響[235]。本案爭點為當事人有無直接向搜尋引擎請求刪除個人資料的權利，因其不希望個人資料公開於網路[236]。歐盟法院裁定被遺忘權存於歐盟法律中，並認為除有公共利益重要性高於當事人之隱私權時，始得捨棄被遺忘權[237]。

其後 EDPB 針對搜尋引擎提供者（search engine providers）執行被遺忘權之情形發布相關具體指引[238]，並影響後來 GDPR 的刪除權（right to erasure）又稱被遺忘權（right to be forgotten），規定於 GDPR 第 17 條第 1 項，當事人於特定情事下，有權要求資料控管者刪除其個人資料，控管者有刪除義務且不得無故拖延。如資料控管者已公開其個人資料，依 GDPR 第 17 條第 2 項規定，資料控管者考量現有技術及執行成本後，應採取合理措施通知其他資料控管者，當事人已行使被遺忘權應刪除任何與其個人資料相關之連結、複本或仿製。

（二）　相關規範

關於被遺忘權之行使要件規定於 GDPR 第 17 條第 1 項，當有符

---

235 Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, HUMAN RIGHTS LAW REVIEW, 14, 761, 762 (2014).

236 *Id*. at 765.

237 *Id*. at 765-766.

238 CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

合下列要件之一，當事人即得行使被遺忘權：

1. 依本項第 a 款規定當運用個人資料之特定目的已無必要，通常適用於個人資料已過時或長久未更新，如當事人的個人資料已從公共公開名冊中移除、組織官網於當事人離職後仍保留其個人資料等情形[239]。

2. 依同項第 b 款規定，當控管者採用同意作為資料處理之合法要件，而當事人撤回同意且無其他合法處理要件之適用。EDPB 於指引表示在實務上此情形較不常見[240]。

3. 依同項第 c 款規定，當事人針對 GDPR 第 6 條第 1 項第 e 款公共利益處理要件及同項第 f 款合法利益處理要件行使拒絕權，且控管者無法證明有其他重要的合法依據（overriding legitimate grounds）較當事人之權利、利益或自由重要。當進行衡平判斷時，應將當事人行使拒絕權之情境納入考量，如當事人是否為公眾人物、涉及之個人資料是否與當事人的專業形象無關但侵犯其隱私等[241]。

4. 依同項第 d 款規定，非法處理個人資料。對於「非法」之詮釋，首先應以 GDPR 第 5 條及第 6 條考量，如有違反 GDPR 以外之法規，亦屬「非法」，應由監管機關（supervisory authorities）以國內法及判例為基準客觀詮釋[242]。

5. 依同項第 e 款規定，因必須遵守歐盟或是歐盟會員國法律，控管者必須刪除個人資料，如控管者須配合禁制令刪除資料等[243]。

6. 依同項第 f 款規定，控管者依 GDPR 第 8 條第 1 項對未成年人提供資訊社會服務（information society services），EDPB 表示大部分

---

239 EUROPEAN DATA PROTECTION BOARD [EDPB], *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)* (2020), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en, at para 19-20 (last visited March 16, 2022).

240 *id*. at para 24.

241 *id*. at para 30, 32.

242 *id*. at para 35-36.

243 *id*. at para 38.

網路經濟活動服務均符合「資訊社會服務」之定義，包含免費網路服務、簽約網路服務、網路資訊提供服務、商業溝通服務、資料搜尋取得服務等[244]。搜尋引擎即屬「資訊社會服務」提供者，蓋如涉及未成年人資料則應刪除，GDPR 前言第 38 點及第 65 點均強調應保障移除未成年人個人資料之權利[245]。

而被遺忘權之限制規定於 GDPR 第 17 條第 3 項，當有下列情形之一，則無法行使被遺忘權：

1. 依同項第 a 款規定，資料傳輸係因落實言論自由、資訊取得自由之必要。EDPB 強調當事人之被遺忘權在一般情況下均較網路使用者取得資料之自由更為重要，惟搜尋引擎提供者仍得考量資料之性質、機敏性、對網路使用者資料取得自由之影響、當事人之公眾生活等因素[246]。

2. 依同項第 b 款規定，資料傳輸係因控管者遵循歐盟、歐盟會員國法律，或為執行公共利益、法定職務之必要。EDPB 表示僅有依歐盟法或歐盟會員國法律授權執行公共法定職務，始有適用[247]。

3. 依同項第 c 款規定，資料傳輸係因公共衛生領域之公共利益必要。EDPB 表示資料傳輸之合法性必須明文規定於歐盟或歐盟會員國法律[248]。

4. 依同項第 d 款規定，資料傳輸為實現公共利益、科學或歷史研究、統計目的必要，EDPB 表示應證明行使被遺忘權對於上述目的將造成嚴重妨礙或完全無法實現，始有適用[249]。

5. 依同項第 e 款規定，資料傳輸係因司法訴訟之必要。

---

244 *id*. at para 40.
245 *id*. at para 41.
246 *id*. at para 48-49.
247 *id*. at para 67-68.
248 *id*. at para 74-75.
249 *id*. at para 79.

二、英國

（一）　有關被遺忘權之規範

英國沿用歐盟 GDPR 對於被遺忘權之規定，規定於 UK GDPR 第 17 條。而 DPA 2018 第 47 條另規定：(1) 當控管者處理資料違反 DPA 2018 第 35 條至第 42 條，或控管者有刪除資料的法定義務時，控管者必須立即刪除個人資料；(2) 當事人得要求控管者刪除個人資料或限制其處理。

（二）　實務案例

英國高等法院於 2018 年 4 月作出「被遺忘權」的首兩宗相關判決[250]，兩案在事實背景相似但並無直接關聯，而當事人 NT1 與 NT2 均是向 Google 搜尋引擎要求移除其有關刑事犯罪資訊的連結。法院在判斷當事人得否行使被遺忘權時，參考包括 DPA 1998 及 WP29 工作小組等法規，於 NT1 & NT2 v Google LLC 案件審理結果公開一個月後，GDPR 及 DPA 2018 始施行，此後被遺忘權之行使均依 GDPR 及 DPA 2018 之規定。

三、德國

（一）　有關被遺忘權之規定

德國有關被遺忘權主要規範在 BDSG 第 35 條刪除權（Recht auf Löschung），原則上符合 GDPR 第 17 條第 1 項事由之一者，當事人得行使刪除權，而控管者負有刪除義務；惟 BDSG 第 35 條第 1 項前段補充 GDPR 第 17 條第 3 項之規定，在合法之非自動化處理情形，如有存在特殊類型的儲存或需透過不符比例的努力加以刪除，且刪除對於當事人利益較小時，則無適用刪除權規定。另外，依據 BDSG 第 55 條第 2 款及第 57 條第 1 項第 6 款規定，控管者在處理個人資

[250] NT1 & NT2 v Google LLC [2018] EWHC 799 (QB)

料時，應提供當事人有關更正、刪除及限制處理等權利之資訊。

（二）　實務案例

德國聯邦憲法法院首次提及被遺忘權，於 2019 年分別作出被遺忘權 I 及被遺忘權 II 裁定。在被遺忘權 I 案件中[251]，原告向第三方（即搜尋結果中第三方網頁之資料控管者）行使刪除權，法院認定「被遺忘權」的行使，會受到哲學上時間向度的推進，而影響公開或報導當事人個人資料的合法利益，及當事人行使人格權保護之判斷。在此案中法院認為相關報導，除被告出版之相關經濟利益外，應同時考量到新聞自由、歷史研究及民主思辯之重要基礎，若原告權利受侵害或影響時，被告應採取適當保護措施，並就個案應予補償，以衡平彼此權益，故判決原告勝訴[252]。而在被遺忘權 II 案件中[253]，原告請求搜尋引擎將其透過蒐集、取得、紀錄或儲存姓名之「連結」移除，法院將相關媒體採訪報導的時間向度、公眾知的權利及檢索姓名對當事人權利之影響進行衡量，由於原告當初既已知悉並同意接受採訪，且有意識地接受並公開於社會職業活動，該項報導屬於經當事人同意且真實之資訊，故判決原告敗訴[254]。

251　判決事實略為：原告因犯下殺人罪而判處刑罰，於 2002 年申請假釋出獄後至今，以「Spiegel」作為 1982 年或 1983 年的關鍵字，仍得搜尋到原告的相關新聞報導，故要求被告刪除相關檔案資料。

252　Bundesverfassungsgericht [BVerfG], https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr001613.html (last visited Mar. 9, 2022).

253　某企業的高階主管在接受廣播電視台的採訪，並以「解雇：雇主卑鄙的伎倆」（Kundigung: Die fiesen Tricks der Arbeitgeber）作為公開放送的主題，使原告後來受到公司解雇，並且只要透過 google 搜尋引擎輸入原告姓名，第一筆顯示的資料即為上開廣播報導，故原告要求搜尋引擎平台刪除相關連結資料。

254　Bundesverfassungsgericht [BVerfG], https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2019/11/rs20191106_1bvr027617.html (last visited Mar. 9, 2022).

四、美國

（一）　CCPA 及 CPRA

CCPA 及 CPRA 第 1798.105 條第 a 項明定個人資料的刪除權，亦包含被遺忘權之概念，即消費者有權請求營利事業刪除其他營利事業自該消費者蒐集之個人資料，並針對營利事業、服務提供者（service provider）及承包商（contractor）區分其刪除義務。（1）營利事業須依同條第 b 項及第 1798.130 條揭露消費者有請求刪除權，依同條第 c 項營利事業接獲經驗證的消費者請求後，應刪除相關紀錄，並應通知其他服務提供者、承包商刪除該消費者的個人資料，且通知營利事業曾出售或共享該個人資料的第三方刪除消費者的個人資料，除非得證明該刪除為不可能或所費甚鉅不符比例。惟依同條第 c 項第 2 款，營利事業為防止個人資料被販售、法令遵循或本法其他事由得保留一份「刪除請求的機密紀錄」（confidential record of deletion requests）；（2）服務提供者及承包商收到營利事業通知後應協助處理，並應通知可能從其取得消費者個人資料權限的其他服務提供者、承包商或第三方，除非可證明該刪除為不可能或所費甚鉅不符比例。惟依同條第 c 項第 3 款，若消費者直接向服務提供商或承包商提出刪除請求，則服務提供商或承包商並無義務遵從。

又依同條第 d 項規定營利事業、服務提供者及承包商有下列情形時無須刪除個人資料，包括（1）為履行營利事業與消費者之間的契約；（2）為協助確保安全性及完整性之目的，消費者個人資料有合理利用必要；（3）為識別及修復損害現有預期功能的錯誤；（4）確保其他消費者行使其言論自由或其他法定權利；（5）履行法定義務；（6）在遵守所有其他適用之道德及隱私法的前提，從事公共或經同儕評鑑（public or peer reviewed）的科學、歷史或統計研究，且消費者已知情同意（informed consent），而企業刪除資料可能嚴重損害或無法實現研究目的；（7）基於消費者與企業關係所生的合理期待，供以企業內部利用。

（二）　UPDPA

UPDPA 並無賦予當事人對其個人資料有刪除權及被遺忘權之規定，統一法律委員會（Uniform Law Commission，ULC）於 UPDPA 前言（Prefatory Note）表明，此係考量為避免企業負擔過重法遵及監管成本，同時為當事人提供「合理水準」（reasonable level）的保護[255]，並避免產生與加州、維吉尼亞州隱私法規有關的合規及監管成本。另在 UPDPA 對於控管者一般性義務的立法意見中，未課予控管者或處理者之刪除義務，係因 ULC 考量控管者或處理者保有個人資料的正當性範圍廣泛，且以現今資料儲存、處理之方式，極難確保任何特定當事人的資料是否已刪除，而認為以具相容性資料處理、不具相容性但取得同意的資料處理規範應足以提供相當保護[256]。

五、日本

（一）　有關被遺忘權之規範

日本個人資料保護委員會於〈個人資料保護法所謂 3 年一次的修正相關研究的中間整理〉（個人情報保護法いわゆる 3 年ごと見直しに係る検討の中間整理）[257]，討論 GDPR 之被遺忘權與日本個資法之刪除權（消去権）仍存在差異。依日本個資法第 35 條第 5 項及第

---

255 Uniform Law Commission, *Prefatory Note*, DRAFT FOR APPROVAL UNIFORM PERSONAL DATA PROTECTION ACT, at 1, 2 (2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=6f7e81fb-9c3e-8f4b-1907-d59fb4fa61ec&forceDialog=0 (last visited Mar. 9, 2022).

256 Uniform Law Commission, *Section 4 Controller and Processor Responsibilities; General Provisions Comment*, DRAFT FOR APPROVAL UNIFORM PERSONAL DATA PROTECTION ACT, at 13, 13 (2021), https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=6f7e81fb-9c3e-8f4b-1907-d59fb4fa61ec&forceDialog=0P13 (last visited Mar. 9, 2022).

257 個人情報保護法いわゆる３年ごと見直しに係る検討の中間整理（案），個人情報保護委員会，平成 31 年 4 月 25 日，https://www.ppc.go.jp/files/pdf/0425_shiryou1.pdf（最後瀏覽日：2022 年 3 月 2 日）。

6 項規定，當個人資料處理業務已無利用個人資料之需要、發生第 26 條第 1 項個資事故或有損害本人權益之虞時，當事人得對個人資料處理事業者請求停止利用、刪除或停止提供第三人，個人資料處理事業者於請求有理由時，負有義務且不得遲延。然依同條第 6 項但書規定，如停止利用、刪除或停止提供第三人所費不貲或顯有重大困難之情形，得依個案具體考量採取對當事人權益保護必要之適當替代措施。

（二）　實務案例

日本有論者提及被遺忘權之實務案例[258]，於平成 27 年 12 月 22 日埼玉地方裁判所之判決，原告請求搜尋引擎刪除其過去所犯兒童買春罪遭逮捕新聞之搜尋結果。法院認為原告依其犯罪性質等，對其過去所犯之罪應存在被遺忘權，故判決原告勝訴[259]。其後，搜尋引擎提起抗告，於平成 28 年 7 月 12 日東京高等裁判所之判決[260]提及，被遺忘權在日本並無法律明文依據，且該權利之要件與法律效果並不明確，故判決被告勝訴。又本案於平成 29 年 1 月 31 日最高裁判所判決[261]，認為針對前科性質的敘述為「屬於個人隱私之事實不當輕易被公開之利益，應可謂為法律所保護的對象」，搜尋結果之提供在某程度上，屬於搜尋引擎表現自由之保障範圍[262]，並針對提供搜尋結果之違法判斷作出標準[263]，包括屬於個人隱私事實之性質及內容、該連結等資訊之提供對事實之傳達範圍、對當事人造成具體被害之程度、當事人之社會地位與影響力，及該事實不公開之法律上利益與該

---

258 宮下紘，〈「忘れられる権利」について考える—平成 28 年 7 月 12 日東京高裁決定を受けて〉，《ロ一·ジャーナル》，第 741 期，頁 1 以下（2016）。

259 上机美穂，〈検索エンジンの検索結果による逮捕歴公表と「忘れられる権利」〉，《新・判例解説 Watch》，第 20 期，頁 115 以下（2017）。

260 同前註，頁 115 以下。

261 最高裁平成 29 年 1 月 31 日第三小法廷，平成 28（許）第 45 號，https://www.courts.go.jp/app/files/hanrei_jp/482/086482_hanrei.pdf（最後瀏覽日：2022 年 3 月 9 日）。

262 上机美穂，〈検索エンジンの検索結果と検索事業者の責任〉，《新・判例解説 Watch》，第 21 期，頁 97 以下（2017）。

263 同前註，頁 6 以下。

連結等資訊作為搜尋結果之理由等因素，衡量後加以判斷。若判斷結果認為不公開之法律上利益明顯高於提供該等資訊作為搜尋結果之情況，則得認該刪除請求為有理由。

六、韓國

韓國 PIPA 賦予當事人有資料刪除之權利，惟概念上與 GDPR 之被遺忘權有所不同。PIPA 對於資料刪除權之內涵，為當事人依 PIPA 第 35 條請求閱覽其個人資料後，得就該個人資料向資料控管者提出更正或刪除請求，而控管者應在接收請求之 10 日內答覆，並根據請求進行更正或刪除。又 PIPA 第 36 條明定當事人得行使刪除權(삭제권)，惟若其他法令明定不可刪除時，則例外得不予刪除；但控管者應立即通知當事人，說明拒絕請求之決定與理由以及申訴管道[264]。而當控管者於接收當事人之請求時，若為進行調查之必要，得向當事人請求提交必要之證明文件。

七、新加坡

目前新加坡 PDPA 並未賦予當事人有刪除權、被遺忘權等相關規範，亦即當事人並無得請求組織刪除其個人資料之權利。

貳、我國規定及分析

我國個資法第 3 條第 5 款規定當事人就其個人資料具有「請求刪除權」，第 11 條第 3 項規定「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」。又第 19 條第 1 項第 7 款及第 19 條第 2 項規定當事人對取自一般可得來源之個人資料禁止處理或利用者，蒐集或處理者應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

過去實務有認為「有關民眾陳情移除透過網際網路 google 及

[264] 個資法施行細則第 43 條第 3 款參照。

yahoo 搜尋引擎搜尋功能出現之商業登記資料，是否符合個資法第 19 條第 1 項第 7 款及第 2 項規定，應先釐清網際網路搜尋引擎搜尋出現個人資料，是否屬本法所稱之蒐集、處理或利用個人資料之行為，如屬上開行為者，宜由個人資料之蒐集或處理者，依個資法第 19 條第 1 項第 7 款規定衡量相較於個人資料之蒐集或特定目的，當事人是否顯有更值得保護之重大利益」（參照法務部 104 年 3 月 11 日法律字第 10403502390 號函）；又有認為「被遺忘權係指要求移除自己負面或過時之個人身分資訊搜尋結果之權利，惟被遺忘權並非我國現行法所承認之權利」（參照臺灣臺北地方法院民事判決 105 年度訴字第 3517 號）。

然而近期實務有認為「資訊主體主張應將其個人身分資訊經搜尋引擎所得搜尋結果刪除時，應就搜尋結果所連結內容之資訊目的、公開資訊之目的及其社會意義、要求刪除事項之性質是否與公共利益有關、公開資訊對被害人造成損害之程度、被害人以何種行為導致發生此種侵害、被害人是否為公眾人物等因素為通盤考量，惟於衡量結果仍不足以正當化該搜尋結果，始得認為有被遺忘權存在」（參照臺灣高等法院 106 年度上字第 1160 號判決）；及「個資主體對於曾經合法公開之個資，因時間經過，其被蒐集、處理或利用之特定目的已不存在，或已逾越該目的之必要範圍，自得請求該資料之蒐集或處理者予以刪除。關於必要性存否之認定，應就個資主體之資訊隱私權與公眾知的權利之公益為法益衡量」（參照最高法院 109 年度台上字第 489 號民事判決）；又有認為「雖因我國並非歐盟會員國，並無 GDPR 之適用或受其拘束，然依釋字第 603 號闡釋資訊隱私權所立足之資訊自主權意涵，被遺忘權顯然已涵蓋在隱私權之範疇，固應受憲法保障至明」（參照臺灣高等法院臺南分院 110 年度上易字第 55 號刑事判決）。

綜上所述，過去實務雖未承認當事人具有被遺忘權，然近期實務見解已有逐漸承認被遺忘權之趨勢，肯認被遺忘權為憲法所保障隱私權之內涵，惟強調仍應回歸個資法規定作法益衡量，且應將時間、處理目的、公益等納入判斷標準之考量。

參、分析與小結

一、 比較法之分析

（一） 被遺忘權之內涵

被遺忘權源起於 2014 年 Google Spain v AEPD and Costeja 一案，歐盟法院認為，當與當事人有關的特定資料因時間之流逝有變得不適當、不相關或不再相關、或過當之情形，且該資料可透由在搜尋引擎鍵入當事人姓名而經特定連結近用時，即便系爭資料之公開為合法，搜尋引擎的營運者有義務個案衡量當事人提出的要求，刪除特定連結，以避免對當事人隱私與資料保護權利之侵害。

綜觀各國法制，目前歐盟 GDPR 體系國家（例如德國）、英國、美國 CCPA 均已明文承認當事人享有被遺忘之權利。以歐盟 GDPR 體系國家（例如德國）、英國之立法體例，規定當事人於特定情事下，有權要求資料控管者刪除其個人資料，控管者因而有義務刪除該個人資料且不得無故拖延；如控管者已公開該個人資料，在考量現有科技及執行成本後，該控管者應採取合理步驟及相關措施（包括數位通訊方式），通知其他處理上開公開個人資料之控管者，有關當事人已提出上開刪除所有與其個人資料相關之連結、複製或仿製的請求之情事。而美國 CCPA 係規定當事人得請求控管者刪除其個人資料，且控管者應通知其他控管者刪除該個人資料相關紀錄，除非控管者得證明刪除為不可能或所費不貲，始得拒絕。而我國、日本、韓國則僅有刪除權之規定，雖被遺忘權係從刪除權所延伸之權利，惟有明文立法例之國家，其所得請求刪除個人資料之範圍更廣，包括所有與其個人資料相關之連結、複製或仿製等。再者，被遺忘權要求控管者在考量現有科技及執行成本，應採取適當措施與技術形式向其他控管者踐行通知義務，因此如搜尋引擎等其他控管者亦負有刪除義務。

（二） 被遺忘權之規範

關於被遺忘權之行使要件，以歐盟 GDPR 體系國家（例如德國）、

英國之立法體例，乃明定應包括：(1) 蒐集或處理該個人資料時之目的已不再需要；(2) 當事人撤回處理該個人資料所需之同意，且該處理欠缺其他法律依據；(3) 當事人依拒絕權之相關規定對處理提出異議，且該處理欠缺更為優先之正當事由；(4) 該個人資料遭違法運用；(5) 控管者依相關規定，有義務刪除該個人資料時；(6) 該個人資料係為向未成年人提供資訊社會服務所蒐集，故係以個資之特定目的消失、欠缺法律依據或正當事由、非法運用等類型為主。而美國 CCPA 則廣泛賦予當事人刪除請求權，未有特定情形下當事人始得行使之要求。

又例外得予以限制當事人行使被遺忘權之規定，由於被遺忘權並非絕對之權利，不論歐盟 GDPR 體系國家（例如德國）、英國或美國 CCPA 均明定於特定情形，仍得限制當事人行使被遺忘權。以歐盟 GDPR 體系國家（例如德國）、英國之立法體例，明定例外情形包括基於言論自由、執行公權力、公共衛生、科學研究及司法訴訟。而美國 CCPA 所明定之例外情形，則包括基於言論自由、執行公權力、科學研究及履行契約等。在共通限制情形之探討上，主要集中於言論自由、執行公權力、科學研究之類型，若係基於言論自由之限制，應考量資料之性質、機敏性、對網路使用者資料取得自由之影響、對當事人公眾生活之影響等因素；而若基於法定職務或義務等公權力行使之限制，仍應限於公共利益必要之情形；又基於科學研究目的之限制，仍應限於可能造成重大妨礙或無法實現之情形。

雖然被遺忘權係賦予當事人得控制其個人相關資料之權利，強化個人之資訊自決權，然而被遺忘權在實施上可能有技術層面之侷限，且因通常被遺忘權之請求係先由搜尋引擎、社群網站等控管者進行審核，故存在私人審查言論及寒蟬效應等爭議性。

二、 小結

綜上所述，由於我國個資法所賦予當事人之刪除權，對於搜尋引擎、社群網站等控管者究屬我國個資法之蒐集、處理或利用者尚存疑

義，得否逕依個資法規定向上開控管者請求刪除搜尋結果、連結等相關個人資料之紀錄，亦難以確定。雖我國近期實務已逐漸肯認被遺忘權，然回歸個資法之刪除權規定，在適用上仍存在諸多限制，並不似被遺忘權得請求刪除之範圍相同，又未課予控管者應負有通知其他控管者之義務，故難謂我國個資法之刪除權等同於被遺忘權之概念。

綜觀各國法制，對於被遺忘權仍訂有相當規範。在被遺忘權之行使要件上，歐盟 GDPR 體系、英國明定應以運用個人資料之特定目的消失、欠缺法律依據或正當事由、非法運用等類型為主；美國 CCPA 則一般性承認當事人得行使被遺忘權，故未定有行使要件。

另考量被遺忘權並非絕對之權利，在例外情形仍得限制當事人行使被遺忘之權利。歐盟 GDPR 體系、英國及美國 CCPA 均明定被遺忘權之限制規定，其限制之例外事由以言論自由、公權力行使、科學研究之類型為主，避免當事人行使被遺忘權對公共利益產生過大影響。在實施被遺忘權之問題上，因搜尋引擎、社群網站等控管者範圍廣泛，通知及刪除之方式、範圍亦都不明確，故仍存在技術、成本上挑戰，亦應注意是否會導致私人審查言論及寒蟬效應之爭議。

第三項 權利限制規定

壹、比較法國家

一、歐盟

（一）　權利行使限制事由

GDPR 第 23 條第 1 項明定，歐盟成員國得制定國內法限制當事人之資料自主權利，包含近用權、更正權、刪除權、限制處理權、可攜權、拒絕權，但限制事由應尊重基本權利與自由，並且應符合民主社會之必要性與比例性。GDPR 列出十項限制事由，包括國家安全、國防、公共安全、刑事犯罪相關事項、歐盟及成員國之經濟利益、司法、特定行業之倫理規範、執行公務機關之監督或調查等職務、保護當事人或第三方之權利與自由、民事案件之執行。又依 GDPR 第 85

條第 2 項基於新聞目的或學術、藝術或文學表意目的所為之處理，會員國為平衡個人資料保護及表意及資訊自由權利而有必要者，應排除 GDPR 第三章當事人權利所定規定。

而 EDPB 發布指引[265]，說明各項事由具體適用情形：(1) GDPR 第 23 條第 1 項第 a、b、c 款為國家安全、國防、公共安全事由，皆與國家利益有關；公共安全應與保護生命事務有關，如因天災人禍而保護人民生命安全。(2) 同項第 d 款與刑事犯罪相關，為防止、調查、偵查、追訴刑事犯罪或執行刑罰，得限制當事人權利以防止刑事偵查曝光而失敗，通常適用於洗錢防制案件或鑑識工作相關之情境。(3) 同項第 e 款之一般公共利益包含財政、國家預算、稅賦，公共衛生及社會安全，如稅務機關為避免近用權行使影響調查結果得作限制，惟限制範圍應以調查之必要性為基準，並應於調查結束時立即解除限制且通知當事人。(4) 同項第 f 款與司法相關，為追求與確保司法獨立及司法程序正當性得限制當事人權利行使。(5) 同項第 g 款為針對特定行業而定，如律師及醫生違反行業道德規範之預防、調查、偵查及追訴，基於偵查不公開原則對當事人權利行使作限制。(6) 同項第 h 款為公務機關依國家安全、一般公共利益、特定行業之倫理規範執行監管職務時，即使為不定期性仍得限制。(7) 同項第 i 款為保護當事人或他人之權利與自由，如當事人涉及職場霸凌之調查，為避免受害者及吹哨者的身分曝光，得限制其近用權；反之，受害者及吹哨者之近用權亦得被限制，以給予涉嫌之當事人適度尊重。(8) 同項第 j 款與民事案件相關，如當事人有可能為民事訴訟案件的原告或被告，則得限制其權利。

（二）　權利行使限制規範

GDPR 第 23 條第 2 項要求前項立法措施，應至少包含下列事

---

[265] EUROPEAN DATA PROTECTION BOARD [EDPB], *Guidelines 10/2020 on restrictions under Article 23 GDPR* (2021), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en, at para 23-35 (last visited Apr. 15, 2022).

項：(1) 資料處理之目的或處理之類型，依 GDPR 前言第 8 點強調權利限制之理由應使一般人易於清楚明白，且資料處理目的應與限制事由相關。(2) 個人資料之類別，如涉及特種個資，因機敏性較高應特別列出。(3) 權利限制之範圍，如僅對特定權利限制，或為全部當事人權利均予限制。(4) 防止濫用或非法近用或傳輸之保護措施，措施為技術上或組織上的措施。措施並不一定要是長期永久措施，亦包含暫時性措施。(5) 明列資料控管者，如無法明列，則應列出資料控管者之種類。(6) 資料保存期限及所採取的適當安全措施，如資料保存期間的計算方式得納入實際處理資料的時間，以及將來爭訟案件之考量。(7) 當事人權利及自由的風險，應進行資料保護風險評估 (data protection impact assessment, DPIA)，EDPB 認為資料處理如對當事人造成歧視、貶低人格、限制言論自由或對弱勢族群影響甚鉅，則法律應規範明確。(8) 賦予當事人關於權利限制之知悉權，除告知當事人將妨礙限制目的實現。此項告知應符合 GDPR 有關告知相關要件，如當事人在調查案件期間申請行使其權利，告知聲明書應明確敘述所限制之權利類型及限制期間之長短。

二、英國

(一)　UK GDPR

UK GDPR 第 23 條與 GDPR 第 23 條之規定大抵相同，其第 1 項規定賦予內閣大臣得以立法程序限制當事人權利，但限於其立法符合當事人權利義務，並應尊重基本權及自由之本質，且係民主社會之必要適當措施，以確保公共安全、刑事犯罪相關事項、歐盟及成員國之經濟利益、司法、特定行業之倫理規範、執行公務機關之監督或調查等職務、保護當事人或第三方之權利與自由、民事案件之執行。復第 2 項規定前項所稱之立法措施亦同前述 GDPR 之說明，即在立法限制當事人權利時，該限制必須明確並使當事人可得而知。另 UK GDPR 第 85 條亦規定基於新聞目的或學術、藝術或文學表意目的所為之處理，為平衡個人資料保護及表意與資訊自由權利而有必要者，應排除第三章當事人權利規定適用。

（二）　DPA 2018

DPA 2018 第 15 條將 UK GDPR 之權利限制規定於附件二至四作列舉之說明。附件二所列舉之權利限制規定共分為六大部分，第一部分包括犯罪、稅務、移民；第二部分為維持公眾保護、監察等公共機能；第三部分係衛生、社會、教育工作者為順利近用資料所進行資料測試之情形；第四部分包括司法訴訟、企業融資、考試分數等情形；第五部分包含新聞、學術、藝術、文學等與表意自由相關；第六部分則是研究、統計、公益目的之歸檔。惟須注意，並非有上述情形即得限制當事人權利，而須依個別情形比對附件二內容始能確定所限制之當事人權利類型。附件三則係針對資料性質決定當事人權利之限制，如健康資料、社會工作資料、教育資料、受虐兒童資料等，並分別判定以上性質之資料在不同場合得豁免之規定類型。另附件四整理英國有禁止或限制資料公開揭露之其他法律規定，如人類受精和胚胎資訊、收養紀錄、特殊教育需求聲明、少年審理程序報告等。

此外，DPA 2018 第 16 條第 1 項及第 2 項第 b 款規定為國家安全及防衛目的之情形不適用當事人權利之規定，又第 1 項授權內閣大臣得制定法令以調節 UK GDPR 有關當事人權利規定的適用。

三、德國

BDSG 第 32 條至第 37 條對應 GDPR 有關當事人權利限制之規定。依 BDSG 第 33 條規定，在採行技術及組織上安全措施，並符合下列情形得限制當事人行使近用權：（1）具有第 33 條第 1 項第 a 款及第 2 項第 b 款或第 3 項事由，為避免妨礙公務機關履行法定職務之必要。（2）因法定保留必須留存紀錄且不得刪除。

關於更正權、刪除權之限制，規定於 BDSG 第 58 條，原則上當事人有權要求更正錯誤的個人資料，特別是涉及個人資訊的評估或陳述，但若未能確認資料正確性時，則資料控管者應以限制處理而非刪除個人資料的方式應對，並於解除限制處理前應通知當事人。又當個人資料之蒐集、處理或利用為非法時，或已無原始蒐集目的之必

要、資料控管者依法負刪除義務者，則當事人應有權要求盡速刪除之。除資料正確性外，資料控管者於下列情形亦應以限制處理代替刪除之請求：（1）有理由假設刪除將對當事人之合法利益產生不利影響。（2）為進行刑事或行政訴訟程序中作為證據而必須保留個人資料。（3）因特定的儲存方式，刪除為不可能或所費不貲的情形。

四、美國

（一）　CCPA 及 CPRA

CCPA 及 CPRA 對於當事人權利之限制，有因權利而異的「個別權利限制規定」以及「一般權利限制規定」，以下分別說明。

1. 個別權利限制規定

首先，當事人權利之行使必須是「可驗證的消費者請求（verifiable consumer request）」[266]，且行使權利之界線不得延伸到其他消費者資料，如刪除權、更正權、知的權利（包括「知悉蒐集之資料、資訊近用的權利」及「知悉被販售、共享、販售及共享對象的權利」）。關於知的權利，依 CCPA 及 CPRA 第 1798.110 條及第 1798.115 條限制消費者行使權利之頻率，原則上消費者一年內僅能對同一營利事業提出一次請求。

而關於刪除權之限制，依第 1798.105 條規定當營利事業接獲消費者請求後，須通知其服務提供商及承包商刪除資料，營利事業僅於刪除之成本不符比例時，得拒絕並應負舉證責任。惟有下列事由亦得拒絕刪除：（1）為達成該個人資料蒐集目的之交易、履行書面保證的條款或基於聯邦法律召回產品、提供良好產品或服務必要，或根據營利事業與消費者的持續營業關係脈絡下為消費者可合理預期、為履

266　依 CPRA 第 1798.140 條第 ak 項規定，「可驗證的消費者請求」係指由消費者、消費者代表其未成年子女、經消費者授權代表消費者的人、消費者之代理人、或消費者之監護人提出之請求，並且可由營利事業以商業上合理的方式，依據檢察長基於第 1798.185 條第 a 項第 7 款採用之相關規定，驗證確實為營利事業蒐集個人資料來源之消費者。

行營利事業與消費者之間的契約。(2)為協助確保安全性及完整性的合理必要使用。(3)識別及修復預期功能之錯誤。(4)行使言論自由，確保其他消費者行使其言論自由權或其他法定權利。(5) 根據加州《刑法典》所須遵守《加州電子通訊隱私法》(California Electronic Communications Privacy Act)。(6) 公共或經同儕評鑑的科學、歷史或統計研究，且消費者已提供知情同意，如刪除資料可能嚴重損害或導致研究無法完成。(7)基於消費者與企業間關係的合理期待供內部使用。(8)履行法定義務。另需注意，如係家戶資料(household data)不適用刪除權、更正權、知的權利等規定，此係考量家戶資料由數人資料組成，如允許其中一人行使前述權利涉及隱私疑慮與公共政策問題。

2. 一般權利限制規定

除了上述個別權利限制規定，CCPA 及 CPRA 第 1798.145 條詳細羅列一般權利行使的界線或例外規定，營利事業基於下列事由得限制當事人權利：(1) 基於聯邦、州法、地方法令遵循。(2) 依法院命令或要求提供資訊之傳票。(3) 遵守聯邦、各州地方政府機關的民、刑事或法令監管之要求、調查、傳票、傳喚。(4)營利事業合理、善意認為潛在違法行為而與執法機構合作處理。(5) 依政府機關要求，為防止他人面臨生命或嚴重身體傷害危險時緊急取得消費者資料。(6)行使法律上權利或防禦。(7)個人資料已去識別化或匯總化。(8) 不得對其他消費者的權利及自由產生不利影響。(9) 勞雇關係例外，但仍須為蒐集資訊之通知，並保留員工有權選擇退出。(10) 不及於非商業活動。(11) 其他法規之法定事由。

(二)　UPDPA

UPDPA 明確提供的資料當事人權利類型包括「請求複製本的權利」(知的權利)、「更正權」及「不因行使權利受報復的權利」。UPDPA 第 5 條第 a 項第 3 款要求資料控管者應該設立合理的驗證程序，以驗證提出請求的資料當事人其身分，而控管者遵從的請求，亦須是經

驗證的資料當事人的請求。有關個別權利限制之規定，(1)請求複製本之權利行使限制，資料控管者僅須於一年內無償提供一份複製本，其餘數量得酌收合理行政費用。(2)更正權之權利行使限制，如資料控管者有理由認為當事人的更正請求不明確、不合理或過度，則得拒絕並須向當事人說明。而一般權利限制之事由有下列情形，包括：(1)不適用公開可得的資料。(2)不適用符合保護人體受試者法規之人體試驗研究所處理或保有之資料。(3)不適用法院令狀、命令或其他法律允許、要求處理或揭露之資料。(4)依據政府資料公開法規須公開之資料。(5)於資料當事人受雇或應徵期間處理或保有之資料。

五、日本

（一）　非公務機關

關於揭露請求權行使之限制，依日本個資法第 33 條第 2 項規定例外情形得限制當事人行使揭露請求權，包括：(1)有損害於本人或第三人之生命、身體、財產或其他權益之虞者；(2)對該個人資料處理事業業務之適當執行，有造成明顯妨礙之虞者；(3)構成違反其他法令者。如有上述情形之一，則個人資料處理事業得拒絕當事人全部或一部分之請求，且必須立即通知本人有關拒絕之決定。而關於更正請求權行使之限制，依第 34 條第 2 項規定，當有其他法令訂有特別程序者，個人資料處理事業得拒絕當事人之更正請求。最後，關於停止利用及刪除請求權行使之限制，依第 35 條第 2 項及第 3 項規定個人資料處理事業如受有當事人請求且有理由時，除非停止利用或刪除成本過高或有困難之情況，得採取必要措施替代之，但應向當事人通知。

（二）　公務機關

關於揭露請求權行使之限制，依第 78 條有特定情形得限制當事人行使揭露請求權，包括：(1)對揭露請求者的生命、健康、生活或財產有侵害之虞的資料。(2)有關揭露請求者以外之他人資料(不包含關於個人所營事業之資料)，而依照該資料所包含之姓名、出生年

月日等其他敘述能識別出揭露請求者以外之特定個人（包括比對其他資訊而能識別出揭露請求者以外之特定個人時）；或是包含個人識別符號者，或雖然不能識別出揭露請求者以外的特定個人，但由於揭露反而會對揭露請求者以外之他人權益造成侵害之虞。(3)有關法人及其他團體，或是經營揭露請求者以外事業之個人與所營事業相關之特定資料。但不包括為保護人的生命、健康、生活以及財產，認為有揭露必要的資料。(4)由於揭露，行政機關首長有相當理由足認可能損害國家安全、損害與其他國家或國際組織之間的信賴關係、或者造成與其他國家或國際組織之間交涉上不利影響之資料。(5)因揭露而行政機關首長有相當理由足認可能妨礙預防犯罪、鎮壓或搜查、公訴之進行、刑罰的執行及其他維持公共安全與公共秩序之資料。(6)有關在國家機關、獨立行政法人等、地方公共團體以及地方獨立行政法人的內部或相互間之審議、檢討或協議的資料，由於揭露會不當損及直接地意見交換或意思決定的中立性，或者不當使國民之間產生混亂，或造成不當賦予特定人利益或不利益之資料。(7)屬於有關國家機關、獨立行政法人等、地方公共團體或者地方獨立行政法人進行的事務、事業之資料，而由於揭露有發生特定情形之可能或其他相關在該當事務或事業之性質上，有對該事務、事業適當遂行造成妨礙之虞。如有上述特定事由，公務機關得依第 79 條拒絕揭露請求或為部分揭露。

有關更正請求權行使之限制，依第 90 條第 1 項但書規定，當有其他法令對於保有個人資料之更正另訂特別程序時，則得拒絕之。而有關停止利用及刪除請求權之限制，依第 98 條第 1 項但書規定，當有其他法令對於保有個人資料之停止利用、刪除或停止提供另訂特別程序時，則得拒絕之；又第 100 條但書規定，因停止利用該保有個人資料，在該保有個人資料的利用目的相關之事務在性質上，可認為對於該當事務的適當執行造成顯著妨礙者，亦得排除公務機關之停止利用義務。

六、韓國

根據 PIPA 第五章規定當事人得行使閱覽、更正、停止利用及刪除等權利。關於閱覽請求權行使之限制，依 PIPA 第 35 條規定資料控管者於下列情形得拒絕並向當事人通知，包括：(1) 法律明文禁止或限制閱覽時。(2) 有危害他人生命、身體、財產或其他權益之虞。(3) 公務機關執行法定職務有遭遇重大障礙之情形，如租稅徵收、學校教育機關成績評量及評選、核定撫恤金等相關事項。

而關於更正、刪除請求權行使之限制，依第 36 條規定資料控管者於接收當事人所提出之要求時，除非當事人為其他法令明定之蒐集對象不得要求刪除外，應立即調查並依照其要求為更正，並應將調查結果告知當事人，且資料控管者應設置使該資料無法回復或重製之措施。另關於停止利用請求權行使之限制，依第 32 條第 2 項公務機關有下列情形得拒絕並應向當事人通知，包括：(1) 基於法令或法定義務。(2) 有危害他人生命、身體、財產或其他利益之虞 (3) 若停止利用個人資料將使法定職務無法繼續執行。(4) 若停止利用個人資料將可能導致債務不履行，且當事人尚未有解除契約之表示。

七、新加坡

關於近用權行使之限制，依 PDPA 第 21 條第 2 項規定，資料控管者於 PDPA 附表 5 所列之例外事項得拒絕當事人請求，包括：(1) 僅用於評估目的之意見資料。(2) 由教育機構進行的任何考試、試卷及公佈前的考試成績。(3) 私人信託受益人的個人資料，僅用於管理信託。(4) 由仲裁機構或調解中心保存的個人資料，僅用於仲裁機構或調解中心管理的仲裁或調解程序。(5) 司法檢調程序尚未完成之文件。(6) 受法律特權約束的個人資料。(7) 個人資料若揭露將洩露商業機密，且可能有損組織的競爭地位。(8) 依 PDPA 附表 1 規定未經同意蒐集、利用或揭露的個人資料用於調查目的，惟調查及相關訴訟程序尚未完成。(9) 由調解員或仲裁員在進行調解或仲裁時所蒐集或建置的相關資料。(10) 由於請求的重複性或系統性將不合理地干

擾組織的運作，或提供存取相關負擔或費用對組織為不合理或與個人利益不相稱。

而關於更正權行使之限制，依第 22 條第 7 項規定，資料控管者於 PDPA 附表 6 所列之例外事項得拒絕當事人請求，包括：(1) 僅用於評估目的的意見資料。(2) 由教育機構進行的任何考試、試卷以及在考試成績公佈前的考試成績。(3) 私人信託受益人的個人資料，僅用於管理信託。(4) 由仲裁機構或調解中心保存的個人資料，僅用於仲裁機構或調解中心管理的仲裁或調解程序。(5) 司法檢調程序尚未完成之文件。(6) 組織在業務過程中，從該組織擁有或控制之當事人或他人個人資料中，得出有關該當事人之個人資料。

八、瑞士

DSG 2020 對當事人權利行使之限制，主要分為知情權及可攜權兩種權利之限制規定。有關知情權之限制，依據 DSG 2020 第 26 條第 1 項明定資料控管者在特定條件下得向當事人拒絕或限制、延遲提供資訊，包括：(1) 依法律規定如履行保密義務等。(2) 為保護第三方之重大利益。(3) 當事人的請求無根據，如目的違反資料保護或明顯有爭議等情形，資料控管者亦得在未向第三方提供個人資料的情況，根據利益衡平決定拒絕之。另一方面，根據同條第 2 項規定，聯邦機構得基於重要公共利益及國家安全，或基於可能嚴重影響司法調查程序等原因，向當事人拒絕或限制、推遲提供資訊。依同條第 3 項規定，當特定條件消失，除該資訊已無法提供或所費不貲的情況外，應盡速向當事人提供。而依同條第 4 項規定，資料控管者拒絕或限制、延遲提供時，必須向當事人說明原因。此外，知情權之限制對於新聞媒體有特別規範，依第 27 條第 1 項規定當個人資料僅用於進行報導時，新聞記者身為資料控管者得基於以下原因向當事人拒絕或限制、延遲提供資訊，包括個人資料可能揭露資訊來源、已向當事人提供報導初稿、公開發表意見之自由可能受到損害。又依同條第 2 項規定，當個人資料僅用於工作輔助時，記者亦得拒絕之。

而有關可攜權之限制，依第 29 條第 1 項規定資料控管者得以第 26 條第 1 項第 1 款基於法律規定，以及第 2 款為保護第三方之重大利益，向當事人拒絕或限制、延遲交付或轉移個人資料。而依第 29 條第 2 項規定，資料控管者須向當事人說明拒絕或限制、延遲交付或轉移個人資料之原因。

貳、我國規定

我國個資法第 3 條規定，當事人就其個人資料得行使「查詢或請求閱覽」、「請求製給複製本」、「請求補充或更正」、「請求停止蒐集、處理或利用」及「請求刪除」等權利，且不得預先拋棄或以特約限制之，惟個資法仍有訂定當事人權利行使之限制。

一、近用權之限制

關於近用權之限制，包含我國個資法所賦予當事人之「查詢或請求閱覽」、「請求製給複製本」權利，依個資法第 10 條規定，公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。而本條但書並訂定 3 種限制權利行使之要件，若有下列情形，公務機關或非公務機關得拒絕當事人之請求：(1) 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益；(2) 妨害公務機關執行法定職務；(3) 妨害該蒐集機關或第三人之重大利益，又依個資法施行細則第 18 條規定，所稱妨害第三人之重大利益，係指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

二、更正權之限制

關於更正權之限制，依個資法第 11 條第 1 項規定，公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。而個資法施行細則第 19 條僅規定當事人向公務機關或非公務機關請求更正或補充其個人資料時，應為適當之釋明，而未訂有更正權行使之限制。

三、刪除權及停止蒐集、處理或利用權之限制

關於刪除權及停止蒐集、處理或利用權之限制，分為三種情形：(1) 依個資法第 11 條第 2 項規定，個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限；(2) 依同條第 3 項規定，個人資料蒐集之特定目的消失或期限屆滿後，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。(3) 依同條第 4 項規定，個人資料之蒐集、處理或利用違反個資法規定，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。

又個資法施行細則第 20 條規定所稱「特定目的消失」，係指下列各款情形之一：(1) 公務機關經裁撤或改組而無承受業務機關；(2) 非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符；(3) 特定目的已達成而無繼續處理或利用之必要；(4) 其他事由足認該特定目的已無法達成或不存在。而個資法施行細則第 21 條規定「因執行職務或業務所必須」，係指下列各款情形之一：(1) 有法令規定或契約約定之保存期限；(2) 有理由足認刪除將侵害當事人值得保護之利益；(3) 其他不能刪除之正當事由。

參、分析與小結

一、 比較法之分析

（一） 近用權之限制

綜觀各國個人資料保護規範中關於近用權之限制要件，主要可概分為「國家利益」、「公共安全或秩序維護」、「司法或訴訟程序」、「公務機關法定職務、非公務機關法定義務或其他法律規定」、「當事人或第三人重大利益」、「公務或非公務機關之利益或業務」、及其他

如「專業倫理考量」、「新聞」、「考試」、「特定資料類別」、「成本或執行可能性」、「權利行使之頻率」、「權利行使合理性」等類別。

表 32 有關近用權之主要類型限制要件比較

	國家利益	公安/秩序	司法/訴訟	職務/義務/他法	重大利益	其他
我國	O			O	O	機關利益
歐盟	O	O	O	O	O	專業倫理
德國	O	O	O	O	O	專業倫理、成本
英國	O	O	O	O	O	保密、特定資料、新聞、研究、考試、稅務、移民、藝術
瑞士	O	O	O	O	O	新聞
美國	X(州法)	O	O	O	O	頻率限制、特定資料、成本、不合理要求
日本	O	O	O	O	O	機關業務、特定資料、審查公正性
韓國	O	O		O	O	考試、補償撫慰金申請
新加坡			O 含仲裁	O		考試、信託、內部評估、商業機密、重複申請、不合理要求

資料來源：本計畫研究團隊自行整理

表 33 有關近用權之其他類型限制要件比較

	機關利益/業務	專業倫理	新聞	考試	特定資料	成本/可能性	頻率/重複	不合理請求	其他
我國	O								
歐盟		O							
德國		O							
英國			O	O	O				研究、稅務、移民、藝術
瑞士			O						
美國					O	O	免費頻率限制	O	
日本	O				O				影響審查公正性
韓國				O					補償撫慰金申請
新加坡	O			O	O		O	O	

資料來源：本計畫研究團隊自行整理

比較其他國家，除了歐盟僅規範得限制之要件，具體規範須由各會員國自行規定，與我國相關規定較有顯著差異者，主要有以下三項：首先，歐盟、德國、英國、瑞士、美國、日本等國家係將「公共安全或秩序維護」及「司法或訴訟程序」列入近用權限制，我國則未將其納入。但公共安全、秩序維護、司法權之行使等，或可解釋為「公務機關執行法定職務」之一種。

其次，英國、美國、日本、韓國及新加坡等國家針對特定資料或業務型態，如考試業務、新聞業務、健康資料、教育資料、兒童虐待資料、家戶裝置資料及非商業活動資料等之近用，予以當事人近用之限制規定。我國個資法並無此類規定，但可能於特別法中予以規定，如兒童及少年福利與權益保障法等。又美國、新加坡等國家考量資料之執行成本或避免權利濫用，規定可以基於重複申請或請求不合理等事由，予以限制當事人近用，或對於近用權訂有免費行使頻率之限制。

（二）　更正權之限制

觀察國際立法例，有部分國家訂有更正權之限制要件。除歐盟僅規範得限制之要件，具體要件須由各會員國自行立法之外。其中，日本僅規定在有其他法律限制的狀況下，得拒絕更正權之行使，此應為法律解釋之必然結果。而英國個資法於第 26 條及附件二、三對於更正權則訂有多項限制規定，美國加州消費者隱私保護法及新加坡個資法亦同。有關各國常見之更正權限制事由，整理如下表 34：

表 34 有關更正權之限制要件比較

	國家利益	公安/秩序	司法/訴訟	職務/義務/他法	重大利益	其他
我國						
歐盟	O	O	O	O	O	
德國						
英國	O	O	O	O	O	特定資料、新聞、研究、考試、稅務、移民、藝術
瑞士						
美國		O	O	O	O	特定資料、成本、不合理請求
日本				其他法律規定		
韓國						
新加坡			O 含仲裁			考試、信託、內部評估、推論出之資料

資料來源：本計畫研究團隊自行整理

（三）　刪除及停止蒐集、處理或利用權之限制

刪除或停止蒐集、處理或利用為一種當事人對於資料蒐集後的事後控制權利。綜觀各國個資保護規範，除同意之撤回外，其他對於個資事後控制以停止利用或刪除之規定，大致上可分為以下三類狀

況：

1. 針對特定的個資利用方式請求刪除或停止蒐集處理利用

於公務或非公務機關對個資進行某些特定方式的運用時，規定當事人針對該種狀況，得請求停止運用或刪除的權利。首先在當事人權利行使要件，目前我國、歐盟（以及與其規範近乎相同之英國、德國）、美國（包含加州消費者隱私法及聯邦健康保險流通與責任法案）及日本（包含個資法及次世代醫療基盤法）皆有針對特定個人資料利用之方式，賦予當事人得請求停止蒐集、處理或利用及刪除其個人資料之權利。又我國於個資法第 20 條規定，非公務機關利用當事人資料進行行銷時，當事人得要求停止利用其個資行銷。

其次於權利限制要件，歐盟針對學術研究以及未成年人保護相關兩個權利行使，訂有限制規定。於基於科學、歷史研究或統計目的利用個人資料時，如資料控管者得證明該統計或研究係基於公共利益執行職務，得不停止蒐集處理、利用個人資料。另外，為提供未成年人資訊社會服務利用個人資料時，得基於以下原因，不停止蒐集處理、利用個人資料，包括：言論、資訊自由；遵守法定義務；基於公共利益執行職務、受託行使公權力；基於公共衛生之公益目的由專業人員操作或採取適當安全措施；基於公共利益目的之建檔、科學或歷史研究、統計且退出會嚴重妨害目的達成；建立、行使或防禦法律上請求。而德國進一步規定，若刪除將涉及不成比例的努力或不可行時，得以限制處理替代刪除之方式。

表 35 針對特定個資利用方式之刪除/停止蒐集、處理或利用權限制比較

	權利行使要件	權利限制要件	效果
我國	非公務機關、行銷		停止利用
歐盟、英國、德國	行銷	歐盟一般限制要件	停止蒐集、處理或利用
	科學、歷史研究及統計	為公共利益執行任務、歐盟一般限制要件	停止蒐集、處理或利用
	未成年人資訊社會服務	言論自由、資訊自由；法定職務或義務；法律規定；公共衛生公益目的；公益目的建檔、科學、歷史研究、統計；司法訴訟相關；歐盟一般限制要件	刪除
	單純自動化決策處理（禁令，非權利類型）		
美國 CPRA	販賣或跨情境行為廣告*分享個資（16 歲以下 opt-in）		停止蒐集處理利用
美國 HIPAA	募款活動		停止蒐集處理利用
日本個資法	以「將法定告知事項告知本人（或置於本人得知悉狀態），且向個資委員會申報」為由將個資提供給第三人		停止蒐集處理利用
日本次世代醫	以「將法定告知事項告知本人，且經		停止蒐集處

療基盤法	主管機關許可」為由將個資提供匿名化業者進行匿名化處理		理利用

*跨情境行為廣告：消費者並未有意與特定業者互動並提供個人資料，但該業者運用用戶追蹤之方式，鎖定消費者投放廣告。

資料來源：本計畫研究團隊自行整理

2. 針對特定蒐集處理利用合法要件請求刪除或停止蒐集處理利用

於公務機關或非公務機關以部分特定要件蒐集個人資料之狀況，規定當事人得提出異議，請求停止蒐集處理利用或刪除其個人資料。首先關於當事人權利行使要件，目前我國、歐盟（以及與其規範近乎相同之英國、德國）及新加坡皆有賦予當事人針對特定的蒐集合法要件得提出異議，並要求停止蒐集處理、利用或刪除之規定。我國個資法第 19 條第 1 項第 7 款、第 2 項規定，非公務機關依「取自一般可得來源」蒐集一般個人資料時，若禁止使用該個人資料對當事人顯然有更值得保護之重大利益時，當事人可請求刪除、停止處理或利用該個人資料。歐盟則針對基於（1）公共利益執行職務或受託執行公權力；（2）正當利益等二種條件所蒐集的資料，賦予當事人異議、請求停止蒐集、處理、利用之權利。而新加坡規定，以「視為同意」蒐集個人資料之情形，賦予當事人有「撤回同意」之權限。

再者，有關權利限制要件，我國個資法第 19 條第 1 項第 7 款、第 2 項並無權利行使限制規定。歐盟則規定若資料控管者得證明其對此一資料的處理，有「具說服力的正當利益」（compelling legitimate interests），或係涉及與司法訴訟及相關權利主張或答辯等事宜，則得拒絕當事人行使權利。新加坡則規定一旦當事人提出申請，應立即停止該個人資料的蒐集、處理或利用，並無訂定權利限制規定。

表 36 針對特定蒐集、處理或利用合法要件之刪除/停止蒐集、處理或利用權限制比較

	權利行使要件	權利限制要件	效果
我國	非公務機關，資料取自一般可得來源，當事人有更值得保護利益		停止處理或利用、刪除
歐盟、英國、德國	公共利益執行職務或委託行使公權力 正當利益	資料控管者對資料有「具說服力的正當利益」或司法訴訟、司法請求有關；歐盟一般限制要件	停止蒐集、處理或利用及刪除
新加坡	視為同意		停止蒐集、處理或利用

資料來源：本計畫研究團隊自行整理

3. 一般性請求停止蒐集、處理、利用或刪除個資

與上述針對特定的個資蒐集情境或特定的個資運用情境不同，此一類型係一般性賦予當事人得請求停止蒐集、處理或利用及刪除之規定。首先有關當事人權利行使要件，目前我國、歐盟（以及與其規範近乎相同之英國、德國）、美國加州、日本及韓國皆有賦予當事人一般性對於個人資料得請求停止蒐集、處理或利用及刪除之規定。其次在權利限制要件上，許多國家對於當事人請求停止蒐集處理、利用或刪除個人資料，均訂有限制規定。其內容大致可分類如下：(1)法律規定、法定職務或義務要求：我國、歐盟、美國加州（限於直接向當事人蒐集之個資）、韓國（可請求停止蒐集處理利用及刪除）。(2) 言論自由、資訊自由：歐盟、美國加州（限於直接向當事人蒐集之個資）。(3) 契約履行、合理預期之商務運用、維護基本服務等：美國加州（直接向當事人蒐集之個資或敏感性個資皆可）、韓國（限於請求停止蒐集處理利用）。(4) 公共衛生、科學或歷史研究、統計、

建檔等：歐盟、美國加州（限於直接向當事人蒐集之個資）。(5) 難以刪除或成本過鉅：德國、日本、美國加州（限於直接向當事人蒐集之個資）。(6) 其他：司法訴訟（歐盟）、主管機關許可（美國加州限於敏感性個資）、防止他人權利侵害（韓國，但限於請求停止蒐集處理利用）。

表 37 針對一般性請求刪除/停止蒐集、處理或利用權之限制比較

	權利行使要件	權利限制要件	效果
我國	正確性爭議	書面同意或執行業務或職務必須	停止處理、利用
	特定目的消失或期限屆滿	書面同意或執行業務或職務必須	刪除及停止蒐集、處理或利用
	非法蒐集、處理或利用		刪除及停止蒐集、處理或利用
歐盟、英國、德國	特定目的無必要（被遺忘權）	言論自由、資訊自由；法定職務或義務；法律規定；公共衛生公益目的；公益目的建檔、科學、歷史研究、統計；司法訴訟相關；歐盟一般限制要件	刪除及停止蒐集、處理或利用
	非法處理		
	法律要求		
	正確性爭議		
美國 CPRA	自消費者處蒐集之個資	完成蒐集目的之交易、履行契約、依法召回、提供服務必須、維持商業或契約；確保安全及完整性；確保服務安全；言論自由；法律規定/義務；經知情同意、同儕審查或公益目的之科學、歷史、統計研究；符合期待的內部使用；不可	刪除

		能刪除或耗費過鉅	
	敏感性個資	提供服務商品必要、提供特定法定服務、主管機關許可	刪除
日本	事故、可能侵權	非公務機關：成本過高或有困難，得採取必要替代措施；公務機關：他法另訂特別程序、法定事務執行	刪除及停止蒐集、處理或利用
	非法處理		
	已無利用必要		
韓國	一般性刪除權	其他法律禁止	刪除
	一般性停止利用權	法定義務/職務；危害他人生命、身體、財產或其他利益；契約履行	停止蒐集、處理或利用

資料來源：本計畫研究團隊自行整理

二、 小結

綜上所述，各國所賦予當事人權利類型上有所差異，然主要得分為「近用權」、「更正權」及「刪除/停止處理利用權」等三大類。在限制規定上亦有不同類型，如國家利益、公共安全或秩序維護、司法訴訟程序、法定職務或義務等，涉及當事人權利保護之衡平。首先關於近用權行使之限制，如針對公共秩序維護、警察權行使、司法訴訟相關業務等，我國是否有必要明定為近用權之限制要件，考量多數限制要件在法理上屬於不確定法律概念，或在執行上存在技術、成本等障礙因素，目前國內各界尚未對此權利行使限制要件規範有明顯共識，宜觀察各國實際應用情境作為後續調整。又針對特定資料類型如兒童虐待資料等或業務型態近用權之限制，是否均適合規定於個資法，得視國內相關法規完備之程度而定。至於近用權行使方式或頻率，考量相關行政成本得參考美國法之規定，若超過一定期間的次數得酌收手續費用，以免造成權利之濫用。

另有關更正權之部分，係以「維持個人資料正確性」為各國個人資料保護規範共通之原則，除英國、美國加州及新加坡外，日本僅以他法另有規定得限制，多數國家則普遍未限制更正權之行使。而有關刪除及停止蒐集、處理或利用權之部分，其限制要件以歐盟對學術研究之特別規範，學術研究為停止蒐集處理利用之權利行使要件，但同時也是刪除權的權利限制要件。再者，我國與歐盟對當事人權利保護衡平之差異，由於我國個資法規定僅有在當事人權利需要保護時，始得請求刪除或停止處理、利用個人資料；但歐盟則係要求資料控管者須證明其利用相較於當事人權利更需要保護之情形。最後，德國、美國及日本將刪除難以執行、成本過鉅等因素納入刪除權之限制要件，但德國、日本要求須採取如停止利用等替代措施，美國則無採取替代措施之規定。惟目前確實有部分科技之應用，如分散式帳本技術等將使記載之資料難以刪除，考量區塊鏈等應用越加興起，當資料無法刪除或成本過高之情形，應得提供替代措施作為當事人權利保障之手段。

第三章　結論與建議

一、獨立專責機關監督權限行使方式

（一）　獨立專責機關之設置

由於個人資料保護應具有專責性，由獨立專責機關統一監管個資法，負責統一解釋法律與認定事實、執行行政裁罰、監管標準，並促進個人資料保護的專業化，使法律監管具備高度專業性，應具有專屬財務與足夠人力始有利於推動法律執行。此外，設立獨立專責機關可於個人資料保護的事前遵循與教育訓練事務推動上，符合國際潮流並強化個人資料保護的國際合作。

目前我國個人資料保護法並未設立獨立專責機關，由中央目的事業主管機關或直轄市、縣市政府執行監督權限。然憲法法庭於 111 年憲判字第 13 號判決主文二，表示「由個人資料保護法或其他相關法律規定整體觀察，欠缺個人資料保護之獨立監督機制，對個人資訊隱私權之保障不足，而有違憲之虞，相關機關應自本判決宣示之日起 3 年內，制定或修正相關法律，建立相關法制，以完足憲法第 22 條對人民資訊隱私權之保障」。其理由為就資訊隱私權之保障而言，應對所蒐集之個人資料採取組織上與程序上必要之防護措施，其中個人資料保護之獨立監督機制為重要之關鍵制度，目的在於確保個人資料之蒐用，均符合相關法令之規定，以增強個資蒐用之合法性與可信度。至於監督機制如何設置，例如設置一個統籌性之獨立監管機制，或於各相關法律設置依各該專業領域設計之獨立監督機制，屬立法形成自由。[267]多位大法官於意見書補充說明，本判決所稱之獨立監督機制，幾乎已經是重視個人資料保障國家之基本法制要求，且是在

[267] 依據該判決理由二之註說明，例如歐盟 GDPR 即規定各會員國應設置至少一獨立監管機關（supervisory authority），職司個人資訊隱私權之保障；該監管機關應依照 GDPR 規定獨立行使職權（GDPR 第 51 條及第 52 條參照）。

我國憲法正當法律程序原則下，不可或缺的事前與事中程序性控制的保障。惟判決就如何設置並未有定見，或可參考國際相關立法趨勢，研議建置個人資料保護的獨立監督機制。

關於我國現行之獨立機關組織規範，依中央行政機關組織基準法之規定，首先其不受其他機關指揮監督。第二，組成上應為合議制機關，原則上成員數量應為 5 至 11 人。第三，合議制成員及正副首長受有任期之保障，相當於中央二級機關之獨立機關，其專任合議制成員任命應經立法院同意；其他獨立機關，一級首長由總統任命。目前相當於中央二級機關之獨立機關總數共計 3 個，包括中央選舉委員會、公平交易委員會、國家通訊傳播委員會；而其他獨立機關，相當於中央三級機關共計 2 個，包括國家運輸安全調查委員會、不當黨產委員會。考量二級獨立機關有數量上限為 3 個之規定，如從既有機關選擇作為獨立專責機關亦為一種方式[268]。

惟若需另立新的獨立專責機關，得參酌國外立法例之獨立專責機關設立方式。依歐盟 GDPR 就獨立專責機關之要求，即認定要素主要分為以下五點：（1）地位獨立，即獨立地位須有法律保障。（2）任命獨立，即委員的提名、解除與任期等需以法律定之，不受政治影響，並須具備相當之專業能力。（3）功能獨立，即決策權不受任何直接或間接之外部影響，包括公、私部門影響。（4）成員獨立，即有權獨立選擇其成員，且該等成員僅受其指揮監督。（5）資源及預算獨立，即須有足夠之資源以有效行使其職權，包括固定、專用的預算，且相關籌備機制亦不受政治或財務控制而影響其獨立性，並須有相應之人力資源。然而，EDPB 在 2022 年 9 月 5 日發布一項調查成果，針對各個成員國在 2020 至 2022 年間對於資料保護主管機關所提供的資源進行調查。關於調查統計區分為經濟資源及人力資源兩大類：（1）在經濟資源的部分，投入最高者為德國，2022 年的預算高達 1

[268] 個資法規範上除了人權保障，亦帶有公平競爭的色彩，在非公務機關之監管部分，由於公平交易委員會、通訊傳播委員會均有委員任期保障的概念，對於保持機關的獨立性相對容易，或許得考量改制作為個資法的獨立專責機關行使其監督權限。

億 1 千萬餘歐元，次高者為義大利則有 4 千萬餘歐元，最低者為馬爾他則約 68 萬歐元，其中有 77%的成員國認為國家在資料保護領域所提供的經濟預算仍有不足。(2) 在人力資源（本年度之人數，非指在職人員）的部分，投入最高者為德國於 2022 年投入人力為 1155 人，次高者為法國有 263 人，最少者為奧地利僅 0 人，其中有 87%的成員國認為國家所提供的人力仍有不足[269]。因此設置獨立專責機關仍需考慮執法層面上是否有足夠的經濟資源及人力資源，避免耗費過大的行政成本。

（二）　監督權限行使方式

首先在調查權限行使方式上，各國獨立專責機關之調查權限大致相似，包含命提供資訊、進行調查、通知違法情況、獲取資訊，以及實地調查等權限。針對調查權之執行，依各國行政程序差異，規範略有不同，如德國要求機關須在一定之期限內作出回應；英國則強調命提供資訊應先為資訊通知、進行調查應先為評估通知；新加坡則分為持法院搜索令進入場所檢查，或在必要時透過發出通知後直接進入場所檢查。而除了歐盟之外，多數國家並未規範怠於行政處理之救濟程序。在歐盟 GDPR 體系，若獨立專責機關未處理當事人之申訴或是未於三個月內通知調查進度或結果，當事人有權向成員國國內法院訴求司法救濟。至於在調查委外的部分，日本、韓國可委由其他單位協助進行調查，如日本個人資料保護委員會得將報告及進入檢查之權限委任由事業所管大臣、金融廳、證券交易監視委員會等行使，前述機關則應向委員會報告前述權限行使結果；韓國則規範資料控管者於處理個人資料有侵害資料當事人權益之虞時，受侵害者得將被侵害事實向委員會通報，委員會得指定專門機關 KISA 之隱私申訴中心受理，進行調查與個人資料保護爭議有關之申訴案件；瑞士則規範聯邦資料保護及資訊委員得在調查範圍內召集其他聯邦機關

[269] EDPB, *Overview on resources made available by Member States to the Data Protection Supervisory Authorities*, https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf (last visited Sept. 28, 2022).

與地方政府警察機關執行。

相較之下，目前我國個資法第 22 條有關行政檢查之規範，包含進入檢查、命說明提供文件、扣留等，已有與國際立法例相似之調查權規範，並未有明顯差異。此外，日本、韓國、瑞士有與外部單位合作執行調查程序；我國亦有委外調查之規定，惟係主要由各主管機關執法。若將來設置獨立專責機關，委外權限應區分係單純委託，或是同時涉及其他部會的職責及監督權限，建議考量有無必要應於法律中明訂委託事宜。另在多數國家於調查程序中，司法不會介入調查，惟美國得由檢察總長隨時介入調查程序，歐盟體系則僅在獨立專責機關三個月內未回覆調查進度或結果時，始得進入司法救濟，此部分由於涉及機關之獨立性與權利救濟之途徑，亦應審慎衡酌之。

其次，關於處分權限行使方式，各國對於獨立專責機關之處分權限大抵內容相似，主要包括發布警告、發布訓誡、命令遵循當事人要求、命令符合法規規範、命令通知侵害、課予限制、命令更正刪除、行政罰鍰、命令停止國際傳輸、執行通知（限期改正）等權限。在受處分之救濟程序上，多數國家採直接進入司法救濟程序有關救濟程序之細節，亦因各國行政程序體系而略有差異，如美國加州檢察長雖有權優先接手案件移轉，加州隱私保護機關不得限制州檢察長執行本法之權力，惟若 CPPA 處分已作成，則受處分企業應依據處分結果，直接進行司法救濟。而新加坡則針對替代性紛爭解決、違規指示、自願承諾或依審查權等作出之任何指示或決定，可依書面申請由 PDPC 重新再議；若不服再議結果，則可在規定期間內向再申訴小組主席提出再申訴。至於在裁罰規範上，除美國、新加坡之個資法本身即未規範公務機關之外，僅瑞士與我國類似，針對公務機關均無裁罰相關規範，其他多數國家之獨立專責機關可針對公務機關進行裁罰。另在處分權限的委外規定，日本賦予委員會得將勸告及命令之權限委任由事業所管大臣、金融廳長官、證券交易監視委員會等行使；而前述機關應向委員會報告該權限行使之結果。

目前我國個資法第 25、47、48 條已有規定，中央目的事業主管

機關或直轄市、縣市政府對於違法者得處以不利益處分。其類型包含禁止蒐集、處理或利用個人資料；命令刪除經處理之個人資料檔案；沒入或命銷燬違法蒐集之個人資料；公布非公務機關之違法情形，及其姓名或名稱與負責人等。而我國相較於國際，已有類似於國際之處分權規範，惟尚由各主管機關進行執法。多數國家之獨立專責機關可針對公務機關進行處分，除美國、新加坡本身未規範公務機關之外，僅我國、瑞士之個資法並無針對公務機關之裁罰權限。另外，多數國家之獨立專責機關所作處分結果不受上級管轄，若受處分者不服獨立專責機關之處分，新加坡有採另組委員會進行審議，而其他國家則採以直接進行司法程序救濟。

綜上所述，各國獨立專責機關之監督權限行使方式，與我國目前個資法所賦予之權限並無太大差異。由於 GDPR 之規範多討論獨立專責機關之行政查察功用，設立獨立專責機關將能夠確保個資法各項法律定義及管理配套之一致性，如進行資料隱私衝擊評估之諮詢，以及指引之頒布。尤其在去識別化、資料可攜性等議題，可能需於不同應用領域之法規雙向進行，須由獨立專責機關監管，以建構完善之資料治理制度保障環境。

二、罰則

綜觀各國法制，多數國家均有將刑事罰及行政罰納入罰則之規範，惟由於各國規範之個人資料運用行為本存在差異，故在裁罰之客觀要件上亦有所不同，主要得歸類為針對違反資料運用之合法要件、控管者義務、當事人權利、目的外利用、國際傳輸、妨礙調查等情形之規範，且針對特種個人資料之處理設有較重之罰責。

關於刑事罰之規範，我國個資法第 41、42、44、45、46 條針對刑事罰之規定均有處罰故意犯，而未處罰過失犯，刑責最高得處 5 年以下有期徒刑，且得併科新臺幣 100 萬元以下罰金，另針對公務人員有加重處罰之規定。而各國雖有部分國家在行政罰會依據受處分對象規模調整，但在刑事罰之罰金部分，皆似我國係採固定額度上限

之作法。至於各國罰金之額度換算大約為 20 萬至 200 萬新臺幣區間，我國為 100 萬新臺幣以下，在各國罰金之額度屬於居中之位置。至於在主觀要件上，目前國際立法例僅韓國有特別針對意圖部分課予加重刑責規定，多數國家則未針對意圖限縮刑事罰範圍，且有處罰過失情形，因此處罰之範圍較大。我國原則上將違反個資法之行為係以民事損害賠償、行政罰作處理，而刑事罰則限縮在行為人意圖為自己或第三人不法之利益或損害他人之利益有違反本法相關規定之情形。考量過失犯的處罰可能對非公務機關運用個人資料產生過大疑慮，建議針對意圖或有惡意之不法行為處以刑事罰，強化一般大眾對於個資法效力的信賴，並產生一定的威懾效果。至於日本、新加坡針對有違反主管機關命令或偽證等情形處以刑事罰之規範，若未來我國設置個人資料保護之獨立專責機關，考慮此涉及刑事犯罪之行為，亦可考慮增加相關刑責規定。

相對地，歐盟、美國多以行政罰作為未履行個資法義務之裁罰手段，但各國行政罰之裁罰基準、程序、處罰對象仍有差別。以我國個資法之行政罰規定是否以命改正作為前置程序之要件，係視違法情狀得否改正或已破壞法秩序的平衡作規範，相較於國際立法例皆未要求機關須先命其改正始得處罰，給予主管機關在裁罰上具有更高的彈性。至於須否裁罰公務機關，觀察多數國際立法例均有裁罰公務機關之規定，我國目前並未針對公務機關有裁罰機制，然而基於平等原則，無論公務機關或非公務機關均有違反個資法行為之可能性，實務上公務機關發生個資外洩或濫用情事屢見不鮮，政策上建議未來修法應納入而非以差異化處理。另外在非公務機關之代表人、管理人或其他有代表權人之處罰，多數國家與我國個資法均有處罰之規定，考量代表人等對於該非公務機關落實個資法遵之可能性具有一定之影響力，相較於行政罰法第 15 條主觀要件及罰鍰額度的限制，建議保留於個資法以生警示作用。最後在罰鍰額度的規定上，鑒於歐盟體系、英國、新加坡、韓國均採行依受處分對象規模調整罰鍰之額度，以針對不同規模的對象達成懲罰之效果，而我國、日本之行政罰鍰則係採固定額度上限。在政策建議上如我國維持採行固定額度之制度，

應上調目前的罰鍰額度，但應訂定最高額度及最低額度，給予受規範對象有預見可能性及主管機關裁罰上的彈性空間；惟若採行比例計算罰鍰額度，則建議仿效新加坡模式以本國營業額作為裁罰標準，避免業者調降資本額以規避罰鍰，或歐盟採行全球營業額之模式可能造成主管機關查證行政成本過高。

由於罰則的規範強度將影響受規範對象履行個資法之可能性，過低的罰責可能無法發揮嚇阻效果，進而阻礙個資法遵之落實。然而過高的罰責亦可能導致創新技術與商業模式的發展。基於個人資料之保護，實有賴個資法之罰則作為最後一道防線，以嚇阻違法蒐集、處理或利用個人資料之各種行為。尤其在數位經濟時代，科技巨頭或大型電子商務企業更應投入個資法遵之成本，故建議未來應透過修法提高罰則之強度，至於有期徒刑之刑度、罰金或罰鍰之額度須待各界凝聚共識後再研議。又將來我國設立獨立專責機關後，建議將處分權限及罰則之規範一併做相應調整，以發揮統一監管功能達到落實個人資料保護之目的。

三、 共通規定

（一） 豁免情形

各國法制的豁免情形規定，主要得概分為政府行為、私人活動或其他私領域行為，以及基本權競合等三類。又針對不同豁免類型可分為全域豁免（例如具有歐盟 GDPR 第 2 條第 2 項所規定之四種豁免情形之一者得排除整部 GDPR 之適用），以及細分為部分豁免之情形。第一類「政府行為」包含統治行為、公務機關執行公務、刑事案件機關程序、刑事案件或少年保護案件之程序、議會訴訟程序等。目前歐盟、日本、韓國等國家在刑事訴追過程等程序上，因有其他法律調和，故於個資法有豁免。第二類「私人活動或其他私領域行為」主要為個人日常活動、單純個人或家庭活動、商業契約或商業活動、民法公開登記、受雇或應徵資料等。在個人家庭活動之部分，幾乎所有國家皆有豁免，較無爭議；受雇應徵資料、或企業內部管理為美國特

別強調；商業契約則為新加坡特有規範。第三類「基本權競合」主要有諸如新聞媒體或出版自由、宗教自由、政治自由、學術自由、藝術自由等基本權利，該相關權利與隱私權之競合，例如歐盟體系特別針對言論自由相關權利（新聞目的及學術、藝術或文學表意目的）有部分豁免規定；日本、韓國等國家則有進一步針對宗教、政治等權利給予部分豁免；有關新聞、藝術、文學或研究目的，菲律賓為全域豁免。

目前我國個資法規定之豁免情形依第 51 條第 1 項，已將個人日常生活中合理利用行為或是公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料，予以排除個資法之適用範圍。而我國個資法排除自然人單純為個人活動目的，而各國相較我國，則有更多針對政府行為、私法行為（如商業契約）、基本權（如言論自由）等之豁免情形。然而在擴大豁免情形之範圍前，仍應衡酌各該領域是否已有完備法制作為個人資訊隱私權之保護，視情形得採整部法規豁免、部分章節或條文之豁免。另基本權如新聞、學術、藝術、文學之目的，較普遍於國際立法例列入豁免情形之規定，將來我國修法得參酌各國在豁免情形規定的設計上，考量是否納入相關基本權競合，或以公共利益、唯一目的等作為豁免之適用前提要件。

此外，我國個資法第 51 條第 2 項「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」規定，未見於其他國家有相類似之豁免立法例，且條文因缺少規範主體，易滋生豁免主體範圍爭議。雖我國相關函釋之實務見解已排除豁免基於職業或業務職掌之公開場所或公開活動影音資料蒐集、處理及利用，惟我國個資法並無類似公開場所或公開活動錄影監視錄影設備之管理規定。雖近年在特定領域逐漸有立法規範，如跟蹤騷擾防治法屬針對公共場所管制的規範，以及尚未通過的科技偵查法等。惟在公共場所錄影監視等行為仍有侵害隱私之疑慮，新興科技如無人機等載具多為公開場所蒐集個人資料，亦應在政策面上考量是否納入。關於各國針對監視器設置的規範，德國、韓國已將之納入個資法，或日本發布指引等作法，值得我國為借鑑。

（二） 域外效力

從我國個資法結構觀之，第 51 條第 2 項僅針對保護我國公民，而我國域外效力管轄範圍，僅針對境外之我國蒐集主體對我國人民個人資料之蒐集、處理、利用行為。其立法理由係為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任。相較於各國立法例，常見域外效力分為「蒐集主體在境外，對境內自然人個資之蒐集處理利用」，及「我國蒐集主體在境外，對境外之我國人民個資之蒐集處理利用」之情形。多數國家亦均以向境內人民提供服務或商品，及以監控境內人民個人資料運用作為域外效力之要件。惟目前我國並未針對境內未設實體，但有蒐集、處理或利用我國境內人民個人資料之情形規範。因此我國個資法第 51 條第 2 項不宜逕以解讀為類似歐盟 GDPR 第 3 條第 2 項之域外效力。

由於我國經濟大幅仰賴國際貿易，在經濟活動上常涉及跨國的個人資料蒐集、處理或利用行為，又考量各國在個資法的適用上均有擴大適用範圍的趨勢，為保護我國人民個人資料被妥善運用，對於境外控管者蒐集、處理或利用境內人民個人資料之行為應有納入規範之必要。惟制定域外效力的規範將可能對國際貿易產生相關影響，仍應審視我國政治經濟背景與競爭力能否有效支持，若規範過嚴可能導致外國企業放棄我國市場，故應從個人資料與產業發展之間衡平的角度，在實際操作上透過執法權協商或做出其他認定標準。參酌現行已有將「針對境外法人或自然人對境內人民之行為」納入規範之國家，均已設有個資法之獨立專責機關，惟我國個資法目前係由各中央目的事業主管機關採分別管理，因此如將來我國個資法明定域外效力，則應建置相關配套措施，避免在執法層面上行政量能不足，否則域外效力條款僅有宣示的效果。

（三） 國際傳輸

由於各國已逐漸重視個人資料保護，為促進數位經濟快速發展，

無論公務機關或非公務機關均有將個人資料進行國際傳輸之需求。然而如何保障國際傳輸後之個人資料仍可以受到一定程度保護，為各國亟欲解決之問題。自歐盟施行 GDPR 以後影響日本、韓國、新加坡等亞洲國家對於資料保護之態度。綜觀各國個人資料保護規範，對於個人資料國際傳輸之限制有不同處理模式，如美國基於資訊自由化及貿易自由的角度，採取「原則開放，例外限制」；而歐盟及日本、韓國等多數國家為強化個人資料保護，則採「原則限制，例外允許」。其中韓國採行之互惠條款，得作為國際傳輸之武器對抗他國不合理之限制。

因此可見多數國家透過立法與政策保護該國人民之個人資料，保護資料不隨意遭到竄改、侵害或外洩。而目前各國普遍強化國際傳輸規定，多採「原則禁止，例外允許」之國際傳輸規定，同時當涉及機敏資料、國家安全等議題時，亦會限制其傳輸。相較於其他國家，目前我國在國際傳輸的管制程度較低，似不利我國人民之當事人權益保護，故建議我國個資法之國際傳輸條款應修法，調整為「原則禁止，例外允許」。

若修法調整國際傳輸條款，關於例外允許之合法要件，得考慮採納接收地之個資保護水準相當、企業採行適當保護措施及特定情形；可先以指引建議企業採行適當保護措施，如企業自我拘束規則、標準契約條款、行為守則及認證，企業得視其規模選擇適合之類型。首先，接收地之個資保護水準相當得參考日本建立白名單制度，由主管機關公布可信賴國家以免除國際傳輸之限制，且於必要時仍得附加條件限制傳輸之範圍。其次，企業採行適當保護措施得分為企業自我拘束規則、標準契約條款、行為守則及認證，企業得視其規模選擇所採行之類型，並應採取補充措施。最後，當接收地之個資水準未相當且企業無採行適當保護措施時，僅於特定情形時得允許國際傳輸，如當事人知悉風險仍同意、保護個人重要利益及保障重要公共利益時，惟若依據此一要件時應就個案判斷，並採行相應之配套措施，且許可應限於一次性傳輸。考量國際傳輸之限制將對企業產生相當影響，合法要件應盡量以原則性方式規定為宜，並審慎評估相關影響訂定國際

傳輸之管制模式，以接軌國際資料保護法制。

四、 蒐集主體及受託處理者

（一） 蒐集、處理及利用之合法要件探討

個人資料蒐集、處理及利用之合法性要件，主要涉及一般個人資料與特種個人資料之法律概念，以及蒐集、處理或利用行為區分不同階段、受規範之主體為公務機關或非公務機關、特定目的之解釋等立法例選擇。然而蒐集、處理、利用三種行為樣態，隨著科技技術發展已難以清楚劃分資料處理與利用之階段，容易衍生後續法規適用上之疑義。以機器學習為例，其演算法之運算，就可能同時涵蓋上述處理定義中所列的編輯、複製、檢索、連結等行為，亦可能有未能於上述定義涵蓋的其他被歸類為「利用」的行為。若將演算過程區分為處理、利用行為，在法律適用上會較為複雜。

從國際立法例觀察，按照運用行為區分個資運用合法性要件者多為亞洲國家，如我國、日本、韓國及新加坡；而未以運用行為區分的，則以歐美國家為主，包含歐盟、英國、德國及美國。我國在電腦處理個人資料保護法立法時，係參考德國當時有效的德國聯邦個人資料保護法，將個人資料運用分為蒐集、處理及利用這三個不同型態，惟德國在合法性要件上則是分別規定蒐集之合法要件及「處理、利用」之合法要件；而德國在 2017 年修法時，已配合 GDPR 規定不再區分個資運用的行為樣態，皆以「處理」規範之。日本、韓國及新加坡雖區分個資運用行為，惟其規定是將「提供第三人」的行為與其他處理樣態分開，形成「蒐集、處理、提供」的規範模式，與我國規範模式仍有差異。而「蒐集」涉及資料之取得，「提供」涉及資料控制權限之轉移，其風險型態確實與其他的處理程序有別。考量數位時代下演算法運算可能同時涵蓋個人資料蒐集、處理及利用之行為，在概念上將逐漸難以明確區別，建議可參考歐盟、美國不以運用型態區分合法性要件；若仍採取區分模式，為使受規範者具有可理解性及預見可能性，建議可依據特定行為之風險予以區分所受規範，例如參考

日本、韓國對於提供第三人之行為另為規範。

又關於受規範之主體，我國個資法有依照其組織性質區分為公務機關及非公務機關，然從國際比較立法例觀察，目前除美國及新加坡個資法規範本就排除公務機關適用外，各國並無明顯的規範選擇偏好，而採取不同的立法模式。其中歐盟、英國、韓國於章節架構及個人資料運用合法要件上並未區分公務、非公務機關，僅有部分條文為特別規定；而現行之德國法亦未於章節架構上區分公務機關及非公務機關，但於個人資料運用的合法要件上，特別加以區分，並規定公務機關之私法行為適用非公務機關之規定；日本則與我國相同，依照組織型態的不同，於個人資料運用合法要件及章節架構上，分別以公務及非公務機關加以規定。從立法歷程觀察，我國電腦處理個人資料保護法立法時係參考當時有效之德國法，採取公務機關、非公務機關分別訂定不同個資運用要件、並以不同章節分別管理的模式，而德國已於 2017 年時，配合歐盟 GDPR 的立法，調整法律章節結構，僅於個人資料運用合法要件上，保留公務、非公務機關的區分方式。

從立法模式而論，區分公務機關、非公務機關的立法模式，其假設公務與非公務機關性質有別，應以不同規範規定；而不區分兩者的立法模式，則認為個人資料運用與管理之基礎原則相通，因此應以同一規定處理為原則，僅於例外部分為特別規定。前者理論上可依機關性質量身打造適合的規範，但立法上須避免掛一漏萬而造成適用困難；後者則雖然大多數要件可一體適用，較不易有涵蓋不足問題，但立法時需以「原則－例外」方式設定要件。總體而論，尚無明顯之優、劣。至於合法性要件上，目前多數國家無論是針對一般個人資料或特種個人資料，多以「公共利益」、「保護個人利益」以及「取自公開資料或一般可得來源」作為其運用個人資料之合法要件，然法理上有屬於不確定法律概念，於具體適用態樣上，目前國內各界尚未有明顯共識，考量此屬於非急迫性議題，宜待觀察各國實際應用情境作為後續規範調整。

另在個人資料之運用上，我國個資法係要求個人資料蒐集時，需

確定個人資料蒐集之特定目的，後續的處理、利用行為原則上需於該特定目的範圍內進行，並針對原蒐集之特定目的外之利用行為，定有目的外利用之合法性要件。比較法上，歐盟則要求若其他利用行為之目的，與原先之蒐集目的不一致時，須取得當事人之同意或會員國依照 GDPR 授權之特別法規定，方可為個資處理；否則須通過「相容性檢驗」（compatibility test），確保進階處理（further process）的目的與蒐集的目的相容。此種相容性檢驗須考量因素，包括蒐集目的與進階處理目的間之連結（link）、蒐集之脈絡（context，尤其是當事人與控管者間關係）、資料本身之性質（例如是否為特種個人資料）、進階處理對當事人可能之後果、所採取之適當保護措施。此種相容性檢驗的規範模式，其優勢在於可以強化個人資料保護程度，因為若透過「相容性檢驗」的方式，將類似但不完全相同的運用目的包含在原蒐集之特定目的範圍內，則可避免控管者擔心資料利用受限，而主張較為寬泛的蒐集目的，反而讓當事人不易預見資料可能被處理的樣態。且相容性檢驗這種考量處理行為之脈絡、影響的作法，似乎可以取代「有利於當事人權益」等要件，要求控管者在進行與原始蒐集目的不同之處理行為時，考量脈絡、影響等因素，以強化對當事人個資安全之要求；惟其劣勢在於相容性檢驗的複雜性也可能造成執行上的困難。質言之，相容性檢驗判斷過程須考量眾多不確定因素且難度高，對控管者而言，可能增加法遵風險；對當事人而言，也增加確認處理行為合法性的困難度。而我國個資法針對特定目的之解釋，鑒於第 53 條規定：「本法所定特定目的及個人資料類別，由法務部會同中央目的事業主管機關指定之。」，目前法務部所發布之特定目的類別，僅為例示規定，並無法完整涵蓋所有情形，運用上有部分類型不易釐清。然而，若未來將設立獨立專責機關，則可透過機關發布指引等形式解決疑義，在產業運用上採行較嚴格的規範仍可運作，故尚非急迫議題，可持續觀察之。

（二）　受託處理者義務

在資通訊快速流通的時代，許多企業在專業化及整體成本的考量下，會選擇將非核心業務委由專業公司處理，而其中若涉及個人資

料的委外，則會產生委外業者蒐集、處理與利用個人資料之問題，並可能涉及適用個資法上的委託關係之相關規範。

觀察各國立法例在個人資料委託之規範，多數國家有明確定義資料控管者與受託處理者。目前我國個資法對於「委託機關」及「受委託機關」並無定義，但綜觀國際間多數國家，多以是否決定個人資料運用之目的、方法，或僅依其指令處理，作為委託機關（控管者）、受委託機關（處理者）之定義。又在進入資料、數位經濟時代後，資料利用的樣態漸趨複雜，許多資料利用樣態似乎並非單純的委託與被委託關係。歐盟為處理漸趨複雜的個人資料運用行為樣態，引入「共同控管者」概念，要求「共同決定資料運用目的或方法」的不同資料控管者，必須約定彼此對法定義務的責任安排。至於在委託關係的監督管理，各國多以法律方式要求委託者與受委託者間，應以書面方式約定資料利用方法、安全維護措施、複委託等事項，並要求委託機關應監督其落實，並課予受委託機關安全維護、通報等責任。相較之下，我國目前並未以法律規定委託關係間之監督管理責任，僅於施行細則中要求委託機關就特定事項監督受委託機關。

考量因應數位時代強調產業分工，有必要協助產業釐清委託者與受託者之間的關係，尤其現階段法規之相關責任義務及定義皆不易釐清，對消費者個資保護較為不利。美國在此議題上，亦採納類似歐盟的規範。此外，我國目前施行細則要求控管者對受託處理者之監督管理責任，應考量專業能力差距，評估是否維持現行監督管理的規定。因此在政策上建議透過修法將個資法的受託處理者義務明定，且在修法前宜先以法規命令或指引加強，使業者在委託關係、複委託關係中簽訂契約落實個資法之監督義務及妥善運用個人資料。

五、產業應用

（一） 科學研究

我國有關因學術研究而蒐集、處理及利用個人資料之規定，主要涉及個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項

第 4 款及第 20 條第 1 項第 5 款。關於上述學術研究條款之規定與資訊隱私權、個人資料自主權之衝突，憲法法庭 111 年憲判字第 13 號判決針對健保資料庫案，判決主文一表示個資法第 6 條第 1 項但書第 4 款規定與法律明確性原則、比例原則尚屬無違，不牴觸憲法第 22 條保障人民資訊隱私權之意旨。其理由為系爭規定中「公務機關或學術研究機構」、「醫療、衛生目的」、「為統計或學術研究之必要」均屬客觀上非難以理解之用語。系爭規定容許公務機關或學術研究機構為醫療或衛生之法定目的，於統計或學術研究之必要時蒐集、處理及利用個人健保資料，並規定相關要件，其意義尚非難以理解、受規範者所不能預見，或無從經由司法審查加以認定及判斷，與法律明確性原則尚無違背。但認為系爭規定係指基於醫療或衛生法定目的，為統計或學術研究必要而蒐集、處理及利用個人健保資料之際，應採取去識別化之措施，使資料不含可直接識別特定當事人之資訊，但其資料仍屬可能間接識別特定當事人之資訊之情形。因此我國現行個資法有關學術研究條款並未違憲，如符合特定主體、特定目的及必要性，並採取去識別化之措施，則可基於學術研究將個人資料進行合法目的外利用。

惟司法院大法官釋字第 380 號解釋認為，所謂「學術研究」係指針對有系統而較專門之學問中的特定主題，作深入且有系統地探討或研查，以發現事實，形成理論並付諸應用。上述說明係屬抽象之法律概念，尚難遽定其範圍及認定標準，而仍須依具體個案分別認定。綜觀各國法制，歐盟、英國、德國及韓國以「科學研究」作為規範用語，美國、新加坡及菲律賓以「研究」為規範用語，僅日本同我國係以「學術研究」作為規範用語。由於規範用語的定義與內涵，將影響資料合法運用要件的適用問題，包括適用的主體及合法事由等法律要件，均將影響產業是否有基於研究或科學研究之目的，而發展資料經濟之利用可汲性。目前除了菲律賓明顯規定基於研究目的而處理個人資料，排除於個資法之適用範圍外，可清楚地區分為二大類型：如屬於歐盟、英國、德國、美國、韓國或新加坡等國家，定義為「研究或科學研究」者，則其適用主體上將不限制為特定主體，而在合法

事由上得基於該研究或科學研究目的，即可為之，而無需限於特定公共利益之目的；但歐盟國家與美國針對研究或科學研究之概念，係限於一定研究方法、研究倫理與隱私法規等範圍。另一類則係我國與日本皆以「學術研究」作為規範用語，並限於特定主體始得適用本款合法事由，但相較於日本之規定，我國之一般個人資料限於公共利益目的，而特種個人資料限於醫療、衛生或犯罪預防之目的。

若未來我國修法調整學術研究條款，除需體系性考量是否配合目的內與目的外利用、公務機關或非公務機關，以及是否區分蒐集、處理或利用等框架性問題調整外，建議一併修改相關規範用語，放寬本款之適用主體，亦得考慮刪除合法事由之特定目的限制，但有關特種個人資料之額外保護措施，可考慮以特種個人資料程序性控管規定加以保障，或另由特別法或授權目的事業主管機關以命令，加以規範為宜。而關於學術研究之彈性措施，我國目前若以學術研究作為蒐集、處理或利用個人資料之目的時，可為目的外利用或免為告知義務，但相較於比較法上其他國家之規定，現行彈性措施仍有調整空間。考量研究業務範疇涉及科學技術發展、產業創新研發及社會生活之提升，若能適度地提供資料流通或彈性放寬研究等特殊規定，將有助於資料經濟之運用與發展。又為避免阻礙創新技術發展，在數位經濟時代為因應各種新興科技與新商業模式的出現，解決現行法規與新興科技的落差，有關科學研究運用醫療個人資料等相關討論，或可採用監理沙盒方式，尤其數位時代快速變動，可能出現許多創新型態的商業模式，恐難以事先推估。惟若採用監理沙盒制度，建議仍須由各部會之監管立場為主導，或設立獨立專責機關統一進行監管為宜。

（二） 假名化及匿名化

綜觀各國法制，有將去識別化依照資料加工程度所呈現之狀況區分為匿名化及假名化，所產生之法律效果及適用之管理規定亦有作區別。相較之下，我國個資法對於去識別化之內涵仍存在模糊甚至衝突之見解，對去識別化作業工具亦未有明確定義，其結果便導致我國在個人資料保護上之立場並不一致，並頻頻受到挑戰；而類似之挑

戰又將使我國在大數據時代下，應如何規範個人資料之釋出與利用處於不確定狀態，不僅個人隱私權之保障可能因此受到侵害，須利用健保資料之政策分析或學術研究亦將因此延滯。因此，如何在政策執行與法律操作層面，將去識別化之概念進一步明確化與具體化，實應屬我國個資法未來發展所應思考之方向。

過去實務見解多認為去識別化之定義，係指個人資料經提供者處理後或蒐集者依其揭露方式達到無從再識別特定當事人之程度，而由於該筆經提供者處理後之資料或蒐集者揭露之資料，已非個資法第 2 條第 1 款所定「得以直接或間接方式識別該個人之資料」，即無個資法之適用。實務上並認為個人資料去識別化之行為應定性為個資法第 2 條第 4 款所稱之「處理」，因要求去識別化資料須達到無從直接或間接識別特定人之程度，故去識別化之加工處理並未增加對當事人權益之額外侵害，故過去認為資料去識別化應達到「完全匿名」之程度，始謂去識別化資料，排除有間接識別可能性之假名化技術。而關於去識別化在個資法所發生的法律效果，實務上並未區分「適用學術研究條款」或「排除個資法適用」兩者。

然而在憲法訴訟健保資料庫案，憲法法庭 111 年憲判字第 13 號判決認為以「經過提供者處理後或揭露時無從識別特定之當事人」為利用個人健保資料之合法要件，亦即為醫療、衛生法定目的，蒐用個人健保資料，其提供者至遲於揭露時須為已經採取去識別化措施處理，使該個人資料成為非可直接識別當事人之資料。因此系爭規定課予採取去識別化措施之義務，使一般人採取當時存在技術與合理成本，在不使用額外資訊時，不能識別特定當事人，已足大幅降低蒐用個人健保資料所生之個人資訊隱私權所生之侵害。若屬於完全不具還原識別可能性之匿名資料，已非受憲法第 22 條資訊隱私權保障之個人資料；而且匿名資料固非全然不具學術研究價值，但已喪失病歷、醫療、基因及健康檢查資料作為學術研究樣本時可擇定變因交互比對、建立相關性之特性者，將無從達成系爭規定所欲追求之特別重要公益目的。綜上所述，本案判決認為資料去識別化僅須達到「假名化」之程度，仍具有間接識別可能性，故認為去識別化資料屬於個資

法第 2 條第 1 款個人資料，並明確認定去識別化之效果為「適用學術研究條款」且應適用個資法相關規定。

在數位時代下如何在資料保護與資料利用之間取得適當衡平，建構完善的去識別化制度為重要關鍵。基於法律穩定性及技術日新月異難以窮列，應採取技術中立原則。惟涉及去識別化技術之可行性，以及重新識別之風險問題，宜先以指引累積國內經驗後，建立從去識別化的加工處理、管理措施、禁止義務到驗證之整體制度，再修法定之。考量各國多已起步發展相關技術及應用，在政策上建議我國於修法前先以發布指引的方式提供給產學界參考，至於修法可能性因涉及技術相關問題，應待各界凝聚共識再研議。

六、 當事人權利

（一） 資料可攜權

綜觀各國法制，目前多數國家對於資料可攜權之規範，首先在形式要件上，資料應具備結構性、通用性及機器可讀性，且傳輸對象應包含當事人及第三方，始達到資料可攜之目的。其次，在資料可攜權之行使要件上，歐盟 GDPR 體系強調應以當事人同意或履行契約作為合法處理要件，且以自動化程序處理為必要；澳洲 CDR 則強調消費者資料權應限於當事人同意，且接收方須取得適格性認證；美國 CCPA 則採一般性承認當事人均得行使資料可攜權。其三，對於例外情形得限制當事人行使資料可攜權之規定，歐盟 GDPR 體系以公共利益、他人自由及權利等類型為主；相對地，澳洲 CDR、美國 CCPA 則未作例外限制，對於符合行使要件之情形，即一般性承認當事人得行使資料可攜權。最後，由於資料可攜權應用領域廣泛，除了透過個資法作一般性規定外，亦有國家透過另定特別法或相關政策推動資料可攜制度，為避免實施上對於產業造成過大衝擊，亦可採取相應之配套制度。由於開放銀行已是全球金融趨勢，透過使用者同意資料可攜式授權將資料開放、共享，提供銀行進行跨產業合作。除了金融業之外，歐盟 GDPR 對於應用資料可攜之產業並不設限，而澳洲則亦

有在電信業、能源業等其他產業實施資料可攜制度。

與之相比，目前我國個資法之當事人查詢或請求閱覽、製給複製本之權利，並未要求應以電子形式提供個人資料予當事人，亦未賦予當事人得將資料作移轉，甚或得請求原控管者將資料傳輸予其他控管者，因此難謂有可攜之概念，故我國個資法尚未保障當事人具有資料可攜之權利。因目前資料可攜仍存在技術障礙，包括資料標準化機制之建置、自動化資料輸入及輸出管道等技術門檻，對中小型業者可能造成負擔甚大，在政策上建議針對資料可攜權之行使與制度的建立，先以鼓勵之方式推動，較為可行。另外基於資料可攜具有創造資料價值、促進公平競爭之目的，除了透過個資法作一般性規定，亦可考慮透過競爭法或相關政策推動資料可攜制度。因此建議可先以發布指引的方式提供給各界，引導業者採取適當因應措施，至於後續修法之可能性須再研議。

（二） 被遺忘權

由於被遺忘權係從刪除權所延伸之當事人權利，亦為當事人對於其個人資料事後控制的權利類型之一。綜觀各國法制，有關同意之撤回及對於個人資料之事後控制，許多國家對於當事人請求停止利用或刪除個人資料之行使，亦設有限制之規定。而我國學術及實務討論上，退出權之概念為個人資料被蒐集後，當事人可要求停止為特定處理或刪除個人資料之情形，屬於當事人之「事後控制」權，並納入為「退出權」之範圍。

在憲法訴訟健保資料案中，依憲法法庭 111 年憲判字第 13 號判決之主文四表示，「衛生福利部中央健康保險署就個人健康保險資料之提供公務機關或學術研究機構於原始蒐集目的外利用，由相關法制整體觀察，欠缺當事人得請求停止利用之相關規定；於此範圍內，違反憲法第 22 條保障人民資訊隱私權之意旨。相關機關應自本判決宣示之日起 3 年內制定或修正相關法律，明定請求停止及例外不許停止之主體、事由、程序、效果等事項。逾期未制定或修正相關法律

者，當事人得請求停止上開目的外利用。」。其理由認為憲法第 22 條保障當事人就獲其同意或符合特定要件而允許未獲當事人同意而經蒐集、處理及利用之個人資料，仍具事後控制權，不因其曾表示同意或因符合強制蒐用要件，當事人即喪失請求刪除、停止利用或限制利用個人資料之權利。僅有個資法第 11 條第 2 項規範個人資料正確性有爭議時；第 3 項規範蒐集之特定目的消失或限期屆滿時；第 4 項規範違反個人資料規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。惟未涵蓋所有利用個人資料之情形，比如合法蒐集、處理或利用正確之個人資料，其特定目的尚未消失、限期尚未屆滿之情形，即不在其適用範圍，故尚難認全部蒐用個人資料之行為，均符合事後控制權之要求。就健保署將個人健保資料提供公務機關或學術研究機構原始蒐集目的外利用，當事人之停止利用權應仍受憲法第 22 條規定保障。但由相關法制整體觀察，卻未見立法者依所保護個人資訊隱私權與利用目的間法益輕重及手段之必要性，而為適當權衡及區分，一律未允許當事人得請求停止利用，而停止利用應遵循之相關程序亦無規定，亦即欠缺當事人得請求停止利用之相關規定，顯然於個人資訊隱私權之保護有所不足。故在事後控制權之部分明確認定當事人應受有憲法保障，惟具體相關細節規劃應待再研議。

因應數位時代來臨，網路搜尋引擎可永久保存個人資料相關紀錄之搜尋結果或連結，因此賦予當事人得以在控管者無正當理由保存相關資料之情形下，得請求移除或刪除已無運用目的必要之資訊，並被社會所遺忘之權利。然而被遺忘權並非絕對之權利，各國對於被遺忘權仍訂有相當規範。在被遺忘權之行使要件上，歐盟 GDPR 體系、英國明定應以運用個人資料之特定目的消失、欠缺法律依據或正當事由、非法運用等類型為主；美國 CCPA 則一般性承認當事人得行使被遺忘權，故未定有行使要件。另在例外情形仍得限制當事人行使被遺忘之權利。歐盟 GDPR 體系、英國及美國 CCPA 均明定被遺忘權之限制規定，其限制之例外事由以言論自由、公權力行使、科學研究之類型為主，避免當事人行使被遺忘權對公共利益產生過大影

響。

與他國相較，由於我國個資法所賦予當事人之刪除權，對於搜尋引擎、社群網站等控管者究屬我國個資法之蒐集、處理或利用者尚存疑義，得否逕依個資法規定向上開控管者請求刪除搜尋結果、連結等相關個人資料之紀錄，亦難予以肯定。雖我國近期實務已逐漸肯認被遺忘權，然回歸個資法之刪除權規定，在適用上仍存在諸多限制，並不似被遺忘權得請求刪除之範圍相同，又未課予控管者應負有通知其他控管者之義務，故難謂我國個資法之刪除權等同於被遺忘權之概念。考量在實施被遺忘權之問題上，因搜尋引擎、社群網站等控管者範圍廣泛，通知及刪除之方式、範圍亦不明確，故仍存在技術、成本上挑戰，亦應注意是否會導致私人審查言論及寒蟬效應之爭議。在政策上建議應透過修法明確保障當事人之被遺忘權利，惟在修法前建議透過發布指引的方式，從個資法賦予當事人之刪除權逐步給予民眾與業者如何行使與因應的指導。

（三） 權利限制規定

綜觀各國法制，可觀察到各國所賦予當事人權利類型上存有差異，然主要仍可區分為「近用權」、「更正權」及「刪除及停止蒐集、處理或利用權」三種類型。首先關於近用權行使之限制，以「公共安全或秩序維護」及「司法或訴訟程序」列為限制事由的國家包括歐盟、德國、英國、瑞士、美國、日本，我國則未將其納入。但公共安全、秩序維護、司法權之行使等，或可解釋為「公務機關執行法定職務」之一種。而針對特定資料或業務型態，如考試業務、新聞業務、健康資料、教育資料、兒童虐待資料、家戶裝置資料及非商業活動資料等，英國、美國、日本、韓國及新加坡有納入限制事由，我國個資法雖無此類規定，但可能規定於特別法如兒童及少年福利與權益保障法等。另外美國、新加坡等國考量資料之執行成本或避免權利濫用，規定可以基於重複申請或請求不合理等事由，限制當事人之近用，或對於近用權、訂有免費行使頻率之限制。因此，針對公共秩序維護、警察權行使、司法訴訟相關業務等，我國是否有必要明定為近用權之限制要

件，又針對特定資料類型如兒童虐待資料等或業務型態近用權之限制，是否均適合規定於個資法，建議得視國內相關法規完備之程度而定。至於近用權行使方式或頻率，考量相關行政成本得參考美國法之規定，若超過一定期間的次數得酌收手續費用，以免造成權利之濫用。

其次，關於更正權之部分，係以「維持個人資料正確性」為各國個人資料保護規範共通之原則，歐盟 GDPR 列出得由會員國立法之限制要件，而除英國、美國加州及新加坡外，日本僅以他法另有規定得限制，多數國家則普遍未限制更正權之行使。因此可見部分國家訂有更正權之限制要件。我國個資法對於個人資料更正權依第 11 條第 1 項有明文保障，但並未規定更正權行使之限制要件。考量更正權之行使將影響個人資料之正確性，當資料同時涉及數人之個人資料的情形，如評鑑制度等可能發生彼此認知的衝突，因此建議應限於達成利用該個人資料目的之必要範圍且屬事實錯誤之情形，始得更正之，避免無法確認資料之正確性。

其三，關於刪除及停止蒐集、處理或利用權行使之限制，其限制要件以歐盟對學術研究之特別規範，學術研究為停止蒐集處理利用之權利行使要件，但同時亦為刪除權行使的限制要件。而我國與歐盟對當事人權利保護衡平之差異，在於我國個資法規定僅有於當事人權利需要保護時，始得請求刪除或停止處理、利用個人資料。惟歐盟則係要求資料控管者須證明其利用相較於當事人權利更需要保護之情形。另外，德國、美國及日本將刪除難以執行、成本過鉅等因素納入刪除權行使之限制要件，但德國、日本要求須採取如停止利用等替代措施，美國則無採取替代措施之規定。因目前確實有部分科技之應用，如分散式帳本技術等將使記載之資料難以刪除，考量區塊鏈等應用越加興起，當資料無法刪除或成本過高之情形，應得提供替代措施作為當事人權利保障之手段，或建議可參考歐盟「暫時性限制」之規定，於釐清相關利益衡量前，暫時禁止控管者利用該資料，以暫時保障當事人權益作為緩衝作法。

綜上所述，關於權利行使限制規定之事由，可觀察到各國規範均有不同，惟可歸類為國家利益、公共安全或秩序維護、司法訴訟程序、法定職務或義務等，其應考量之重點在於與當事人權利保護之衡平。由於多數限制要件在法理上仍屬於不確定之法律概念，或在執行上存在技術、成本等相關障礙因素，目前國內各界尚未對當事人權利行使之限制要件規範具有明顯共識，建議宜觀察各國實際應用情境作為後續調整之參考。

參考資料

一、外文資料

1. 〈個人情報の保護に関する法律についてのガイドライン（通則編）〉，日本個人情報保護委員會，https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/#page_top。

2. 宮下紘，〈「忘れられる権利」について考える―平成 28 年 7 月 12 日東京高裁決定を受けて〉，《ロ―ジャ―ナル》，第 741 期 (2016)。

3. 上机美穂，〈検索エンジンの検索結果による逮捕歴公表と「忘れられる権利」〉，《新・判例解説 Watch》，第 20 期 (2017)。

4. 個人情報保護法 いわゆる 3 年ごと見直しに係る 検討の中間整理，個人情報保護委員会，平成 31 年 4 月 25 日，https://www.ppc.go.jp/files/pdf/press_betten1.pdf (2019)。

5. 総務省，携帯電話・PHS の番号ポータビリティの実施に関するガイドライン，令和 2 年 12 月 18 日最終改正，https://www.soumu.go.jp/main_content/000775806.pdf (2022)。

6. 総務省，情報信託機能の認定に係る指針 Ver2.1，情報信託機能の認定スキームの在り方に関する検討会，令和 3 年 8 月，https://www.soumu.go.jp/main_content/000764120.pdf (2022)。

7. 18th Congress House Bill NO. HB01188, republic of the philippines house of representitives, https://www.congress.gov.ph/legisdocs/basic_18/HB01188.pdf (2019).

8. ALAN CHARLES RAUL, THE PIVACY ,DATA PROTECTION AND CYBERSECURITY LAW REVIEW, 6th ed (2019).

9. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 05/2014 on Anonymisation Techniques, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (2014).

10. ARTICLE 29 DATA PROTECTION WORKING PARTY, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf (2014).

11. ARTICLE 29 DATA PROTECTION WORKING PARTY [WP29], Guidelines on consent under Regulation 2016/679, https://ec.europa.eu/newsroom/article29/items/623051 (2018)

12. Australian Competition and Consumer Commission [ACCC], Consumer Data Right accreditation guidelines (2022).

13. BMBF, Handreichung Datenschutz, Aufl. 2, https://www.forschungsdaten-bildung.de/files/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf (2020)

14. Bundesamt für Sicherheit in der Informationstechnik [BSI], Review of the midata voluntary programme, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/327845/bis-14-941-review-of-the-midata-voluntary-programme-revision-1.pdf (2014).

15. Bundesministerium des Innern [BMI], Neue Wege bei der Einwilligung im Datenschutz – technische, rechtliche und ökonomische Herausforderungen, S.4.13, https://pdffox.com/download/neue-wege-bei-der-einwilligung-im-datenschutz-pdf-free.html (2017).

16. Bundesamt für Sicherheit in der Informationstechnik [BSI], Mit Sicherheit: Verschlüsselung als Grundlage für eine sichere Digitalisierung, S. 62, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2018_02.pdf?__blob=publicationFile&v=1 (2018)

17. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit [BfDI], Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterung, S. 60-61, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf;jsessionid=CF855B1389AB879E987D57A3812BEF42.intranet241?__blob=publicationFile&v=9 (2020).

18. Case C(2020) 8599, Commission Implementing Decision (EU) 2020/2165 of 9 December 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D2165&rid=7 (2020).

19. Chris Achatz and Susan Hubbard, US vs. EU Guidelines for De-Identification, Anonymization, and Pseudonymization, JOURNAL OF INTERNET LAW, 20(11), (2017).

20. CJEU, Case C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

21. DEPARTMENT FOR BUSINESS INNOVATION & SKILLS, midata company briefing pack, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/34747/12-983-midata-company-briefing-pack.pdf (2012).

22. DEUTSCHE BANK, PSD 2, open banking and the value of personal data, https://www.dbresearch.com/PROD/RPS_EN-PROD/PROD0000000000471102/PSD_2%2C_open_banking_and_the_value_of_personal_data.pdf?undefined&realload=2pyvxUlrP29v~ns0a~dqPkVc0prVE/hRiuLLPpnfPruj4W6MNlPtoAzjc/bZpOMh (2018).

23. DPC, A Practical Guide to Controller-Processor Contracts, https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190624%20Practical%20Guide%20to%20Controller-Processor%20Contracts.pdf (2019).

24. EDPB, Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en (2018).

25. EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en (2018).

26. EDPB, Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679, https://edpb.europa.eu/our-

work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_en (2019).

27. EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_en (2019).

28. EDPB, Guidelines 3/2018 on the territorial scope of the GDPR, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en (2019).

29. EDPB, Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak, https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf (2020).

30. EDPB, Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1), https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-52019-criteria-right-be-forgotten-search-engines_en (2020).

31. EDPB, Guidelines 04/2021 on codes of conduct as tools for transfers, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-042021-codes-conduct-tools-transfers_en (2021).

32. EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en (2021)

33. EDPB, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en (2021).

34. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en (2021).

35. EDPB, Guidelines 10/2020 on restrictions under Article 23 GDPR, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en (2021).

36. EDPB, Guidelines 04/2022 on the calculation of administrative fines under the GDPR, https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-042022-calculation-administrative_en (2022).

37. EDPB, Overview on resources made available by Member States to the Data Protection Supervisory Authorities, https://edpb.europa.eu/system/files/2022-09/edpb_overviewresourcesmade_availablebymemberstatestosas2022_en.pdf (2022).

38. EDPS, A Preliminary Opinion on data protection and scientific research, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (2020).

39. Eleni Frantziou, Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos, HUMAN RIGHTS LAW REVIEW, 14, 761, 762 (2014).

40. EUR-LEX, COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (2021), https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (2021).

41. EUROPEAN COMMISSION [EC], JRC Conference and Workshop Report, Unfolding opportunities form the use of APIs in Europe, https://publications.jrc.ec.europa.eu/repository/handle/JRC124758 (2021).

42. EUROPEAN COMMISSION, Adequacy decisions, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (2021).

43. EUROPEAN COMMISSION, How the EU determines if a non-EU country has an adequate level of data protection, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en (2022).

44. EUROPEAN UNION AGENCY FOR CYBERSECURITY, Pseudonymisation techniques and best practices: Recommendations on shaping technology according to data protection and privacy

provisions, https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices (2019).

45. ICO, Anonymisation: managing data protection risk code of practice, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf (2012).

46. ICO, Contracts, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/contracts/

47. ICO, Principle (b): Purpose limitation, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/purpose-limitation/

48. ICO, What needs to be included in the contract?, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/what-needs-to-be-included-in-the-contract/#10

49. MOH, Singhealth's It System Target Of Cyberattack, https://www.moh.gov.sg/news-highlights/details/singhealth's-it-system-target-of-cyberattack (2018)

50. NERDWALLET, Credit Card Tokenization: What It Is, How It Works, https://www.nerdwallet.com/article/credit-cards/credit-card-tokenization-explained (2021).

51. NPC, PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2017-018, www.privacy.gov.ph/wp-

content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-018.pdf (2017).

52. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-001, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-001.pdf (2017).

53. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-23, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-023.pdf (2017).

54. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2017-31, www.privacy.gov.ph/wp-content/files/attachments/advopn/NPC_AdvisoryOpinionNo._2017-031.pdf (2017).

55. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2018-068, www.privacy.gov.ph/wp-content/files/attachments/advopn/2018/v1[Redacted]%20Advisory%20Opinion%20No.%202018-068.pdf (2018).

56. NPC, PRIVACY POLICY OFFICE ADVISORY OPINION NO. 2020-018, www.privacy.gov.ph/wp-content/uploads/2020/10/Redacted-Advisory-Opinion-No.-2020-018.pdf (2020).

57. NPC, NPC Circular No. 2020-03, www.privacy.gov.ph/wp-content/uploads/2021/01/Circular-Data-Sharing-Agreement-amending-16-02-21-Dec-2020-clean-copy-FINAL-LYA-and-JDN-signed-minor-edit.pdf (2020).

58. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2019-032, www.privacy.gov.ph/wp-content/files/attachments/advopn/2019/AdOps_2019-032.pdf (2019).

59. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2019-036, www.privacy.gov.ph/wp-content/files/attachments/advopn/2019/v1[Redacted]%20Advisory%20Opinion%20No.%202019-036.pdf (2019).

60. NPC, PRIVACY POLICY OFFICEADVISORY OPINION NO. 2021-023, https://www.privacy.gov.ph/wp-content/uploads/2021/07/Redacted-Advisory-Opinion-No.-2021-023.pdf (2021).

61. Office of the Australian Information Commissioner [OAIC], CDR Privacy Safeguard Guidelines (2021).

62. PDPC, Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/Advisory-Guidelines-for-NRIC-Numbers---310818.pdf?la=en (2018).

63. PDPC, Advisories on Collection of Personal Data for COVID-19 Contact Tracing and Use of SafeEntry, https://www.pdpc.gov.sg/help-and-resources/2021/05/advisory-on-collection-of-personal-data-for-covid-19-contact-tracing#advisory1 (2021).

64. PDPC, ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PDPA, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-

Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Oct-2021.pdf?la=en (2021).

65. PDPC, Advisory Guidelines on the Personal Data Protection Act for Selected Topic, Chapter 7 Data Activities Relating to Minors, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (2021).

66. PDPC, Advisory Guidelines on the Personal Data Protection Act for Selected Topics, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (2021).

67. PDPC, ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT FOR SELECTED TOPICS, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Selected-Topics/Advisory-Guidelines-on-the-PDPA-for-Selected-Topics-4-Oct-2021.pdf?la=en (2021).

68. PDPC, GUIDE TO BASIC DATA ANONYMISATION TECHNIQUES, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf (2018).

69. PDPC, Guide To Data Sharing, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Data-Sharing-revised-26-Feb-2018.pdf (2018).

70. PDPC, GUIDE TO MANAGING DATA INTERMEDIARIES, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Managing-Data-Intermediaries--2020.pdf?la=en (2020).

71. PDPC, GUIDANCE FOR USE OF ASEAN MODEL CONTRACTUAL CLAUSES FOR CROSS BORDER DATA FLOWS IN SINGAPORE, https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Practical-Guidance-Provided-by-PDPC/Singapore-Guidance-for-Use-of-ASEAN-MCCs---010921.pdf?la=en (2021).

72. PDPC, Laws Requiring Collection of NRIC Number by Organisations, https://www.pdpc.gov.sg/guidelines-and-consultation/2020/02/advisory-guidelines-on-the-personal-data-protection-act-for-nric-and-other-national-identification-numbers/nric-extracts (2019).

73. PDPC, PDPC Reminds Organisations on NRIC Advisory Guidelines Compliance Deadline, https://www.pdpc.gov.sg/news-and-events/press-room/2019/08/pdpc-reminds-organisations-on-nric-advisory-guidelines-compliance-deadline (2019).

74. Rat für Sozial- und Wirtschaftsdaten (RatSWD), Handreichung Datenschutz, Aufl. 2, Berlin, https://www.konsortswd.de/wp-content/uploads/RatSWD_Output8.6_HandreichungDatenschutz_2.pdf (2020).

75. Rossana Ducato, Data protection, scientific research, and the role of information, COMPUTER LAW & SECURITY REVIEW 37 (2020).

76. Taeger, Jügen und Gabel, Detlev, DSGVO BDSG Kommentar, §3 Verarbeitung personenbezogener Daten durth öffentliche Stellen, Aufl. 3 (2018).

77. Uniform Law Commission, Prefatory Note, DRAFT FOR APPROVAL UNIFORM PERSONAL DATA PROTECTION ACT, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=6f7e81fb-9c3e-8f4b-1907-d59fb4fa61ec&forceDialog=0 (2021).

78. Uniform Law Commission, Section 4 Controller and Processor Responsibilities; General Provisions Comment, DRAFT FOR APPROVAL UNIFORM PERSONAL DATA PROTECTION ACT, https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=6f7e81fb-9c3e-8f4b-1907-d59fb4fa61ec&forceDialog=0P13 (2021).

二、中文資料

1. 立法院第 2 屆第 1 會期第 4 次會議議案關係文書（1993）。

2. 立法院公報，第 83 卷第 45 期（1994）。

3. 立法院公報，第 97 卷第 48 期（2008）。

4. 立法院公報，第 102 卷第 4 期（2012）。

附件一、諮詢會議之會議記錄

「個人資料保護法相關議題」第1場產學專家學者諮詢會議會議紀錄

壹、 時間：110 年 10 月 6 日（星期三）上午 9 時 30 分

貳、 地點：本會寶慶辦公區 610 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、 太穎國際法律事務所謝律師穎青

（一） 建議增加我國個資法施行以來所遭遇之問題處理，並反省以作為未來修法參考。借鏡澳洲有關個人資料保護法的立法與實踐，其司法判決明確指出應留意與英國、歐盟與加拿大等國家之個資保護相關法制，使澳洲經濟、社會及生活與上列先進國家結合成一個共同利益區塊。而我國個資法之未來修法走向，究竟是要採取歐盟 GDPR 體系或向美國靠攏配合 APEC 的 CBPR 體系，是先決條件必須做好價值判斷。自 2016 年 APEC 特別組成工作小組討論資料隱私(data privacy)，至今尚無具拘束力的共識。

（二） 議題一，依據我國個資法第 1 條立法目的，係為避免人格權受侵害，並促進個資的合理利用。依據司法院釋字第 603 號解釋，人格權包含個人隱私，惟現行個資法卻無明文規定包含個人資料自主權。根據最高法院刑事大法庭 109 年度台上大字第 1869 號裁定，認為個資法第 41 條罰則之規定，有關「意圖為

自己或第三人不法之利益」，應限於財產上之利益；至所稱「損害他人之利益」，則不限於財產上之利益。因此，針對個資法指涉之「公共利益」，究包含個人法益或國家法益，建議未來修法時應做概念上的釐清。

（三） 公共利益應與被遺忘權一併討論，但是，不論係個資自主權或被遺忘權，目前我國個資法並無明文規定。例如臺灣高等法院106 年上字第 1160 號民事判決，法院最終因原告屬於公眾人物，而新聞媒體的報導具有公共利益，故以公共利益直接駁回當事人的請求。我國個資法第 3 條已明訂當事人之請求權利，但國內目前缺乏個資法的專責獨立機關，制度設計的結果容易導致並無太多的案件在法院處理，難以瞭解司法實務確定見解。

（四） 議題二，分享曾經參加 APEC 會議的經驗，日本修訂個資法將「難以取得同意」列入法律規範，主要係當時發生電車的重大事故，家屬詢問醫院相關訊息，但醫院卻不願意回答，因為沒有得到當事人同意。然而，同樣案例發生在我國時，是否有同樣問題及修訂之必要，應進一步衡量及研究。

（五） 議題三，關於「有利於當事人權益」或「對於當事人權益無侵害」的討論，主要係到底什麼是當事人權益的問題，是否限於隱私或一般人格權？是否包含財產權？相關法律概念的闡明有其必要性，否則對於實務適用時會產生困擾，例如：我國個資法第 21 條第 3 款解釋上的困擾，目前只有國家通訊傳播委員會於 2012 年時，曾發布法規命令明白禁止傳輸個資到中國大陸地區，其他行政機關並無相關規範。這對於國內外企業在布局國際市場時，究應以什麼標準來衡量國際傳輸，無所適從。

（六） 議題四則是對個資法長期的誤解，以律師公開資料為例，律師

將自己的營業地址、姓名、事務所名稱或其他聯絡資料公布至公會通訊錄，其用意係讓多數人知道業務聯繫方式。建議這部分不需修法處理，而係透過公會的自律方式，要求公會不要對外公開與營業無關之資訊，例如住家資料、年齡、出生年月日等。從比較法的觀點而言，瑞士及奧地利基於其社會長期維護個人隱私價值的通念，立法不允許以電話行銷侵擾個資當事人。若未來修法能將國內生活實例導入修法過程，亦有助於釐清個資與隱私的保護層次。

二、 國立陽明交通大學科技法律學院陳教授銘雄

（一） 本次會議討論的四個議題，整體而言可簡化為一個議題：受規範的公務和非公務機關本身內部的「利益衡量」自律能力的大小。自律能力高，制度上就能朝向開放廣泛的蒐集處理利用範圍，而透過原則性的利益衡量來約束。反之，若機構自律能力低，就要透過具體類型化的制度設計，以避免濫用。

（二） 利益衡量雖然概念上容易理解，但在操作層面上並不容易，例如新聞自由與個人隱私之界限不容易拿捏。在被遺忘權的討論中，有一種論點認為由 google 自己判斷對於個資當事人的報導是否應該被遺忘，是否會影響網路上的言論自由及民眾知的權利。現實面是：規模愈大的機構，愈可能成立內部單位安排人力來作審查，包括聘請隱私個資專家參與；規模小的機構，就不太有人力來作這樣的審查。

（三） 制度設計的原理應提供誘因，使機構願意為了較方便的個資蒐集利用方式，而投入法遵成本提高個資保護水準。如果直接和間接識別，兩者權利義務相同，機構就缺乏動機對資料加密，而傾向於以直接識別的方式儲存個資。因此，如果我們對於機構資安保護程度的不同，自律程度的不同，而給予寬嚴不同層

次的蒐集處理利用範圍，而不是不分任何產業，不分任何種類個資，一律給予相同的「權益衡量」之抽象原則或「類型化的具體規則」，會有助於讓機構有動機投入更多法遵成本，以換取較彈性的操作空間。

（四） 本次會議蒐集了許多國家的制度，但比較法應作體系比較，注意配套措施的設計，而非只注意個別條文。以 GDPR 為例，雖然以「正當利益+利益衡量」為主，但卻是在一些配套措施下進行。例如，GDPR 要求若有大規模的蒐集個資，需進行資料隱私衝擊評估（Data Privacy Impact Assessment），且符合一定情形時，要諮詢個資專責機關，且個資專責機關也會頒布一些指引（guideline），對於如何作權益衡量有更細緻的規定。

（五） 由於個資法的違反會有嚴重的民事賠償、行政裁罰甚至刑事處罰，所以規則的明確性非常重要。因此，若法條明訂廣泛的抽象要件以及權益衡量，實際上還是需要訂出具體明確的判斷標準，使公務及非公務機關不致於為了避免違法而不敢行動。但有些中央部會，並未投入足夠人力去設計各領域個資保護的具體規範，是我國個資利用面臨障礙的主因。解決辦法之一，是透過「監理沙盒」的方式，鼓勵中央部會投入人力資源，研發出該領域的個資保護具體規定。由於各產業特性的差異，統一交給個資專責機關去訂定各產業的個資保護，未必達到最適效果。可參考美國的部門式個資保護架構，考量每個產業的數位化及創新速度不一，所以針對各產業制定創新規定，可因應產業的需求來調整。重點是要透過制度設計，鼓勵各中央部會，不要把問題都只交由一個專責單位或機關處理，而是各部會需要瞭解個資保護，例如設置個資保護官或組成一個以個資專家為主的功能性委員會，以發展屬於該產業的具體規定，俾利明確化個資蒐集處理利用的構成要件，提高各機構在法律遵循上

的標準明確性。

三、 中央研究院歐美研究所何副研究員之行

（一） 首先，主要的問題為「公共利益」屬概括條款，若必要性的判斷不夠清楚，會產生適用上的困擾。歐盟基於公共利益目的，將涉及特種個資的健康資料（health data）劃分四個層級：1.重大（substantial）公共利益，當涉及時間緊迫性時，公共利益會拉到非常高的層級，但相對則是限縮同意權，例如可以不需要當事人同意或是限制退出權、2.重要（important）公共利益，當不涉及時間或空間急迫性時，如涉及公共健康（public health）或健保資料庫，此時公共利益就往後限縮，同意權模式就會修正，並給予當事人退出的可能性、3.一般（general）公共利益，例如涉及公共利益的學術研究，但應細膩區別該研究是否對公共利益有重大影響，或僅係研究者的好奇回應，不同公共利益的層級劃分，將影響到必要性衡量的判斷及當事人同意模式的配套機制、4.無特別的公共利益。

（二） 針對議題二以 GDPR 處理原則來看，蒐集資料時須符合目的特定、資料最小化及透明性原則，並且對資料控管者（data controller）做合理的限縮規範。此時，若為避免國家成為最大的資料控管者，而將資料控管者區分公務機關或非公務機關，將「難以取得同意」納入判斷對當事人有無侵害、有利於當事人權益是有必要的。但相關討論應建立在無法取得當事人的同意條件下，而相關適法性基礎的判斷應由獨立個資保護監管機關決定之。

（三） 有關議題三、四，觀察歐盟 GDPR 規定係強調資料二次利用時，須與原來蒐集目的做相容性判斷，檢視二次利用與原始利用目的二者是否相容，相容性判斷性質類似利益衡量。但放在

公開領域之資料是不是能夠進行二次利用，需要檢視其原來蒐集目的為何，意即判斷二次利用與原始蒐集目的間之相容性，以限縮公領域的所有資料皆可無限制地二次利用。

（四） 歐盟在二次利用除了相容性判斷，還包含檢視是否有適當的安全維護措施、主觀上當事人有沒有合理期待等配套機制。如果在公開領域的資料去做相容性判斷，認為當事人沒這樣的期待，例如報告人提到放榜例子，當事人並沒有期待他的資料被拿去做二次利用的時候，即不得因取自公開來源作為合法性基礎。

四、 中央研究院法律學研究所吳副研究員全峰

（一） 本次會議議題主要涉及能否將「公共利益」或「正當利益」作為構成正當性的基礎？但目前我國個資法下的公共利益，內涵並不清楚。因而使得公共利益本來在限制個人資訊自主權的概念之上，作為利益衡量的概念，但定義不明使得公共利益變成形式上的衡量。

（二） 此外，我國個資法將學術研究機構納入規範，造成同一個研究目的或同一個使用目的，由於商業或學術角度不同而影響公共利益的解釋。公共利益不僅是類型化的問題而已，其本身也牽涉到很多不同的情境（scenario）。法務部函釋也敘明公共利益難以類型化區分或明確定義，需要個案判斷。但其基本要件應在法律上提供例示或說明，至少立法理由須明確說明公共利益能夠限制個人資訊自主權的範圍為何。

（三） 另外，是否公共利益類型化與利益衡量為互斥條件，是否當正當利益的要件滿足後，就不需要做利益衡量？以澳洲為例，澳洲對公共利益的正當性判斷，為個案審議加上類型化。而英國係個案審議加上法律明文為主。因此，公共利益類型化後，未

必無須進行利益衡量，二者並非互斥概念。尤其，在公共利益或正當利益判斷上，需要依據不同情境彈性調整時，利益衡量就必須要出現。因此，我認為定義衡量的條款相對於判斷公共利益或正當利益，更具有重要性。

（四） 議題三，我認為應將「對當事人權益無侵害」與「有利當事人權益」區隔。有利當事人屬於積極概念，係避免積極的侵害出現，某種程度會預設當事人同意，並合理期待限制其資訊自主權，以保障其利益；另外一個討論係對於這個利益，國家有義務去保障其利益。因此，當事人侵害的內容或概念，必須非常明確且嚴重，始得例外限縮當事人的自主權。而對當事人無侵害屬於消極概念，惟難以解釋沒有侵害的概念為何，尤其國外在沒有侵害的概念上非常嚴格，係指任何的權利或是任何可能的利益都不能夠產生侵害，始構成對當事人不侵害。但是，我國對於當事人無侵害的概念很廣，有關概念性解釋、相關程序或配套機制應如何訂定，將影響當事人之保護程度。

（五） 有關於正當利益的問題，討論上與前述問題類似，應釐清利益衡量之正當程序為何、正當利益之要件為何，若公務機關已經可以藉由法律規定去處理正當利益，相關必要性的判斷必須更細緻與嚴謹，而非單純簡單形式上滿足正當利益即可允許限縮限制。

（六） 議題四，公開資料理論上也應該要謹慎處理，對於當事人解釋上係指其可預見的運用情境，但超過這個合理預見的範圍之後，理論上不屬於當事人不反對的討論範圍。

（七） 最後，討論歐盟 GDPR 有其重要性，因為 GDPR 具有很強的域外效力，國際上包括美國也針對 GDPR 做出相關討論。目前我國無法排除 GDPR 相關規定，且其規定相當嚴格，故未來修

法應有相應之調整規範。

五、 理律法律事務所曾律師更瑩

（一） 議題一 GDPR 並未強調特定目的內、外之概念，現行法之區分方式並無實益，徒增困擾，建議可思考調整。公共利益通常與生技或醫藥有關，但適用個資法第 6 條相對嚴格，故執業上較少建議客戶適用此要件。比較常見的係個資法第 20 條的討論，當檢調或刑事訴訟機關向業者要求提供當事人個資時，得基於增進公共利益之需要，而提供當事人個資給檢調機關。以業者的角度，明確規定公共利益之類型，將有助於業者判斷。

（二） 在議題二討論上，個資法第 19 條及第 20 條規定，已經將蒐集、處理及利用區分特定目的範圍內與特定目的範圍外，但若路邊有人昏倒，是否能取其口袋的健保卡交給醫院？尤其不具備特定目的時，個資法第 19 條需要有相應規範處理之。但建議不要增加太多條件，否則實務上將難以判斷。

（三） 議題三，依據 GDPR 第 6 條之規定，正當利益屬於利益的權衡，性質上不會是有利於當事人權利或無侵害，因為本質上就是認定對其為不利才需要正當利益作為合法基礎；如果有利當事人權利或對當事人無侵害，則根本就不用比較。例如車禍發生時能否蒐集對方車牌號碼？蒐集當事人個資係行使訴訟權利並具有正當利益，但對方的利益將受到損害。

（四） 議題四，分享實務經驗與產業想法，目前客戶主要關心未來如何行銷的問題，若只能在蒐集特定目的範圍內利用，將會很難行銷。現行個資法關於公開資訊與一般來源之規定有存在的必要，特別是國內業者購買龐大資料庫，若未來公開資料都不能運用的話，這將對於產業在行銷上造成困難。

六、 國立政治大學法律學院劉教授定基

（一） 進入議題討論前，有二個大方向問題可先提出討論：我贊同謝律師提到修法要有方向與目標的問題，尤其歐盟與 APEC 體系在個資保護的程度上具有差異，但是否完全無法調和可請研究團隊做細部分析。另外，觀察近期美國各州之法律，美國似以保護個資為趨勢，雖然不到歐盟這麼嚴格，但從業者角度而言，符合兩套法遵的成本有一定難度。

（二） 另一個大方向是，修法前應一併考慮三個問題：第一，是否還須區分蒐集、處理及利用的合法要件？尤其某一個合法要件只有放在蒐集、處理或是放在利用，沒放在另外一邊。特別是在 AI 的時代要清楚切分蒐集、處理、利用可能有困難，而歐盟就以 processing 涵蓋之。第二，是否需區分特定目的內外的利用？歐盟相容性判斷操作上頗為複雜，且部分是抽象概念(例如：當事人期待)，判斷上可能更不清楚。第三，是否仍區分公務與非公務機關？若相關前提能夠確立，將有助於後續議題的討論。

（三） 議題一有關公共利益，我認為國內實務針對公共利益條文確實有解釋上的困難建議若參考其他國家以法律規定的情形為限，立法體例上比較像歐盟的模式，但這可能會影響公共利益規定運用之彈性，要一併思考。此外，目前有關公共利益的必要性要求以及利益權衡的討論，主要依據個資法第 5 條，實務操作上容易遺漏。建議強調公共利益的必要性與利益權衡，或是參照 GDPR 第 5 條規定，直接於總則以條文敘明或臚列重要的個資保護原則，一體適用全部的蒐集、處理或利用要件。

（四） 議題二，個資法立法目的雖僅提及人格權，但從司法院釋字第 603 號解釋的脈絡，憲法第 22 條人格權指涉的資訊隱私，此概念又包含私密領域保護與個人資料自主控制二個概念。在這

前提下探討議題二會更容易理解，納入當事人難以取得同意的要件能彰顯資料自主控制權利的意涵。

（五） 議題三正當利益條款，歐盟在適用上限於非公務機關，因此應限制適用於非公務機關。觀察國外相關討論與實務的案例，正當利益的條款需搭配利益權衡，由於正當利益範圍很廣，故利益權衡屬於平衡個資保護與合理利用的重要機制。而我國個資法並無相關規定，因此長期造成適用上的困擾，例如無合法事由則容易傾向將此資料解釋為不是個資。

（六） 議題四，目前對一般可得來源或合法公開資料的條款，實務上確實存在誤用情況。就歐盟條文解釋而言，在網路上蒐集的資料並非任意使用，仍須視其公開情境為何。若未考慮公開的原始目的，容易誤會合法公開後也無須進行利益權衡，可任意使用。因此，假設議題三被採納，則議題四可檢視什麼情境無法納入正當利益權衡條款內（例如：特種個資的蒐集、處理或利用若無正當利益權衡條款的適用）；如果可以被正當利益條款吸納，則一般可得來源及合法公開資料的條款可以考慮刪除。

七、 開放文化基金會林法制顧問誠夏

（一）開放文化基金會協助政府機關針對開放資料的處理與應用，發現過程中常常產生理解上的灰色地帶與或認知上的衝突。尤其，我國個資法以公務機關與非公務機關為二分法，因國內缺乏個資保護機關而容易造成雙重標準，例如公務機關認為可利用個資時，則以符合公共利益為合法事由；相反地，公務機關不認為可利用個資時，則以保護個人利益拒絕之，造成民眾無所適從。

（二）國發會希望取得 GDPR 的適足性認定，GDPR 條文多討論專責機關之行政查察功用，若未來無專責機關或取代機制，將難以

取得適足性認定。若存在個資保護的專責機關，則劃分公務機關或非公務機關較為合理性，例如「資通安全管理法」將資通安全管理分成國家設施與重要基礎建設，在非公務機關的情形，資安主管機關須承擔資訊安全保護的責任。因此，專責機關能夠確保公務機關與非公務機關，二者的行政管理配套的一致性。

（三）議題一，若公共利益類型化為趨勢，未來個資法修訂原則上是沒有問題，但公共利益類型並非屬於直接阻卻違法事由。觀察美國跟歐盟開放資料的專法，其亦將公共利益列為評估基礎與審查條件，但並不是符合此條件後，個資從此以後就可以使用，其立法方式比較像是著作權法的特例使用，特例使用須符合著作權法第 65 條的權衡規定，而著作權法第 44 條至第 64 條存在合理使用的型態舉例；因此，當存在合理使用後，仍須以著作權法第 65 條權衡規定予以評估。我認為能夠加入類型化進行調整，但是不要把公益類型化直接當成阻卻違法事由。

（四）議題二，同意對於目的外利用時，可仿效日、韓規定限於難以取得同意的情況下，才能蒐集當事人個資。若取得當事人個資無法取得其同意時，則必須限於時效上不及或難以同意的情形，才允許未經同意取得資料來利用。若無明文要求限於難以取得同意才能利用當事人個資的話，則無疑架空個資法的立法目的。

（五）議題三，目前承認取自公開資料或一般可得來源為合法事由的國家非常少，而議題三及四是連動的，是否需訂正當利益，確定對當事人無侵害才可以使用，跟是不是已經公開資料或一般取得來源都可以使用，應可一併討論。分享一個德國案例，一位知名導演認為維基百科登載其出生年月侵害其個資，因此提告，而維基百科辯駁此個資為原告自己公開的資料，原告公開販售的圖書已公開相關資訊。最後，德國的法院判決認為，並非當事人自行公開的資料，就不受到個資法的保護，其基本邏

輯的核心仍須檢視有無侵害當事人的利益，並判決原告敗訴，理由在於原告出生年月日已眾所皆知，而無待維基百科公布，他人也知悉，且經事實調查亦無影響當事人利益。從上述案例，即使現行條文是引據當時德國法規定，但德國實務上在審判時，也並非直接引用公開資料或一般可得來源即得任意利用，仍須進行個案評估。

八、 中華民國無店面零售商業同業公會塗副秘書長家興

（一） 從電商角度來分享，個資法指涉的公共利益為何，會影響執行端之理解何者合法及何者違法的問題，但公共利益過於寬泛又導致權力擴張，但過於狹小又可能無法處理。就電商業者而言，並沒有要蒐集民眾個資，早期蒐集個資主要是想瞭解消費者，但科技發展至今業者只需蒐集當事人的行為即可，並以帳號作為連動而無須輸入與個人有關的資料。

（二） 在電商平台之中，電商業者與賣家屬於合作關係，彼此間存在明確蒐集資料的規範，尤其跟物流業者合作，因貨物會寄送到消費者手上，故相關明確的個資蒐集須予以保護。但在 C2C 的拍賣平台之中，並無針對賣家蒐集資料，性質類似開放市集平台提供銷售管道，因此認證內容包含手機、電子郵件或銀行帳戶的正確性，但業者無法連結至特定個人。

（三） 以國內電商業者的結構，中小企業佔整體的 97.65%，其中微型企業（5 人以下）佔 67.5%；因此，修法調整若能有效地讓業者便於理解，且實務上易於操作，並有明確的規範與執行內容，對於國內電商業者非常重要。

九、 達文西個資暨高科技法律事務所王律師慕民

（一） 針對議題一及二的討論，考量修法的過程繁複及版本更動，在

修法幅度最小的立場，如何調整法令應取決於操作或應用上涉及的重大爭議或困難。有關公共利益操作上或免除當事人生命身體自由財產危害，如實務操作上無重大爭議或困難，修法順序建議可以不用優先討論。

（二） 針對議題三，就實務經驗來看，較少主張對當事人無侵害或有利當事人權益，該條款並非以資料控管者的利益作為考量，可能係以當事人的權利有沒有被侵害的考量或有利於當事人權利作為考量，有法遵意識的業者較不會主張該條款。若討論公務機關何時主張對當事人有侵害或無侵害，則實務操作可能有一些法律條文會被架空。因此，我認為與其以當事人權益有無侵害作為機關蒐集、處理個資的法律依據，不如考量以「機關的正當利益」取代，而把對當事人權益的利弊納入機關評估正當利益優勢性的判斷要素。

（三） 議題四，若能接受將控管者的正當利益作為蒐集、處理及利用的合法事由的話，則有關當事人自行公開或合法公開或資料取自於一般可得來源，可能無須列為蒐集、處理或利用個資的合法事由，而是做為權衡機關正當利益的判斷要素，因此議題三與四需搭配討論。而有關自行公開或合法公開，該如何劃定特定目的的範圍仍有討論的必要。另外，分享今年 8 月份的法院判決，當事人的護照資料被媒體透過翻攝的方式呈現於新聞，法院審理的依據即依據一般可得來源；然而，適用上應考慮同款但書規定，當事人對資料之禁止處理或利用有更值得保護的利益，不在此限。因此，若未來修法仍保留本款的話，應確認但書應該如何行使的問題。

柒、 會議結論：

一、 有關專家學者提出修法架構性的建議，後續將調整討論題綱，

考量是否須區分目的內及目的外、歐盟相容性判斷，以及是否須區分公務機關與非公務機關等問題，並在後續相關討論內容將重要訴訟案件納入討論。

二、 未來修法主要是與國際趨勢接軌，以便業者布局國際市場，惟國際化亦應考量同步解決國內業者遇到的問題。

三、 感謝各位學者專家提供的寶貴意見，所有的意見將會納入個資法修法的參考。

捌、 散會（上午 12 時 10 分）。

「個人資料保護法相關議題」第2場產學專家學者諮詢會議會議紀錄

壹、 時間：110 年 11 月 3 日（星期三）下午 2 時 30 分

貳、 地點：本會寶慶辦公區 610 會議室

參、 主席：高副主任委員仙桂(楊參事淑玲代理）

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、太穎國際法律事務所謝律師穎青

（一） 建議修法要與世界人權保護接軌，同時反省我國隱私保護的意識，例如歐盟立法例特別將集會結社自由、不表意自由納入保障；以及考量法律所保障的隱私，目的在落實反歧視。

（二） 案由一贊同特種個資的定義跟範圍擴張包括種族、血緣、宗教、政治傾向，且擴充健檢資料不限於醫事機構進行者亦有其必要，但不建議採行例示規定，而是透過立法過程中廣徵民意，將本次修法當作嚴肅的公民檢討、反省的機會，爰建議未來採取具體列舉之立法方式。

（三） 案由二以代理外商在臺投資申辦電信服務為例，電信公司似有濫用通傳會要求其負擔義務之範圍，而要求公司負責人提出過多個資，如完整揭露公司負責人之護照、本國住居地址、甚至同住人數等資訊，但申請書並無相關要求，電信公司雖表示是依據通傳會的規定，但通傳會僅要求提供雙證件，電信公司似乎是要求提供了不必要的個資。

（四） 案由三建議應考量兒童權利保障問題，常見 18 歲以下未成年

人之照片、生活足跡等，被親人放上網路，甚有被盜用照片作為癌末病童服特效藥治癒廣告的案例，這些個人資料雖然是經合法公開，但可能對於無自主決定權之未成年人保障不足，也涉及兒童及少年福利與權益保障法第 69 條的規定。

（五） 案由四不建議納入公共利益，理由是我國尚無個資專責機關，且公共利益難有大眾普遍認同的定義，倘真正涉及公共利益，多數已規範於法律中，透過「法律明文規定」一項要件應已可處理。建議應先檢討現行法中對個資保護不足的部分，例如金融消費者保護法第 10 條對於金融消費者不提供個資與取得金融服務之關聯，是否會對金融消費者保護不足。

（六） 有關書面同意之困難點在於電子簽章法第 4 條第 3 項，授權行政機關得公告排除使用電子文件，因個資法並無主管機關，導致實務上幾乎皆以紙本方式取得書面同意，未能援用電子簽章法之便利性。癥結在於雖有電子簽章法，但行政機關擴大排除電子簽章法之適用，使實務運作面臨困難。

二、達文西個資暨高科技法律事務所葉律師奇鑫

（一） 開會通知單之議程案由二(第 4 頁)所引述歐盟 GDPR 第 6 條第 3 項第 b 款規定翻譯有誤，正確應為「若援引執行法定職務、履行法定義務作為運用個資之合法要件，該法律內容『可能』(may)包括…」，會議簡報第 15 頁已為正確修正。

（二） 案由一有關特種個資定義範圍應參考各國文化、價值觀，健康檢查是否一定限於醫事人員所為，亦可參考 GDPR 適當放寬，犯罪資料也建議擴張到刑事案件程序。但目前因法院組織法有關判決應公開之規定，已等同將犯罪前科資料公開，若能擴大到保護刑事案件之相關程序，對個資保護應有相當助益。生物特徵部分，贊同比照 GDPR 納入特種個資，因為

隨著 AI 發展各種新識別方式，生物特徵可作為追蹤個人之強大科技工具，列入特種個資可提升對個資的保護。

（三） 當事人書面同意部分，例如健康雲等產業，倘蒐集特種個資必須以紙本為之，會使消費者產生寄送紙本前之決策空窗期，提升猶豫、不參加之可能性，對相關健康產業會造成衝擊。但倘可藉由電子簽章法之輔助，以符合現行特種個資經當事人書面同意要件，應可降低衝擊。

（四） 有關當事人自行公開或其他已合法公開資料部分，如近期的 Deepfake 案例，因現行法處罰過輕，僅可能構成妨害名譽、加重散布猥褻物品等罪，法務部於日前討論修法方向時，亦有部分人士建議以個資法處罰，但個人並不建議。此問題在於國家領袖的面容因召開記者會、公共場合被蒐集等因素被合法公開，個資法對於蒐集作為其他用途的界限為何並不明確，因此贊同對此有所調整。

（五） 公共利益部分贊同納入合法要件，尤其是重大公共利益，但其內涵須更具體並嚴格限縮，如疫苗通行證是否可行等問題，為讓指揮中心得以快速反應，應需要類似公共利益之條款授權，以因應各種緊急狀況，使指揮中心得以推動重大公共政策，但也需有相關配套規定。

（六） 有關書面同意部分，特種個資應可使用電子簽章法的電子簽章，無須採用憑證或 CA。謝律師提到行政機關公告排除電子文件之適用可能會是潛在威脅，但目前相關機關似未排除適用或就相關程序另為規定。此部分建議可由國發會或電子簽章法之主管機關做相關函釋。

三、臺北醫學大學醫療暨生物科技法研所李教授崇僖

（一） 歐盟與美國對於個資保護之基本概念不同，歐盟較為嚴格，但執行面亦產生相關問題，再透過個資專責機關判斷處理；美國則是於發生不同案件時再個別處理。倘若我國要擴張個資法功能，將來專責機關就必須有足夠能力因應。

（二） 應先行區分是資料不當利用衍生的隱私侵害，或是個資保護的問題。應避免將所有問題放在個資法處理，亦不宜因科技發展而將資料作不同之使用就調整特種個資範圍。因此，針對整體個資法框架部分，建議不需要區分一般或特種個資。特種個資係因屬敏感資料而予以特別保護，並提高利用難度，惟健康個資之利用對公共衛生、精準健康而言具有高度公共利益價值，關鍵是如何管理其使用。又倘若將健康檢查資料放寬到健康相關資料，則該特種資料範圍將無限擴大。另，以當事人同意之合法要件而言，特種或一般個資之差別僅在於「書面」，倘若可透過電子簽章為之，則實際上其他合法要件並無太大差異。

（三） 關於當事人公開資料部分，會議簡報第 18 頁所述「承認國家較少」，請確認是否僅是未明文將此事由列入合法要件。若將已公開之資料的不當利用以個資法處理，即類似歐盟體制，將個資法當作數位時代基當事人權基礎。例如 Deepfake，不一定是個資法問題，而應從刑法上討論。

（四） 贊同納入公共利益條款，因為僅使用當事人同意作為合法要件對於資料流通或利用並不足夠，但公共利益類型化較為困難，未來應由專責機關作 guidance。以醫學研究而言，獲得當事人同意可取得較完整之資料，以串接其他品質較佳之資料進行研究，但缺點是資料量較少。醫院病歷資料庫或健保資料，多數並非透過當事人同意取得，雖資料量大，但品質較差、較難串接，資料利用上具侷限性。1980 年代 OECD 提

出個資保護指引形成當代的個資法，但其背景因素已歷經 40 年變化，導致現行法令與科技條件有所落差，目前對於資料利用與侵害，除涉及個資保護外，尚涉及肖像權、人格權等，應考量如何進行整體個資之保護，此部分由專責機關把關可能較為可行。

四、 私立醫療院所協會醫院資訊暨智慧醫療發展促進會孫會長培然

（一） 醫療院所面臨醫療 AI 研究之阻礙，建議應定義特種個資所囊括之範圍及用途為何？倘為公共利益或醫學研究，應從寬解釋。

（二） 案由一建議參考日本之例示方式，承認其他對當事人產生不當的差別待遇、偏見或其他不利益者亦可屬特種個資，並以類型化方式呈現，若採用列舉方式，一旦有所改變則須修法。另外，亦應鼓勵正當之利用以促進醫學進步。

（三） 醫院做臨床研究時會請病人簽署同意書，並由倫理委員會(IRB)認證，但倘若要求去連結化，則無法進行後續追蹤，建議可在個資法予以鬆綁，為公共利益之目的允許利用特種個資。倘若做不正當的利用，則無論是否公開或經同意，則可以主張侵犯個人隱私或違反個資法。若健康相關資料納入病歷醫療資料，將導致健康產業無資料可蒐集，精準醫療或國民健康將更難執行，阻礙科技發展。

（四） 至於書面同意部分，民國 98 年起實施電子病歷相關法規後，醫事人員雖可以數位憑證(CA)簽章、認證，但一般民眾並無 CA 認證，因此，為取得民眾簽署之同意書，目前大部分醫院實行辦法是採用一邊簽名一邊錄影存證的電子簽名方式，倘若日後數位國民身分證有 CA 認證就可以比照數位憑證(CA)

簽章。

五、中央研究院法律學研究所吳副研究員全峰

（一） 特別保障特種個資的原因是該資料被誤用之影響重大，例如歐盟將宗教、政治傾向等列為需要特別保護之特種個資，便可能是因與言論自由保障有關;但即令對特種個資特別保護，法規範上對於特種個資亦未完全禁止利用。

（二） 而健康資料屬特種個資也是在這個脈絡下發展出來，因其與人性尊嚴有緊密之關聯性。而就行動裝置上取得的健康資料而言，其實產業界關心的重點並不在於該資料是否為特種個資，而是政府對廠商蒐集、處理這些資料之程序是否清楚明確；依目前法律規範下，可透過當事人同意取得個資，且倘若產品要在歐盟販售，廠商亦會傾向符合 GDPR 規範。因此，對產業而言，這個議題的重點不在個資類型，而在是否方便取得「書面」同意之問題。如同葉律師所述，書面同意若可透過電子方式為之，且明確化相關使用方式或要件，產業利用特種個資上並不存在問題。

（三） 日本法之例示規定，其實是將歐盟 GDPR 之概念導入，界定特種個資之內涵實應考量其特別保護的根本價值，同一份資料不會因是否係由醫師使用而產生保護程度之差異，而應以資料本身內容決定。倘若以特種個資須特別保護之本質觀之，其範圍或界定必須細緻討論與區隔。因此，較不贊成單純只以例示方式規定，以日本、韓國為例，雖於母法為例示規定，但於施行細則為進一步具體規定，而非使主管機關個別決定。

（四） 案由三有關當事人自行或其他已合法公開資料，倘用於與當初公開範圍以外之用途，則應評估此種目的外利用是否符合原本公開資料時之預期，對於當事人權益會較具保障

（五） 案由四公共利益應有類型化之必要，否則將賦予主管機關過多裁量空間，現行依據法務部之函釋對公共利益尚無法做一致性之判斷，其實造成實務上之困擾；此外，不能否認公共利益之判斷有其複雜性而不一定能有列舉式之規定，仍須留有判斷空間，故建議應納入正當程序(due process)，亦即如何透過正當程序作成個資使用是否符合公共利益的判斷，以英國為例，主管機關便應就個資使用所涉及之公共利益以及其重要性、必要性等進行說明。

（六） 有關簡報第 22 頁，美國規定符合當事人期望，是否即表示無須符合「難以取得當事人同意」要件，建議再行確認。另，醫療資料在人體研究法或是人體生物資料庫管理條例亦有關於同意或去連結等相關規範，並非鬆綁個人資料保護法之同意要件，其他相關法規即隨之鬆綁，必須釐清。

六、中央研究院歐美研究所何副研究員之行

（一） 擴張特種個資的定義範圍，不必然對產業之利用造成困難，主因是敏感性資料之蒐集、處理、利用規範是原則禁止，例外許可，因此，對產業之影響程度，應視例外許可之規定而定。生物識別資料在 GDPR 已納入特種個資範圍，因此亦建議納入，至於宗教、工會等涉及人權保障之概念部分，歐盟因有專責機關可做相關社會性質之認定，於我國是否須納入並無特別意見。

（二） 利用醫療個資在實務上的障礙，並非醫療個資之定義問題，而是個資法第 6 條但書第 4 款。適用該規定之主體限於公務機關與學術研究機構，商業研究則必須透過產學合作始得進行，觀察歐盟 GDPR 之規定，並未以主體進行限制。此外，要求書面同意部分，對於醫療端採取電子方式蒐集資料，並

行使同意造成很大困難。

（三） 案由二建議應將 legitimate interests(正當利益)清楚定義；案由三當事人自行公開資料部分，納入相容性判斷有其必要性，可參考歐盟對於相容性判斷之相關脈絡規範；案由四公共利益之類型化有其必要，且建議應納入利益衡量。以歐盟 GDPR 為例，雖未特別處理類型化的問題，但第 9 條規定於難以取得當事人同意時，須經過利益衡量，為保護當事人或他人之重大利益時得處理敏感性資料，會員國的立法，或司法機關解釋，可看出如何把公共利益類型化，區分為 substantial、important 與 general public interest 等類型。

（四） 前曾討論健保署研擬於健康存摺上同意權的行使透過區塊鏈技術進行簽章，但是否符合電子簽章法之數位簽章或電子簽章則難以確定，又電子簽章法主管機關為經濟部，但涉及個案認定則又須由衛福部醫事司解釋，而新技術是否符合電子簽章法之定義與要件，主管機關倘未釋明，就會形成實務上之運作困難。

七、開放文化基金會林法制顧問誠夏

（一） 書面同意依照電子簽章法第 4 條現行規定，倘雙方同意以電子方式為之，且可經事後查驗，則可將之視為書面；然而實務界仍有許多人未知相關規範可資準據，建議將電子簽章法此處規定，於新修訂之個人資料保護法裡，直接立文入法。

（二） 區分一般個資跟特種個資之目的是須給予特種個資之特別保護，並限制利用。例如工會身分在德國、英國、瑞士特別列為特種個資，而在我國，也會隨著工會抗爭(例如華航罷工)提升相關意識。倘若要擴充特種個資範圍，則須如同歐盟 GDPR 有科技設備(如資料儲存加解密保護)等相關配套措施，而目

前我國個資法之安全維護措施及相關事項之規定似乎太過空泛。

（三） 案由三針對依法公開之資料，不應被當作阻卻違法或阻卻侵權之條件，如德國司法判決亦會就個案權衡是否侵害個資當事人之核心權益。另應限於難以取得當事人事前同意之情況下，始可為之；並應納入公私益衡量。

八、理律法律事務所曾律師更瑩

（一） 特種個資範圍應是與各國歷史文化有關。歐洲係因歷史原因，而將種族、宗教、政治傾向、公會身分等列為敏感性個資；日本則是因蒐集相關資料將對當事人產生不當的差別待遇、偏見或其他不利益；我國 2012 年提出特種個資類型，包括病歷、醫療、基因、性生活、健康檢查及犯罪前科 6 種，其中關於犯罪前科有可能會造成歧視，但目前種族或歷史淵源、家族，反而是可能在臺灣社會造成歧視之類型，但卻不會被列入特種個資，文化與社會評價似乎與人民認知有所落差。針對特種個資類型需各面向之利害關係人討論取得共識，如雇主為管理職場安全，想知道員工確診狀況，但確診資料不僅是特種資料，依據傳染病防治法雇主亦需保密，相關規定不一定規範於個資法，而是在傳染病防治法或就業服務法。

（二） 案由二個資法第 6 條第 1 項第 2 款之「履行法定義務之必要」要件，但因法定義務內容規範不明確，違反將承擔刑事責任，因此實務上不會建議客戶使用此一合法要件。建議可於條文、或透過指引、解釋，進一步為細部的規範與類型化。

（三） 案由三部分，同意合法公開之資料須在特定目的範圍內處理，且應符合其目的性或利益權衡。案由四部分，因為公共利益、保護個人利益之相關概念並不清楚，實務上亦不會用以作為

合法要件。因此建議應有細部類型化、明確化之規定。若採納保護個人利益，則應該限於當事人或他人之生命、身體、財產之危險或限於難以取得同意之情形。

（四） 前曾詢問經濟部商業司，倘於實體店面購物加入會員，以平板電腦填寫個資，最後點選送出同意成為會員時，並於平板上手寫簽名，如何符合個資法規定之書面同意？獲得的建議是須檢視雙證件並全程錄影，才算完成電子文件，但這樣應沒有企業可達成。倘若以網頁點選同意可否認定屬電子文件部分，現在部分網頁會經過身分驗證程序，惟經身分驗證是否屬電子文件，經詢問商業司，僅得到依據電子簽章法第 4 條規定辦理之回復。

九、中華民國無店面零售商業同業公會塗副秘書長家興

（一） 案由一所提到新興科技的部分運用越來越廣泛，現在刷臉解鎖手機、刷臉付款或是智慧型手錶蒐集你的血壓心跳等資料，不管儲存在硬體或是連線到雲端，消費者應比較在意它的應用，如原目的係以指紋解鎖開關，但資料傳輸至雲端後是否做其他利用，建議思考應該做一些保護措施。

（二） 剛才謝律師提到公司申請電信服務的部分，電信業者要求任何變更都需要負責人雙證件，第一次設立登記可能還合理，但倘若所有變更都需要雙證件，我認為範圍過大。

（三） 案由三公共利益的部分，建議應該要有清楚的定義跟容易的判斷，避免無限制擴張。

十、本會李參事世德

（一） 有關個資法與電子簽章法之適用，法務部於 91 年與 96 年依電子簽章法第 4 條之公告並未包含當時之電腦處理個人資料

保護法，雖當時電腦處理個人資料保護法未明定書面同意是否包含電子簽章法，但是踐行的方式並未排除電子簽章法，所以仍適用電子簽章法。

（二） 101 年個資法擴大適用後，於施行細則第 14 條規定書面同意有電子簽章法適用，104 年修正時，以當事人同意蒐集一般個資時，不再限於須書面同意，書面同意僅限於特種個資，個資法施行細則第 14 條亦配合修正，因此，修正後之個資法亦無排除電子簽章之適用。

柒、 會議結論：

一、 有關是否擴張特種個資範圍，納入生物特徵部分較具共識，其他則就正當性謹慎思考，並儘量尋求社會共識。

二、 有關當事人自行公開或已合法公開資料納入目的相容性、利益權衡等要件較具共識；公共利益則多數意見認為應類型化，並納入必要性及利益權衡之考量。

三、 針對合法性要件中不夠具體、不具操作性之部分，將進一步思考，納入後續參考。

捌、 散會（下午 4 時 45 分）。

「個人資料保護法相關議題」第3場產學專家學者諮詢會議會議紀錄

壹、 時間：110 年 12 月 6 日（星期一）上午 9 時 20 分

貳、 地點：本會寶慶辦公區 B136 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、東海大學法律學院范姜教授真媺

（一） 日本 2020 年修正前的個資法基於憲法保障學術研究自由之考量，將學術研究排除於個資法適用範圍，但 GDPR 適足性認定時特別強調此部分不能排除適用個資法，所以於今年修法時將學術研究納入個資法之適用範圍。

（二） 日本 2020 年修正前的「個人情報保護法」適用於非公務機關，針對公務機關則適用「行政機關個人情報保護法」。由於對公務機關與非公務機關適用規範不同，對於研究規範亦有別，造成私立大學或私立研究機構、國立大學或國立研究機構因適用不同之法規範而結果不一致，此次修法則將「個人情報保護法」、「行政機關個人情報保護法」、「獨立行政法人個人情報保護法」合併為一部法律，也就是將於明年實施的個資法。有關學術研究的部分，新法將其納入現行法第 16 條、第 23 條，而其內容與現行法定義並無太大變動，包含範圍除學術研究機構外，尚包括學術研究機構的所屬人員，如會員、大學教授等。

（三） 日本考量私人倘因學術研究而保存個人資料，若濫用、目的

外利用或洩漏將難以管理；因此，從保護個人資料的觀點而言，並未開放「個人」之學術研究，仍需在組織架構下，得透過組織加以監督管理個人資料檔案安全維護或目的外利用。但在產官合作的部分則有放寬，允許學術研究機構跟民間進行合作開發，惟仍限於學術研究範疇。而所謂學術研究之目的，需視機構提出之計畫加以審查是否以學術研究為主要目的，產官研合作計畫內容可包含其他產品之開發目的，但若完全以產品開發為主要目的,則不屬於學術研究之目的。

（四） 修法前之「行政機關保有個人情報保護法」第 4 章之 2 規定對於行政機關非識別加工資料的匿名化制度已經有完整規定，而有關產業利用的部分，新法也併入相關規定。由行政機關先整理其保有的個人資料檔案，有可匿名化後提供產業利用者，再依「行政機關情報公開法」判斷是否有不能公開的事由之後，並公告哪些個人資料檔案經匿名化後，可依據計畫需求申請，再由情報保護委員會審查申請資格要件、計畫目的、計畫內容及安全維護等。最後，提供匿名化資料的行政機關，透過簽訂行政契約的方式提供匿名後檔案，並予以收費。

（五） 綜上，日本透過嚴格的審查機制加以控管，此機制涉及下次會議討論的去識別化議題；我國現行個資法關於假名化、匿名化之規定尚未釐清，建議於建立完善的去識別化機制後，再提供給非公務機關做產品開發或市場研究。現行法架構下，要合法提供產業利用有相當之困難，且必須建立如日本之妥適監督機制，實不宜冒進。

二、國立陽明交通大學科技法律學院陳教授銘雄

（一）從國家數位發展的角度，支持擴大適用的範圍。討論這些問

題有一個重要的思維，就是目的之不同，而非機構之差異。觀察各國的規定，重要的是目的本身必須具有某種意義的公共性，無論科學知識或公共利益產生的成果是屬於大家共享的，所以建議某種程度予以放寬，因此，「公共性」是很重要的判斷，同時應該要有相關機制，以確保對當事人的個資影響風險降到最小。

（二） 如何避免對個人權利的影響，各國做法不一，涉及到將來實行時，是透過全國一致性的標準，還是由各個目的事業主管機關去訂定相關標準。簡報第 15 頁提到個資法第 6 條第 1 項第 4 款修法前原有「經一定程序」之規定，但後來刪除，建議個資法應該要訂定稍微嚴格的標準，例如：公開聽證的過程，並經個資專責機關同意後彈性排除等方式；並授權目的事業主管機關根據其產業的特性訂定不同規範。考量立法的時程，可以參考其他國家運用監理沙盒處理相關議題。

（三） 商業機構的特性與學術研究機構具有差異性：第一，商業機構缺乏在訴訟法上得抵抗法院調取資料的權利；第二，商業機構(尤其是跨國公司)倘發生公司併購、破產等情形，致使資料保有者變動，將產生管轄權的問題；第三，商業機構較缺乏自律的倫理規範，應有其他機制確保商業機構的法遵。

（四） 針對相關監督管制措施，有由主管機關管制者，如：GDPR 規定於涉及大規模個資等情況下，有諮詢主管機關的義務，或要求進行 DPIA，或訂定契約範本；有訂定專法者，如：日本次世代醫療基盤法；或要求契約當中應該包含重要的原則：第一，禁止為再識別的行為、第二，資料移轉給其他機構時，也要簽訂相同保護程度的契約，確保其資料保護水準不會因為契約資料的移轉而降低、第三，當資料移轉後在別的機構外洩時，有追溯通知的義務。

（五） 有關假名化的部分，假名化本身也有程度的差別。例如美國 2013 年修正 HIPAA，加入 Limited Data Set 條款，其要件是將 18 種法定的識別因子當中去掉 16 種，符合以下兩個要件就可以不需要經過當事人同意，第一是必須基於某個特定的目的，例如公共利益、醫療或是科學研究之目的；第二是必須簽訂一定的契約，如：資料分享契約，滿足一定水準之資料安全保護。假名化的程度可能會因為不同產業類型而有差別，建議授權主管機關就各個產業訂定經一定程序之豁免條款。

（六） 有關「實質等同」，為相當重要之概念，例如生醫領域的資料，已有人體研究法、人體生物資料庫管理條例，如果主管機關能訂出實質等同的方式，套用在商業機構上，就可允許其在沙盒期間內進行研究。參考其他國家的作法，共通點是由專責機構審核，最明顯的機制是隱私影響評估，例如新加坡 2018 年設立的沙盒計畫（簡報第 31 頁），提到組織應進行資料保護影響評估。新加坡只限於促進業務改進目的跟基於研究目的，始可識別個人，若不以可單獨識別個人形式的利用，無法合理的實現目的，則有例外的保護條款(簡報第 30 頁)。新加坡是一個以服務業為主的國家，所以立法思維與我國面臨的問題有類似性，值得我國參考。

（七） 此外，針對假名化部分，許多國家會於個資法規定「禁止再識別」，並輔以刑事處罰。另外，菲律賓相關規定提到適用條件(簡報第 32 頁)，除了經過國家隱私委員會審查之外，也要符合專業道德倫理規則，此為第三方監管的概念，由專門監管機構來確認執法。

三、臺北醫學大學醫療暨生物科技法律研究所李教授崇僖

（一）個資法是基本規範，若其他法律有特別規定，則適用特別規定。因此面臨個人權利保護與公共利益、資料利用的價值，甚至產業發展等平衡上，對個人權利做某些限縮時，未必在個資法上做限縮，可以透過特別法處理。惟依以往經驗，政府在特別立法並不積極，如健保資料庫應可訂定專法處理，但迄今仍停留在個資法層次。特別立法也不全然是為了鬆綁規定或限制個人權利，亦可能是強化個資保護，補充個資法之不足。如：AI 倫理、AI 造成資料濫用的特殊形態等。歐洲的個資專責機關原有意監管 AI 時代的資料濫用問題，後來體認此非個資機關可處理，因此成立 AI 運用之倫理委員會或是管理機制。

（二） 建議應讓個資從個人權利保護的思維邁向資料治理、制度保障的架構，在不同的應用領域、依據不同的法規，由專責機關來把關，建構資料治理、制度保障的環境。目前有兩種做法，一是特別法，例如日本，另一個是成立個資專責機關。至於應採「學術研究」或「科學研究」用語，建議採用「科學研究」，且有 2 個方案，一是限於「學術研究機構」之「科學研究」，一是不限於「學術研究機構」之「科學研究」，要採哪一個，應看有無相關配套措施。

（三） 英國的數位文化媒體部在今年 9 月發布「Data：A New Direction」報告，UK GDPR 已施行 3 年，但在英國脫歐後，不一定會完全依 GDPR 規定，而可能配合整個數位發展，思考個資保護，尤其相較以工業為主的德國，其工業 4.0 或工業 AI 不太需要用到個資，英國則是服務業、金融業為主，個資利用是產業發展的重要資產，因此英國脫歐後，決定量身訂定法規。該報告內容包括如何釐清研究使用的定義和法遵及科研定義和科研利用，以及目的外利用的途徑。英國認為

內國法應有更明確的規定，如：GDPR 前言提到可接受科研、概括同意的方式，但是在條文內容卻沒有規定，導致解釋上的混淆。

（四） 很多先進國家為因應大數據的研究發展需要，重新檢視利用科研資料的法規，使其更明確化。建議針對學術研究機構提供較寬、較明確的法規，同時搭配專責機關之設立。另建議個資法明定部分例外條款授權專責機關審查之機制，使專責機關由整體制度性保障去考量，而非僅立於絕對保障個人資料自主權角度。

（五） 建議醫療大數據需要特別立法處理，醫療個資是特種個資，因屬於敏感資料，相關之利用規定應特別嚴格。但醫療個資的利用又涉及人權最基本、最核心的健康權利，若妥善利用這些資料可以提升人民健康福祉，甚至影響整個醫療資源的妥善分配利用，其公共利益性非常明顯，恐怕很難在個資法中找到平衡點，因目前個資法認為醫療資料要特別嚴格保護，所以建議另以其他法律處理，例如規定利用目的、去識別化標準、審核機制、申請程序與資格，甚至 IRB 的定位等，應要特別立法一併討論。

四、 臺北醫學大學大數據科技及管理研究所許教授明暉

（一） 醫療健康數據跟產業相關，中國在去年 1 月 11 日對全世界公布 COVID-19 病毒序列的資料，莫德納公司約 2 天就決定疫苗序列，不到 1 個月第 1 批莫德納疫苗就完成，也就是說取得數據在生醫產業不可避免。

（二） 有關學術研究，可區分為「轉譯研究」與「非轉譯研究」，轉譯研究就是目前應該有用途的研究，非轉譯研究就是暫時尚無用途的研究，學術機構每年向科技部申請計畫時，若不是

轉譯研究，非常難拿到經費，因為國家希望相關研究具有經濟效益。例如牛津大學教授放棄 AZ 疫苗專利，因已放棄產業利益，是否可認為是學術研究？

（三） 另外，TCGA 是美國國家衛生研究院(NIH)用稅金蒐集 1.1 萬個美國人的基因資料，類似我國科技部現在推動的健康大數據永續平臺， 2014 年 Data Use Agreement Certification 中提到不主張智慧財產權，因為健康是人類最大的利益，因此使用 TCGA 發表論文，再推廣新創產業，NIH 並不要求利益分潤。

（四） 美國亦把 5 萬人的加護病房電子病歷，去識別後公開給全世界申請利用，因美國認為經去識別之資料，就不屬個資。美國 Sweeney 教授在美國政府任職、也在哈佛大學任教，其破解州長去識別的資料，促成 HIPAA 立法，她說：如果認為可以簡單去識別則過於天真，不應因顧忌放棄去利用這些資料，但也不能天真認為有 100%去識別的方法。

（五） 另外，NIH 已開始注意脆弱族群，擔心因過度保護，讓某些族群資料不在研究範圍，反而對其造成一種傷害，所以應該用更寬廣的角度討論。在醫學領域，有以研究為原始目的的研究，適用人體研究法，對各方面的保護非常的嚴謹；即使非原始蒐集目的，也都要有知情同意，每一個研究計畫都是單一的同意，即使是去識別的研究，也准許病人有選擇參與跟退出的權利。

五、 臺灣生醫品質保證協會羅理事瑋瑜

（一）目前生醫產業界主要使用或接觸一般與特種個資，以臨床試驗或製造細胞醫療產品為主，臨床試驗階段有藥品優良臨床試驗規範(GCP)保護受試者的隱私資訊；在細胞醫療產品製造時，

目前有捐贈者適宜性的相關規定，來保護這些受試者或捐贈者的隱私。

（二）此外，像韓國或新加坡所定義的「為了業務或產品開發所需之研發活動」，產業亦有許多學術研究活動，而且這些學術研究活動並未與大學或醫院進行合作，而是在產業內部進行研究，可能包含檢驗方法或產品製造方法的開發等，會採特定或生物性的檢體，譬如血液、幹細胞等，採集這些生物性的檢體，會伴隨捐贈者所提供的特種資料及一般個資，用來判定血液適用性。

（三）針對「為了業務或產品開發所需之研發活動」，過去產業界在使用這些生物性檢體以及相關特種個資時，曾詢問食藥署相關法規遵循、如何合法利用個資，食藥署表示只要是產業的內部應用，不需要申請 IRB，也不需要申請臨床試驗。產業界也很怕觸法，一旦觸法，相關罰則將對公司營利造成極大影響，因此一般產業會做自主性管理，捐贈者來源是公司員工、員工的親友，或是特定客戶。我們會要求捐贈者簽署捐贈同意書，類似目前 IRB 所要求的資料，也包含產業界對於捐贈者資料之相關保護義務，且絕對不能洩漏。在產業界以 GCP 與 IRB 保護受試者的資料，目前多半是產業界做自主性的管理，避免資料外洩。

六、 淡江大學公共行政學系涂助理教授予尹

（一）關於個人資料的利用，不外乎是個人的資訊自主權以及公共利益兩者間的平衡，會有目的外利用的爭議，是如何解釋合法要件的問題，若要追求個人資訊自主權、個人資料保護，無可避免對公共利益的實現會稍微嚴格，若要追求公益的實現，個人的資訊自主權，就有可能受到一些傷害。

（二） 關於個資法第 16 條第 1 項第 5 款學術研究的要件放寬，應考量如何在追求公共利益、學術研究的前提下，讓個人資訊自主權可以獲得平衡。目前個資基於學術研究目的使用，符合 16 條第 1 項目的外利用的要件者，不需當事人同意，與其說放寬，更是學術研究概念釐清。

（三） 放寬到產業發展之範圍，我個人持保留態度，因為從學術研究跨足到產業發展的範圍較廣，且對於個人的資訊自主權的侵害程度也更強。但是界定學術研究跟產業發展也不容易，各國的定義不同，界定其定義有困難度，若將學術研究推到產業發展的概念，建議要做更細緻的安排。

（四） 而如何區別產業發展或學術研究，我認為重點在於目的別而非機構別，雖然可以定義學術研究機構，包括大學、公私立研究機構等，但這些機構所做的事情是不是純然就是學術研究，有解釋空間。學術研究機構也有可能因為產學合作關係，有一些產業發展的面向；相對的，產業界投資在新產品、藥品技術的研發等，也有基礎研究，所以我認為單純從機構別做區分，不是非常適當。立法技術上或許可以負面表列的方式，例如哪些不適合解釋為學術研究的概念，在個人資料自主權與公共利益之間求取比較好的一個平衡點。

（五） 個資保護獨立專責機關相當重要，希望臺灣未來也有自己的 PDPC。目的外利用之合法要件，以學術研究為例，依照個資法第 16 條第 1 項第 5 款的規定，不需要當事人同意，也沒有告知義務，而學術研究過程隨著對個人資料侵害性加強，是否也要賦予個人在一般的情況下有退出權？若個人連受到告知都沒有，又如何行使退出權？也許難以逐一告知，但至少告知獨立專責機關作為代替。建議未來的 PDPC 要有更積極的權力，包括像日本個人情報保護委員會跟資料利用者，訂

定行政契約作為監管方式；建議未來的個資獨立專責機關，接受報備跟主動進行許可之間的權力必須要掌握，這樣才可以作為公益代理人。

（六） 綜合而言，若個資法第 16 條第 1 項第 5 款豁免的要件，從學術研究跨足到產業發展，或許是將開放政府應討論的議題納入個資法。界定開放政府與個資保護比較大的差別點，在於開放政府 open data 的想法下會有資料監理的問題，政府有資料監理的義務跟責任，故這個議題也要跟開放政府的議題跟退出權的議題合併思考，也包括個資獨立專責機關功能的討論。

七、 達文西個資暨高科技法律事務所葉律師奇鑫

（一） 去識別化的規定很重要，與合法要件有連動關係，也就是去識別化如果規定越完整、越嚴格，那合法要件就可適度放寬，反之，如果去識別化的規定不夠清楚，合法要件就要嚴格。另外，亦贊成去識別化規定應更完整，有助於對政策的說明，並化解民眾的疑慮。

（二） 今天討論的題目有多種情境，個資法畢竟只是基本法，建議特種個資的部分，應該由該產業的主管機關為特別規定，例如健保署的資料如何使用，健保署有非常多的醫學專家、有管道跟醫學界聯繫，或官員就是來自醫學界，會比國發會或未來的獨立機關更了解。雖然可採用沙盒，但沙盒是暫時性的，例如金融沙盒要求試驗後三年內要立法，並非反對沙盒，只是沙盒試驗後，仍須由法律規定，因為牽涉到人民的個資基本權利義務。

（三） 一般個資也有可能由主管機關(例如經濟部、未來的數位發展部)另外訂定相關規定。個資法為基本法，因此仍要討論基本

原則，但因為實務上情境多元，例如醫療、網路大數據，性質差別很大，無法規定在同一個構成要件。美國也是 CCPA 規範較鬆，但 HIPAA 規範就很嚴，難以規定在一個基本法中。

（四） 贊同學術研究與學術研究機構一定要定義，因為違反個資法有刑事責任，若適用範圍有爭議，會增加法律適用的不確定性，主要是涉及刑責，而如何定義則是另外一個問題。學術研究尚無正式定義，科學研究不限於跟錢有關，但學術研究大致上會跟錢無關，而科學研究例如 mRNA 有巨大的商機。現在很多學術研究跟產業有密切關係，全世界皆如此，例如美國大學的專利原本屬於國家，現在則屬於學校，並希望孵化一些新創產業，像 Google 就來自史丹佛大學。世界各國的科技產業基本上都是和學術彼此互相扶持，若僅限「學術研究」勢必會窄化發展，臺灣科學研究比較多、基礎研究較少，臺灣很多產業在國際上有競爭力，多是產官學合作結果，也都跟金錢有關。因此較贊成採用「科學研究」用語，因其允許一定的利益，而利益是研究非常大的驅動力，亦對人類社會有幫助，再以去識別化的機制保護、合法性要件的限制，以及各目的事業主管機關的監管，還有特別法的監督，較符合臺灣目前產業的需求。

（五） 提醒要注意國際傳輸與本議題的關聯，建議研究團隊稍微考慮此問題，例如金管會規定不允許金融機構將資料傳到國外雲，但是現在準備開放上傳到國內的雲。因為金融機構的資料是信用財務的資料，金管會認為非常敏感，所以嚴格限制。依照目前 AI 的發展，並非不使用國外的計算力就能解決問題。AI 比的是計算力、模型跟演算法，這個議題跟國際傳輸會有間接的關係，建議下次可以納入這個議題。

（六） 有關間接蒐集的告知義務，現行個資法規定尚屬足夠，因直

接蒐集時須告知，稍有規模的學術研究樣本量大，不可能個別告知，因此歐盟 GDPR 也規定不用告知。我贊成涂教授所述，若個別告知不可行，能否以其他方式，例如向第三方單位進行通知，或以網路公告的方式，像現在個資外洩時，若數量過大通知有困難時，也允許用網路公告的方式告知。

八、 中華 R 軟體研發暨應用協會楊常務理事雅惠

（一） 協會例如健康醫療業、大數據的金融應用，或者在行銷領域有很多產業的業者，如同葉律師所述，在不同領域的應用上落差很大，要限制的方法跟範圍也有很大的不同，要一部法律一體適用有其困難，建議在不同的領域去個別制定規則，可能不見得是法律層級。

（二） 本次會議討論的題目，對目的外利用的影響比較大，因為如果是目的內利用，不管是做研究或者提供服務，學術單位或業者都很清楚要符合的規範或是履行告知的義務，如同剛剛羅理事所述，業者不想觸法，比主管機關還緊張擔心，所有環節都很小心處理。但是目的外利用受限個資法規定的適用對象與目的，在公益性的部分發揮很大的影響，雖然同意在個人的保護跟公益性必須要取得平衡，但目前業界較傾向個人的保護，整個公益性相對來說權重較小。

（三） 立法時，雖然可以參考很多大國的規範，但亦應考量人口規模的差異，例如美國的一個醫療保險集團，可透過自己的商業機制蒐集大量資料，發展公共利益的服務，但在我國若不用聯合、資料互相交流或匯流的方式，其實很難達到。因此討論法規要鬆綁到什麼程度，建議不能完全參考英國、美國或日本等人口較多的國家，可參考新加坡、菲律賓或韓國，較容易達到公益跟個人資料保護的平衡。

（四） 目的外利用的部分，研究機構較有鬆綁的空間，其不一定是公共利益或學術研究,而且規範目的會比規範機構更有意義。規範目的從條文來看是以學術研究為主要，有論者認為不能與錢相關，但如同剛剛葉律師所說的，可以不用避諱談錢，因為錢是最大動力，如果不涉及金錢利益，研究動機就會變小，我國科技發展速度相對會變慢，因此不贊成限縮在學術研究，較贊成以科學研究，或者以負面表列的方式規範哪些研究不得進行，對業界而言較容易遵從，排除不可以做的事情後，業界的應用就會很多元，對整個社會而言，會是一個比較正向的發展。

九、 國際通商法律事務所余律師若凡

（一） 贊成放寬科學研究目的意見，如同前面先進提及，實務很多研究不只有學術跟科研單位，亦有許多產業界研究，尤其例如穿戴裝置、IoT 相關廠商，原則上廠商在蒐集資料可以接觸到這些資料，也有一些計畫可以做更多研究。研究方式可能為組織內的研究，或直接與學術或科研單位共同研究，甚至廠商先進行相關資料研究後，再分享給其他相關的第三方單位。目前規定尚不夠清楚，有很多產業不易遵循。

（二） 個資法第 6 條第 1 項第 4 款規定，希望讓公務機關跟學術研究機構可以有更多利用，實務上常被詢問一般產業機構研究是否只要資料不能識別當事人就可直接利用，尤其去識別化或無從識別並沒有嚴格定義，而造成適用的困擾。

（三） 議題三會與其他議題連動，不只是在去識別化的部分，還有涉及國際傳輸是否要求在地化，或主管機關的權限等連動議題。我認同以目的控管，但應思考不同面向，例如現在缺乏產業面向，針對產業如何研究設計其相對應可遵循的規範。

（四） 贊成採用沙盒的方式，雖是短期運用，但現在產業有很多想法，很難透過個資法或主管機關事先想像可以研究的範圍，或許可透過沙盒保留相當的彈性，達到個資保護以及確保各類研究之發展。

柒、 會議結論：

一、 感謝各位先進提供思考觀點，我國個資法目前係由各部會分散管制，未來個資法應該會朝成立專責獨立機關之方向修正，將關注如何因應各類不同的科技技術、主管機關及產業不同的需求，運用子法或其他方式賦予彈性管理。

二、 有關運用醫療個資相關討論，或許可以採用監理沙盒的方式，特別是數位時代的快速變動下，出現許多創新型態的產業模式，難以事先想像且複雜多元，然而監理沙盒制度仍須由各部會之監管立場為主導。非常謝謝大家今天的蒞臨及參與，提供許多寶貴的意見及觀點。

捌、 散會（上午 11 時 30 分）。

「個人資料保護法相關議題」第4場產學專家學者諮詢會議會議紀錄

壹、 時間：111 年 1 月 13 日（星期四）上午 9 時 30 分

貳、 地點：本會寶慶辦公區 513 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、中國文化大學資訊工程學系蔡副教授敦仁

（一）經濟部標準檢驗局（簡稱標檢局）訂立的國家標準 CNS29100-2 資訊技術－安全技術－個人資訊去識別化過程管理系統之前身為「個人資料去識別化驗證規範」，最初訂定目的係避免產業運用 open data 牴觸個資法，由行政院討論訂定標準，讓業者通過驗證後較有信心使用該等資料。初始係由台灣商品檢測驗證中心（Taiwan Testing and Certification Center, ETC）進行驗證，選定財政資訊中心，針對 103 年家戶綜合所得稅資料去識別化，將 720 萬筆資料中數百個欄位留存 72 個。後續行政院指定內政部與衛福部辦理個資去識別化驗證，最終衛福部將幾批資料驗證並取得證書。

（二）現 CNS 29100-2 將於 2022 年由全國認證基金會（TAF）接手認證業務，認證程序係先由 TAF 針對驗證單位做認證，再由驗證單位到各機關、團體、公司進行驗證，驗證通過後才頒發蓋有 TAF（Taiwan Accreditation Foundation）之證書。受驗證單位主要可能是已取得 ISO 27001 資訊安全管理系統驗證證書的單位，至於取得驗證證書之效果，如研究單位簡報第 19 頁

提到法務部 105 年「公務機關利用去識別化資料之合理風險控制及法律責任」研析報告的驗證功能。驗證是對於去識別化過程進行驗證，基本上是採取技術獨立，不特別指定技術，現在業界主要以 K 匿名技術作為最後成果的檢驗。

（三）去識別化技術包含匿名化及假名化，目前 CNS/ISO 20889 隱私增強資料去識別化術語與技術分類，已整理去識別化技術標準，未來可能根據此技術報告產出各行業特定去識別化標準，係值得參考的範本。

（四）驗證的核心是「隱私風險」，無論以何種技術去識別化，其風險不可能為零，需考量最後「剩餘風險」可否可被接受。風險與當初設定應用的環境與情境有關。例如 open data 讓不特定對象使用，其要求之去識別化程度較高，但也會造成可用性降低。任一資料去識別化前，應先設定未來使用的情境與相關管理的措施，例如衛福部資料中心在全國有 8 個管制環境，提供學者專家為學術論文使用，其去識別化程度不會如 open data 嚴謹，以利於學術用途。

（五）資料隱私保護與資料使用二者互相衝突，例如 big data 講求關聯性越高越好，隱私保護則要求關聯性越低越好，如何同時顧及二者，就是剩餘風險可否被接受的議題。現在電子商務或行動商務發達情況下，例如 Apple Pay、Samsung Pay 進行符號化（tokenization），將信用卡轉成另一組號碼，該資料對於攔截號碼者無法辨識，是假名化的概念。該機制有兩個先決條件：（1）一次性使用（one time use）只針對特定目的；（2）有中央控制系統讓資料可逆，可以重新識別。目前許多電子商務使用符號化作為去識別化方法之一，建議未來個資法將實務發展納入相關規範。

（六）CNS 29100-2 有保留「重新識別」一節，在某些嚴格控制或要求情況去識別化必須可逆。若要求產業做到完全不可逆，實際上會有很多機制無法運作，建議規範該可逆的狀態在可控制或值得信賴的環境之下，由政府或相關法人留存去識別化的資料、相關證據或需要重新識別的資料。例如：金管會針對 KYC（know your customer）作業，就允許金融機構蒐集的資料轉給另一個金融機構，不需要再重新填表格，也許未來也可以建立類似機構以進行中央管控。

二、國立陽明交通大學科技法律學院陳教授銘雄

（一）規範是否要在法律中明定，取決於相關規範未來是否得由專責機關另外訂定，若無專責機關得為事後規範，則於法律中加以明定。相關制度係因有資料分享需求，而將資料交給他人時，得透過契約確定標準一致，但是違反契約僅具有民事責任之效果，因此訂定相關法律以提高行政裁罰，甚至刑事罰。許多國家更以刑事處罰再識別行為，例如日本《次世代醫療基盤法》即規範員工本人若違反規定會有刑事處罰。

（二）建議應提供激勵（incentive）措施，提升機構採取匿名化或假名化措施之意願。匿名化與假名化使用的範圍不同，而因假名化區分為高度與低度，較易產生爭議。日本對於驗證機構的假名化過程有詳細描述，其他國家對此並無明確規定。美國 HIPAA 對於假名化「有限資料組」（limited data set）的規定，屬於高度假名化措施，共有 18 種識別資料，去除其中 16 種、留下 2 種跟其他資料進行連結，以得到關於一個人整體面向的資料。因此要建構關於個人的文檔（profile），該資料有些是影像或數字的連接，而在「有限資料組」下不需要得到當事人同意，但有兩個條件：（1）符合特定合法目的，以及（2）簽署「資料分享協議」（data sharing agreement）。

（三）我國健保資料庫也有類似高度假名化措施的規範，106 年判字第 54 號判決重點在於，衛福部雖有金鑰可以辨別資料，但衛福部的內控機制風險很低，因此允許衛福部採用透過內控要求換取不經當事人同意的作法。

（四）高度假名化是我國法律的灰色地帶，低度之假名化與匿名化適合在法律中明文規定原則禁止例外許可，經由主管機關規範許可，讓高度假名化可運用在個別產業。而部分國家係就敏感或一般個資分開規範，例如一般個資的保護密度較低能在個資法中明定，敏感個資應透過各業別主管機關制定該領域法規。至於標準，則贊同採取英國的「有心侵入者測試」。

三、東海大學法律學院范姜教授真嫩

（一）日本於修法前只有匿名化之規定，在產業利用上產生很多困難，因為匿名化程度越高資料可用性越低，所以在 2020 年修法時加入假名化資料之規定。我國關於匿名方式雖然施行細則已有詳細規定，建議可參考日本國立情報研究所對匿名加工資料方法之詳細規範報告書，惟日本政府就匿名化之技術與規範訂有指引供參考，然業者仍認為相關規範難以理解、難以分辨是否需匿名化、是否符合標準等。在此次新修法納入假名化，無論匿名化或假名化之資料仍皆屬於個資，只是匿名化個資之目的外利用或提供第三人無需得到當事人同意；而假名化則限於企業內部研究之用，雖放寬個資利用，但仍限於企業內部研究利用，無法提供給第三人，後續效益目前尚無法確定。

（二）不同於歐盟以最高技術水準不可回復原狀為基準，由於個資有流動性與相對性問題，日本將匿名化要件明定於個資法，不從技術面設定「永遠不能回復」的要件，而是規定匿名化過程必須透明化及機關應公告之相關資訊等，由社會發揮監督的力

量，監督違法濫用或回復原狀的事情發生，建立匿名化或假名化資料可被安全合理利用的機制。

（三）此外，匿名化資料不得回復原狀。因此，匿名化資料提供第三人使用，可不經當事人同意，但應要求第三人不得將匿名化資料回復原狀，違者有相應之處罰，即「雙方戴口罩理論」；業者對於匿名個資的流向有紀錄義務，若資料回復原狀可立刻查詢軌跡紀錄，查明何環節之違法。

（四）日本《個人情報保護法》只有規定匿名化和假名化要件與加工時遵守之原則，而由獨立專責機關以命令或行政規則就詳細加工方式等予以規定，但因各業界要利用個資的目的與方法不同，因此匿名化與假名化的方法與程度也會不同，若要全部由監督機關負責確有困難。

（五）另外，日本《次世代醫療基盤法》將醫療資訊之匿名加工利用方式另立法為規範，主要是由於醫療資訊的價值非常高，考量其屬敏感性個資，且具高度公共利益及利用可能性，若被濫用對個人傷害很大，不應規定於個資法，建議我國亦應另為規範。

（六）是否達到匿名或假名標準，法規有二個層次：第一層次是「識別性」以何者為判斷對象；簡報第 14 頁所提「特定人基準說」是在討論政府資訊公開是否涉及個人隱私時採用之標準。有關個資匿名化之判斷日本現採「提供人基準說」或「一般人基準說」，此點在我國學者間未有一致看法，日本則是經過一段時間討論後，採取較不嚴格的「提供人基準說」，以原持有資料者為判斷對象。第二層次是「以何標準判斷有無回復能力」，此部分不採「提供人」為標準，而是以「一般業者」之技術水準是否可回復，作為標準。

（七）事實上，日本在匿名化或假名化過程中，除了徵詢學者專家或

業者意見以外，還會邀集利害關係人（stakeholder），包括消費者團體、業者、主管機關等共同開會討論，以訂定標準，因為個資利用會牽涉到社會價值判斷，也要讓消費者安心，訂出國民可接受、「具有社會容受性」的規則，以取得社會大眾的信賴。

四、理律法律事務所曾律師更瑩

（一）根據研究單位的報告，匿名化與假名化是有技術程度差別，並沒有不可回復的去識別化。贊成訂定於法規，並考量合理性，在什麼情況下可以認為它不是個資，其效果與技術建議於施行細則或透過指引去訂定，以利於配合時間與技術變化而調整。

（二）贊成假名化的概念應在法規明定，如同陳教授所述，如果符合某一種標準是高強度的假名化，則應該要討論在個資法上的各項權利義務或所受到的限制是否不同？例如研究團隊簡報第24頁，比較法上假名化之效果多數為免除個資事故的通知。以駭客入侵為例，實務上業者的疑慮是倘若駭客拿到的資料無法辨識當事人，為何業者還需要進行個資通報等。因此，在資安事故部分，若達到一定程度的假名化，且外界以一般標準無法輕易辨識時，應至少可免除個資事故通知。

（三）至於排除當事人權利等立法例，或許可考慮是否依據使用目的判斷，如學術研究目的，則予以放寬，或考量醫療資料的特殊性，則予以限制等，或是提供一套不同的規範。至於業者期待的資訊分享與行銷則較難處理，因不適宜過度寬鬆或嚴格。

（四）另外，對於「技術中立」部分，電子簽章法的立法就是技術中立，但技術中立會導致業者不知道哪個電子簽章是可以合法使用的技術，不論技術名詞是否寫入法規，若有更多例子協助業者瞭解其法律效果，使業者在開發技術時有範本可以參考，知

道該技術在法律上的效果，始能提升業者使用該技術之意願。

五、　臺北醫學大學醫療暨生物科技法律研究所李教授崇僖

（一）技術標準不宜訂在法律中，參考 GDPR 立法例係由各會員國國內的專責機關視情況調整規定。再者，資料匿名化程度越高或加密程度越高，則管理此資料的成本越高，且資料利用價值越低。因此，歐盟 GDPR 強調受託處理者（data processor）的角色，明確規定相關的權利義務，以委外處理作為解決這個困境的重要機制。

（二）匿名處理或假名化處理是一種加工處理方式，在加值處理後不必然會使它的利用價值降低，若已知道利用目的，可在匿名的前提下為標籤化，雖然匿名後無法還原身分，但是可以對它做分類或標籤化，使得該資料雖非與身分有關的編碼，但對利用者來說是有用的。技術、產業和法律三個環節具高度相關性，法律必須提供產業一個框架，產業才能去發展技術，產業亦可協助法律落實。

（三）從技術中立的角度，是鼓勵技術發展，但是 big data 於適用現行個資法上有許多困難，此牽涉到在個資法中是採取相容模式，或是採不相容模式，而另外訂特別法。個人較傾向另訂特別法，但並非針對整個大數據利用皆訂於特別法，而是針對「特定領域」之大數據另訂，例如醫療領域的健康大數據，使其不受個資法基本原則的限制，但仍有專責機關加以監管。

六、　國際通商法律事務所余律師若凡

（一）產業目前最困難的地方是不確定匿名化、假名化之相關規範，觀察法院對「無從識別」當事人的見解亦未臻一致，難以分辨資料整體是否適用個資法。如同剛剛曾律師所述，產業即

使從法院判決也無法判斷到底是否為個資，這部分建議透過立法釐清基本概念，以提供可依循之判斷標準，也讓產業知道基本概念的分別。

（二） 實務上較少將風險概念帶入去識別化或無從識別，考量匿名化不可能完全匿名，因此應讓業界知道，匿名化時之風險因子，使產業可評估可逆或不可逆風險因子等。

（三） 運用個人資料的公司也包括國際公司，其資料庫並非僅處理、利用臺灣之資料，建議日後使業者判斷未來風險控管或應採取的驗證標準，也考慮與國際標準接軌。

（四） 現行個資法對於個資運用，主要是學術科研或公務機關的利用，並未考量產業應用，建議對於產業應用，考量利用之公益性、提供當事人加入或退出之選擇權等因素開放，亦得以沙盒的方式進行測試。

七、 達文西個資暨高科技法律事務所王律師慕民

（一）韓國 2020 年修正前的個資法並未規定匿名資料，而修法後於第 58 條之 2 引進匿名概念，其規定為：「以合理時間、費用、技術予以評估，即使結合其他資料也無法識別個人者，不適用本法」。此外，韓國在 2020 年修法時，亦將假名資料納入規範，將其定義為：「若不結合其他可還原識別的其他資訊，就不能夠識別特定個人的資料」。

（二）建議一併討論匿名化、假名化之限制與義務，參考韓國個資法規定，即使未取得當事人同意，但基於統計、科學研究、公益等目的，可以使用假名資料，且提供第三者時，條文明訂不得提供可還原識別的資料，須分開保存。韓國個資法第 28 條之 3 也特別提到，若要結合不同人所保有的資料，需由

個資保護委員會或相關中央行政機關首長指定之專門機關執行，建議可以觀察後續實務運作情形。另外韓國也有安全措施之規定，政府會頒布相關的假名資料的技術、管理、組織上的安全措施及配套規定。有關陳教授提到的誘因，在韓國的規範就是假名資料不適用某些個資法規定，例如可以豁免某種程度的告知、保存期限、個資侵害事故通知，以鼓勵業者使用假名資料。

（三）贊同匿名或假名於個資法清楚訂定，因為去識別化的方式，於現行個資法確實可能造成誤會或不知如何適用，雖然本次議題討論主要是針對產業，但我認為公務機關也有運用之需求。前面先進提到衛福部衛生福利資料加值應用中心有完善規定，也可以參考例如勞動部勞動及職業安全衛生研究所之相關作法，由申請人提出申請，在可控的環境下把資料帶入，並先經過倫理委員會按照計畫目的審查，讓其在可控的實體網路環境下串接資料，再將結果就資料匿名化進行審查，確認該資料無從識別後才可攜出。

（四） 討論匿名或假名之法律要件時，建議從三個方面來討論：

1. 匿名與假名之資料，於資料的保存與刪除能否有一定條件的放寬？很多業者期望在特定目的消失或期限屆滿後，得以不可識別的方式來保存資料，而非刪除資料。

2. 我國很多中小企業不見得有能力分析資料，會有委託分析或處理的需求。由於較多境外業者提供相關技術，但由境外雲端服務業者進行資料分析，會牽涉到跨境傳輸的議題，將來若禁止此種傳輸，可否用假名化或其他方式因應？參考金管會針對金融機構委託處理業務相關的管理辦法，委託雲端服務業者之資料，要求以加密或代碼的方式導入安全措施，若

此雲端服務業者是境外業者則須事先申請。

3. 與第三人分享、提供或串接資料，可否用雙方共同的 key 值將兩個欄位勾選計算出更大量的資料？牽涉到這個 key 值是原始資料，或是必須要用雜湊（hash）、編碼還是假名的方式來進行，以及資料如何運用。若要討論匿名或假名，在要件上從內部、委託與第三方這三個角度來討論，既然要區分匿名與假名，就要有不同的法律效果，匿名的效果應該回到函釋見解－完整的去識別化可不適用個資法，且條件要嚴格認定，否則實務上會發生機關自認為達到匿名就開始利用，但是資料輕易被還原，此時雖然受到處罰，但當事人的權益已經受損。

（五） 去年 8 月愛爾蘭罰 Whatsapp 2 億多歐元，Whatsapp 表明資料已 hash 處理，而且 hash 不是 1 對 1 而是 1 對 16，其目的並非為了識別特定個人，只是幫助用戶的朋友註冊後，用戶可以找出對方。愛爾蘭資料保護委員會（Data Protection Commission, DPC）原接受此說法，惟經歐盟個資保護委員會（European Data Protection Board, EDPB）徵詢其他國家主管機關意見後，則認為在 GDPR 規範下，能否識別的重點在於風險而非意圖。因此重點應放在「識別風險」，雖然嚴格規定會導致使用匿名資料的意願降低，但是建議導入 GDPR「合理可能」的要件，否則難以鼓勵使用匿名資料。

（六） 假名化是強調安全措施、識別對照資料另外保存，然後搭配放寬目的外利用、保存期限、侵害事故通知等，及其他限制，如韓國限制在某些目的使用假名資料得不經當事人同意，或以簽約方式申請特定的假名資料，在契約內控管風險，於契約約定試圖重新識別者應承擔之責任或是禁用資料庫等處罰，也可考慮分為一次性或永久性提供資料。

（七） 至於技術加工方式，同意前面幾位先進的意見，因為法律的修正比不上技術更新的速度,用法律規範可能無法及時因應,建議法律可以訂出框架，再以施行細則、指引或其他方式來適當更新加工方式。例如若 CNS 標準控制措施達到的效果是去連結，與假名規範相符，在假名措施的框架下，會有剩餘風險，則剩餘風險可由運用機關評估訂出相關規範。

八、 中華 R 軟體研發暨應用協會楊常務理事雅惠

（一）從資料服務業者的角度，比較贊成在法律中明確定義匿名與假名，讓業者有明確方向可依循。但是相關定義建議要區分不同情境，例如我國個資法用最終呈現的方式來做評估，如果在最終呈現上可以達到匿名的效果，是否就可以排除適用個資法，若有明確的定義，對業者而言會較易遵循。

（二）至於如何做到匿名，因技術日新月異，方法亦各有不同，在法律定義何種程度才是匿名，或認定不可復原皆有困難，事實上應無任何的技術是完全不可復原。業界需要較清楚或不斷擴充修正之指導原則或方針，俾供參考與遵循。

（三）認證亦為可採之方向，許多情境下，資料匿名化後就無法使用,很多分析目的都無法達到,而失去產業應用資料之目的,此情況下，假名化為可行的方向，許多外國立法例會規範限於企業內部使用，規範就較為寬鬆，包含臺灣很多企業將資料委外處理，是否等同企業內部使用，這部分需要有明確的定義。

（四）於資料分享提供第三方使用部分,建議未來要有清楚的定義,使產業界易於遵循。至於管理措施，所有管理措施都會產生成本，若我國個資法參考英國規範方式，要求業者承擔一定的責任與義務，相信大家某種程度下會願意承擔。

九、 淡江大學公共行政學系涂助理教授予尹

（一）應先確認本案蒐集之各國立法例，所使用匿名化或假名化的詞彙定義，是否相同？「去識別」應是一個狀態，假名化或匿名化只是為達此狀態所做的努力，去識別化或可作為匿名化及假名化的上位概念，而依其去識別程度的差別可能可以分成匿名化與假名化。

（二）以目前個資法施行細則第 17 條的規範模式而論，其規定「依其處理方式無從識別」，涉及個資法第 6 條、第 9 條及第 16 條等規定之「無從識別特定當事人」是指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從識別該特定個人者，此條文解讀重點應該在「以代碼、匿名、隱藏部分資料或其他方式」，而非「無從識別」，因為依照個資法第 2 條對於個人資料的解釋為「…得以直接或間接方式識別該個人之資料」，若已無從識別就不是個人資料，就不適用個資法，亦無於施行細則規範的必要。

（三）另外，在各種不同個案情境中，對於代碼、匿名、隱藏部分資料，須達何種程度有不同看法。依最高行政法院 106 年健保資料庫個案的判決主張「本院認為資料尚未去識別化，主要的理由是輔助參加人衛福部與被上訴人都有還原資料與主體連結之能力。此等結果顯然與由被上訴人單方掌握還原能力之去識別化標準不符。」但此判決對上訴人（台權會相關代表）及衛福部與健保署之間最大歧異在於，最高行政法院判決認為健保資料庫處理的做法已經可以達到匿名要求，而台權會認為尚未達到匿名要求，最多僅達假名程度，因衛福部尚掌有金鑰可以再識別。

（四）從健保資料庫判決觀察，建議未來個資法修正重點應將匿名

與假名要件定義清楚，達到匿名化程度才能為目的外利用，或至少要類型化。假名化與匿名化各自都有處理的方式，建議應規定哪些效果足以認為達到匿名化或假名化，另因為技術中立，理論上規範結果即可，不需規範過程。

（五）個資法是普通法，不同種類的個人資料，在個別法律領域內都有進一步加強或放鬆管制的正當性。而個資法應訂立匿名與假名個資的要件，以作為一般性規定，例如金融、醫療個資是否在何種程度內要有更強烈的擔保義務，應由個別法規規範。

柒、 會議結論：

一、 個資法必須與時俱進，過去個資法訂定時未預想到資料會具有高度價值，目前共識是匿名及假名之規範應更明確，使產業有所適用，目的是產業發展與個資保護雙贏。

二、 法規需要衡量個別產業與個別應用情景，在產業運用與個資保護之間取得平衡，規範訂定的細節程度，與執法機關的風險控管能力有關，其中匿名化的成本高、運用範圍廣；假名化成本低、運用範圍低，應回歸成本控管角度或依應用情境決定，法規之訂定應該更有彈性。

三、 訂立彈性化的法令是一個很大的考驗，因為會涉及不同產業界、各種利害關係人。個資法將會朝有獨立專責機關的方向修正，後續再由獨立專責機關為風險控管與執行，會將所有利害關係人納入討論，感謝大家提供寶貴的意見。

捌、 散會（上午 11 時 45 分）。

「個人資料保護法相關議題」第5場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 2 月 25 日（星期五）下午 2 時 30 分

貳、 地點：本會寶慶辦公區 610 會議室

參、 主席：高副主任委員仙桂(楊參事淑玲代理）

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、世新大學法律學院戴副教授豪君

（一） 有關控管者與受託處理者之關係，我國個資法係規定委託關係，雖未使用受託處理者之用語，但仍採受託處理個資之概念。

（二） GDPR 將控管者之基本責任規定於 GDPR 第 24 與 26 條，受託處理者責任則規定於 GDPR 第 28 條。另外 GDPR 第 28 條第 9 項規定，委託者與受託處理者間之關係須以契約約定，歐盟並有實際裁罰案例。2019 年 10 月波蘭政府公報中心委託其他受託處理者處理個資，惟未依該規定簽訂契約，因此波蘭個資保護主管機關（Urząd Ochrony Danych Osobowych, UODO）對其開罰。若我國要參採 GDPR 第 28 條第 9 項的規定，則須討論未簽訂契約者如何處罰、屬行政處罰或民事責任等議題。

（三） GDPR 針對控管者和受託處理者的責任規定大致相同，第 27、30、31、37、46 條係共同規定，第 25、33、35、36 條則僅規範控管者。而我國個資法施行細則第 8 條則多有認為逾越母

法規定，課予受託人跟委託人非母法規定之義務。即使委託人履行個資法施行細則第 8 條之義務及監督工作，其責任仍未被免除，因個資法第 4 條規範受託者所有行為責任由委託者負擔。一般而言，倘要求委託者有監督管理義務，則其善盡此義務後，責任應有一定的免除。建議未來將施行細則第 8 條回歸母法規定，至於契約內容是否需使委託人有監督受託人之義務，則有爭議。歐盟僅要求締結契約，並未賦予監督義務，而我國要求委託人監督受託人不合理之處，在於委託人可能係因欠缺相關專業才進行委託，因此亦難以善盡監督之責，建議考量是否要以監督方式，或以契約約定。

（四） 去年英國 Heathrow 機場推動旅客自動化流程，原本過海關、託運行李、檢疫、免稅店、登機須不斷出示護照和登機證，而此流程，可在經過當事人的同意後，從機場報到至登機全程以臉部辨識自動化方式通過。此為共同控管者之案例，因過程中資料流會經過如海關、航空公司、地勤公司、免稅店、保安、機場服務公司等，利用共同控管者的概念，全程自動化通關，故贊成建立共同控管者制度。

（五） 共同控管者待解決之其他問題，如個資衝擊影響評估（Data Protection Impact Assessment, DPIA），機場旅客自動化流程，可能海關認為對個人權利影響重大，但免稅店則認為影響輕微而無須進行 DPIA，倘若其處理的部分未對當事人權利造成重大影響，亦未觸及特種資料，依法無須進行 DPIA，但若其他共同控管者將蒐集特種資料，會否使整個流程皆須進行 DPIA？根據歐盟最近的見解，原無須進行 DPIA 之控管者，不會因為參與共同控管者而必須跟進。產業利用將涉及整體資料流動，若共同控管者制度能做完整安排，對於產業會有很大的幫助。

（六） 有關個資外洩的議題，以曾擔任個人資料管理代表之經驗，處理個資外洩通知之成本及壓力相當大。但也有如同銓敘部做法，並未個別通知僅發公告，現行個資法第 12 條關於外洩通知當事人之問題在於查明困難。歐盟原則是先通知主管機關，僅於對當事人權益有重大影響才例外通知當事人，我國相反，原則上無須通知主管機關。最近歐盟公布之個資外洩指引，以保險經紀公司將 A 保險經紀人的客戶名單誤寄給 B 為例，雖屬個資外洩，但因保險經紀人 B 跟公司亦有保密協定，也進行矯正措施，因此認未造成重大風險。而對於當事人有重大風險之情況,歐盟亦有留存紀錄但不需通知的選項，因通知會引起後續的成本，我國未來個資法修正時，建議在此部分參考 GDPR 規定。

二、圓矩法律事務所林律師煜騰

（一） 是否定義委託關係應考量受託者跟委託者的權利義務有無差異，依個資法第 4 條條文而言，區分意義不大，因為受託者等同於委託者，皆負擔保護個資的義務，對於消費者而言是個資保障最充分之情況。是因為我國個資法施行細則第 8 條要求「委託機關應對受託者為適當之監督」,賦予兩者不同的權利義務，才產生區分實益。但受託者跟委託者權利義務的差別，目前提綱似乎是討論對業者的影響，沒有考慮到對於個資主體的保護，此部分建議也需要納入制度設計的考量。

（二） 如果就個資法施行細則第 8 條討論，以業界實際運作經驗而言，難以想像委託者的監督義務如何落實。資訊科技相關的新創業者，很多公司一開始可能僅 1、2 名人員，其資料可能會存放於 Google、Amazon，或委託其他業者辦理資安維護。他們並非不想保障消費者個資，只是要這些業者負擔監督、管理的義務，有實際運作之困難。因此建議在分配「委託機

關」以及「受託者」的權利義務時，需考量專業分工的問題。

（三） 有關共同控管者概念，若取得當事人一次同意便可運用資料，在資料使用上有其便利性，但對消費者以及個資主體的保障似較不周全。若以消費者跟個資主體角度思考共同控管者設計，在個資侵害的問題發生後，可能有責任不易釐清的問題。因此建議在設計共同控管者的概念時，彼此間資料利用方式以及責任歸屬問題必須釐清，否則發生爭議時，對消費者或個資主體而言，會是很大的負擔。

（四） 此外從資料利用者的角度切入，共同控管者的概念，也會有問題。舉例而言：著作權案中亦常有客戶討論是否可約定共同著作，一起享有著作的權利。但在業界運作上，共同著作的操作並非保障共同著作人使用著作之權，反而限制其利用。因為只要沒事先約定清楚如何行使權利，此後的著作使用皆須彼此同意，對於利用人而言其實是一種負擔，未來應用亦不方便。若直接約定主要著作人，其他以授權方式處理，較有主、次之概念，責任釐清上相對較清楚。在分配共同控管者如何使用個人資料時，可能也可以有相對應的思考。

（五） 最後，我國無類似 GDPR 規定要求特定機構設定隱私長，因此在很多情境下，如前所述，很難期待委託者落實針對受託者的監督管理責任。若將受託者之權利義務透過法條規範明確化，也不一定需要委託人實際上執行監督。透過幫助委託人理解如何透過契約架構，與受託者間分配責任和風險，審慎履行法律所約定之責任比較務實。

三、台灣科技產業法務經理人協會余秘書長啟民

（一） 個資跟資安密不可分，我國許多資安事件係導致個資外洩的重大原因，因為公務與非公務機關常將業務委外，而委外倘

未釐清權責將會產生問題，以過去經濟部商業司、工業局的個資行政檢查經驗，資服業者常主張只是幫忙處理後臺、未處理個資，但雙方合約並未提及個資處理之權責，因此產生問題。共同控管者係範圍比較大的觀念，若納入共同控管者規範，須要求當事人間以契約方式明確約定權利義務跟風險控制等事項。

（二） 案由一委託關係的定義，若委託機關是否妥為監督受託者難以舉證，則課予監督義務是否有實益，目前有相關責任易推拖、處罰規範不清之問題。近三年所審核之個資爭議，針對各目的事業主管機關之消保之應記載、不得記載事項，曾有業者認為個資法已規定，而因此應記載部分不必詳細記載，然而應記載的部分係要保障消費者，未寫明將產生執行檢查的困難，導致消費者權益沒有獲得保障，衍生個資外洩事件。

（三） 另一問題是，後續開罰須有具體理由，逐項檢查違規事項，才能開罰。如電商業者，因無相關能力，將相關資訊系統委託工業局主管之資服業者辦理，若以共同控管者的角度來說，應將資服業者列入共同控管者，因目前受託者間關係不清，若改用共同控管概念，並且要求須有契約釐清權責，未來可依契約舉證以釐清權責、遵循義務。個資外洩事故通知當事人相當重要，目前資服業者須負擔個資外洩通知、防止詐騙之簡訊費用，至少都負擔 10 萬元以上，應釐清雙方包含通知及責任承擔等關係較為合適。

（四） 法律位階要求固然明確，但是實務操作上若要讓業者因應，須有配套措施：須有鼓勵機制、標章的制度，搭配賞罰，並有內稽、外稽之要求，例如 DPI A 即屬於內稽的部分。若無配套制度，縱使用法律位階，成效仍難以彰顯。金管會已要求上市櫃公司之公司治理列入查核項目，但是國內多半是中

小企業，並未在該範圍。

四、輔仁大學法律學系翁副教授清坤

（一） 本次三個議題在 GDPR 架構下定義相對清楚，相關角色為控管者、受託處理者、共同控管者，其契約等事項皆在 GDPR 中有規定。此外，美國有制定消費者隱私法的三個州，其法律亦有控管者與受託處理者的定義，即使美國抗拒歐盟體系，在此部分也採納類似歐盟的規範，可見此部分之立法分類較具技術性。另美國《統一個人資料保護法》(Uniform Personal Data Protection Act, UPDPA)亦有控管者與受託處理者之界定。

（二） 歐盟跟美國之間早期有安全港條款（safe harbour），美國商務部跟歐盟簽訂之安全港條款協議（safe harbour agreement），其中前向傳輸（onward transfer）即係歐洲企業消費者的資料傳輸到美國，美國接收者要確保保護水準與歐盟相同，須確保有同等之保護才可以做國際傳輸。於控管者傳輸至受託處理者，亦在落實類似概念，受託處理個資相關業務，應確保個資保護程度立於控管者相當之立場。

（三） 例如人力銀行求職者資料外洩，企業宣稱係委外資料處理而不負責，以消費者的立場而言，信任資料會受保護，才給予資料，企業或公務機關蒐集資料，不可因超出能力範圍就不負責，公務機關亦同，過去許多國賠案件係因管理措施不當，而後國賠法第 4 條修正，受委託幫公務機關處理事情，公務機關亦要負擔國賠責任。

（四） 委託關係放到民法體系，若人力銀行之企業規模有限，無法進行大規模的資訊處理，而進行委外，大企業委外給小規模資訊公司，或者小企業委託給大規模資訊公司，將有契約談

判力之問題。且此部分委外係屬民法上僱用、委任或承攬等關係，可能是由契約規範或法院決定。

（五） 我國民法第 224 條規定債務人、使用人、代理人的行為等同債務人，因此若受託處理者發生個資事故，則控管者依照民法第 224 條負責。而歐盟之定義有許多國家採納，表示可解決許多問題。在國際傳輸方面，歐盟提出避免洗資料（data laundry）之概念，從保護較高之國家，傳到保護比較低之國家，逐步降低保護，到最後如同洗錢手法，將本來禁止事項變成允許，而控管者跟受託處理者之規定與此有異曲同工之妙。

（六） 新加坡有相關認證制度，我國亦有發展出 TPIPAS 認證資料蒐集者之個資保護是否達到個資法要求的水準，在美國亦有類似之認證。國外討論控管者規模較小，但受託處理者規模較大之狀況，該契約談判力（bargaining power）係透過認證的方式，認證目的跟處理方式都符合個資法要求，進而判斷控管者是否已盡責任而可主張免責。

（七） 關於控管者跟受託處理者間之契約，歐盟已有很明確的規定。歐盟也針對定型化契約或標準契約提出相關解釋，較有標準可循。若資料接收業者所在之國家未取得歐盟之適足性認定，業者仍可以簽署契約之方式，保證其接收之個資按照歐盟規範保護程度。

（八） 方才余秘書長所提，消保處針對不同的交易型態與交易領域，有定型化應記載與不得記載事項，以供實務上運作，個資領域也可考慮訂定定型化契約條款，供控管者跟受託處理者依循。

五、臺淡江大學公共行政學系涂助理教授予尹

（一） GDPR 的第 4 條關於控管者之定義，係對資料處理有控制權限的主體描述，而亦有控管者同時也是受託處理者的情形，因現在高度的專業化，所以個人資料蒐集、處理或利用也相當具有高度的專業性，在此情況下控管者可能往外委託給其他第三人處理。另外，亦有可能受託處理者極度專業，在經濟利益上另有所圖，有其他管道進行更細緻的分析、利用，或者有商機可能性，故受託處理者同時也對於個資有控制的權利，而具有控管者的身分。建議針對「委託」定義時，要先釐清上述情況，進行類型化的分類。

（二） 贊成案由三將具體情況進行規範，不應僅注重控管者跟受託處理者兩者之間私法自治的問題，亦可能有法律保留的問題，是否可能要求特定的情況下，受託處理者必然是共同控管者，或者是在特定情況下控管者與受託處理者之契約須包含某些項目，或甚至不得再委託出去。

（三） 個人資料已屬於寶貴資產，若可輕易委託，則對資料主體所蒙受隱私被侵害的風險相當大，若控管者為公務機關，亦有相應決策上的危險，例如 AI 相關應用，特別是人工智慧、機器學習之部分，民間業者有強大資訊技術與設備，若公務機關將所蒐集到個人資料委託給有強大機器學習能力者進行後續分析，甚至用以輔助行政機關之決策，卻未說明其論證邏輯或見解，建議思考本質上不應委託之類型。

六、台灣雲端物聯網產業協會吳監事漢章

（一） 此議題對於產業推動相當重要，從服務業者的角度分析複雜性，雲服務是 2B 或 2C，這個雲服務是所謂的應用即服務（Software as a Service, SaaS），也就是基礎設施即服務（Infrastructure as a Service, IaaS），兩走向交叉出四個格子，

此四個格子中有一個格子無意義，因 2C 不會直接利用 IaaS。剩下之三個格子中，以 2B 直接使用 SaaS 之狀況較為複雜。舉例而言，去年上市之雲服務公司 91APP，係幫助小型商家做電商，其客戶係小商業客戶，並沒有資訊能力，所以將開店、收錢等等都委託 SaaS 的雲服務廠商，以定義而言，小型店家是控管者，而 91APP 是受託處理者，小型店家在個資法的體系中應承擔法律責任，但其未必有能力監督 91APP，對於雲服務業者而言，大部分也會將其權利義務完整列於商業條款中。

（二） 從雲服務的角度，2B 的 SaaS，因為 SaaS 本身面對到數據，因此較複雜，2B 面對 IaaS 相對單純，因為 IaaS 通常規模大，後端有很好的規範。若跟隨 GDPR 運作經驗或其他較清楚之解釋，有助釐清關係。委託關係之監督管理，以醫療為例，因醫療主管機關會規範醫院，目前困難係被要求監督責任，但無細節規定，廠商難以遵循。

（三） 再以醫療產業為例，現在醫療生技業者皆想蒐集很多資料，許多資料的來源可能來自於不同廠商，混用資料將資料價值極大化，採用共同控管者之方式相當適合。

七、 陽昇法律事務所鄧律師湘全

（一） 此次三個案由，重點圍繞在共同參與不同的形態的個資蒐集、處理或利用。關於委託部分法律適用，是依個資法第 4 條以委託作為基本形態，其實就算無此條規範，本來在蒐集處理利用就要適用個資法規定。此外，在施行細則第 7 條，依照委託機關在公務機關跟非公務機關有適用之區別。案由二共同控管的概念，因為在處理單一的委託關係不足以因應現代個資委託關係。

（二） 案由三的監督管理，在經濟部個人資料保護作業手冊中有提及委外作業的監督程序，亦有相關表格讓中小型企業可以適用。共同控管者可以參考歐盟 GDPR 的規定，但我國司法實務在法律上許多的共同參與、共同侵權行為責任、承攬再承攬，都是在討論侵害他人權益時之責任歸屬，也都可以作為參考適用的判斷標準。

（三） 案由二主要目的在於修法說明不清楚之處，具體文字建議應再思考，因為不單純係委託的關係，有很多的類型，至於類型可在施行細則再為規範，在類型化上須考量要件及效果、機構規模、遵循指引所需資源、簽訂契約等事項，也就是說，類型化後才能就各種控管、委託及受託等情形，涵括在內，法令規範部分修訂，才不致有所缺漏。

（四） 在委託關係的定義，應該著重如何規範多人參與，以及多人參與的形態在共同控管者是否被涵蓋？再討論監督的部分該如何細緻化，對修法或運作上會較為順暢。

八、 中華航空公司個資暨品質管理室標準規劃組莊組長佳勳

（一） 因為航空產業涉及全世界各地，所以航空公司須符合各國個資法要求，華航目前主要是遵循 GDPR 法遵框架的要求，符合相關規定。

（二） 委託關係的定義，以 GDPR 而言，包括控管者、受託處理者，以航空公司的角度，名詞上的定義越清楚越好，建議參考 GDPR 的規定，明定各角色應該做之工作內容。

（三） GDPR 第 26 條就共同控管者有所定義，以航空業而言，當機場欲使用航空公司蒐集之資料進行後續通關作業，則要有授權或依據，原則上於蒐集旅客個資時告知蒐集的目的，以及

告知該個資依其旅程於目的地國家使用。資料提供給機場公司，也要符合當地的法規。Heathrow 機場不只是通關，也包含免稅品販售或其他目的外的運用，除非請旅客於報到櫃台確認，否則超越原本的蒐集目的，不應提供資料給機場公司。如果參考 GDPR 第 26 條規定，共同控管者於蒐集的目的、告知的責任義務等都有符合個資法規定，可以解決此問題的話，這樣的運作我們其實也是樂見其成，但是在操作上並不容易，需要協調跟討論機制。

（四） 案由三，個資法委託關係之監督管理，華航在委外時，會在主約、附約請各委外廠商簽署，請廠商務必遵循個資法規定。有時不一定有相關專業能力對廠商進行監督，但其目的在舉證責任。我們也會定期進行查核，若有相關個資事故發生，我們也必須提供證據以利釐清責任。委託關係之監督管理，在航空業而言，目前運作方面上順利，但若我國個資法能夠更明確把 GDPR 等規定涵蓋，則可更完整。

柒、 會議結論：

一、 個資外洩通知當事人及通報主管機關部分，確實係相當重要之議題，未來修法必將納入檢討。然而針對通報主管機關部分，去年行政院建立一個平臺，要求中央目的事業主管機關透過相關安全維護辦法要求非公務機關發生個資外洩時，須通報主管機關，主管機關再通報至該平臺，讓公部門對於個資外洩的案件情況有一定進度的掌握。

二、 GDPR 對於控管者與受託處理者的架構確實值得修法時之參考，各位學者專家亦提到，我國目前施行細則要求控管者對受託處理者之監督管理責任，可能必須要把委託者跟受託者間之專業能力差距納入考量，是否維持現行監督管理的規定，

將會再進一步研議。

三、 目前規範在委託者跟受託者之間的法律關係不明確，造成法律上的責任義務不容易釐清，反而對於消費者個資的保護不利，此部分亦將進一步歸類，針對責任歸屬整理與釐清。

捌、 散會（下午 4 時 30 分）。

「個人資料保護法相關議題」第6場產學專家學者諮詢會議

會議紀錄

壹、時間：111 年 3 月 2 日（星期三）上午 9 時 30 分

貳、地點：本會寶慶辦公區 610 會議室

參、主席：高副主任委員仙桂

肆、主席致詞：（略）

伍、報告事項：（略）

陸、討論事項發言摘要（依發言順序排列）：

一、 圓矩法律事務所林律師煜騰

（一） 國際傳輸議題可以從國家角度及資料主體的角度進行討論。從國家的角度切入，涉及國家安全與經濟發展的問題。在參考比較法上所參考的對象，需要先釐清我國在國際傳輸過程扮演資料輸出國或資料輸入國？若從保有多數資料的企業所在國家判斷，較容易理解為什麼在比較法上針對國際傳輸的立場會有差異。舉例而言：美國因為有諸多全球大型的資訊科技公司，是資料輸入國；而歐盟則也可以歸類為資料輸出的國家。因此 GDPR 對於個人資料的保管及傳輸有較多限制。現實上，我國的地位應較偏向資料輸出國，在國際傳輸原則的立場選擇上，建議應參考資料主要輸出的國家，而非集中於資料輸入的國家法制。

（二） 決定立場後，再進一步判斷，如讓我國的資料輕易地大量輸出，是否會影響國家安全？此外，資訊科技的發展是大者恆大，取得越多資訊者會佔有較優勢的地位。讓國外大型科技公司持續、大規模的擁有我國資料，會不會影響我國資訊科

技產業的發展？這都是從國家的角度思考國際傳輸問題，所應考慮到的面向。

（三） 從資料主體的角度討論，國際傳輸議題的一個直接影響是「救濟」的問題，當使用者點選同意按鍵時，即知悉個資傳輸至國外。但告知風險的同意其實是虛晃一招，因為目前學界已有諸多研究證實，使用者（或消費者）其實並不會仔細詳讀內容。因此，在國際傳輸的過程發動以及傳輸後的應用，資料主體可說是一無所知。而且接收方的個資保障法制亦存在差異性，讓資料主體的個資保護陷於不確定性。

（四） 此外，討論個資保護議題時，時常預設大型公司運用資料的便利性及法遵能力。但事實上目前很多雲端的服務以中小型企業為主，可能只需要一個工程師、於美國架設一個伺服器，即能就資料進行國際傳輸；即使負責網站開發的人在國內、公司負責人實際上住在在國內，但伺服器架設在海外，雲端服務上的資料蒐集行為發生在海外，即無法適用我國個資法，亦無法透過國內的法律監管妥適確保國際傳輸過程的安全措施。若產生個資外洩或個資侵害，對於消費者的保障更是不足，而需要至國外尋求救濟管道，這對資料主體而言會是相當大的負擔。

（五） 因此，在討論國際傳輸合法要件之制度設計時，建議要注重三個層次的保障：第一，國際傳輸過程必須保障消費者的個資權利，包含：知悉權、資安保障等要求。第二，國際傳輸的過程必須可追蹤，即使個資傳輸出去後消費者仍然可以追蹤個資的後續應用情形；第三，必須有可救濟性。個資一旦傳至海外就難以掌控，因此需要建立可行的救濟制度。制度設計上未必我國人民要進行跨國提告，而是人民可以透過國內法院的司法程序要求直接或間接協助個資傳輸至海外的公

司提供協助，這些都是可以考慮的方向。

二、 台灣數位治理協會陳理事長春山

（一）現實面上可分為四點提供意見：第一，我國作為資料的輸出國，基於國際上的互動必須要提供保護，但某種程度也需保持彈性。第二，未來資料經濟或數位轉型，整個經濟的發展 50%都屬於此區塊，所以必須了解這不只是法制的選擇，同時也是產業發展的選擇。第三，我國在國家安全議題上有很大的壓力，因此必須有原則但有彈性的限制。第四，目前世界公民或數位國民的想法被壓抑，但需考慮到未來思潮反撲時，我們在法制的選擇必須要有原則、目標及價值，但也應適當保持彈性以達到多元目標。

（二）我建議研究團隊於比較法上可研究愛沙尼亞，不是單純法制的選擇或條文的描述，而是從一個 10 年長期、多元利益的戰略來看，就會更清楚，愛沙尼亞從 2000 年之後，長期戰略內容、達到的目標以及相關影響為何？建議先預想整個長期戰略思維，相信這會讓風險降低很多並保持多元的利益。

（三）如果「原則許可，例外禁止」是 1.0，而「原則禁止，例外許可」是 2.0，或許可以朝向 1.5 的方向進行思考，如果直接跳到 2.0，必須做更精緻的法制設計，以保護多元利益，而非一刀切的制度選擇。在 1.5 的想法下，應進一步設想如何保護個人資料、國家安全，如何以標準制或核准制作為保護機制等問題。如果採取標準制，則參考類似 CBPR 認證標準，較能在產業界實踐、發展及探討。

（四）除了 1.5 制度設計與配套措施外，我認為需要沙盒機制，例如今年 2 月美國發布印太經濟架構（Indo-Pacific Economic Framework, IPEF），若有沙盒機制則將有利於國際合作的戰略

發展。最後，我國數位發展部將於今年 7 月 1 日成立，相關議題的討論對於數發部非常重要，建議未來行政院協助數發部，透過類似科技會報或平臺方式納入更多意見，例如 AI Medica 或國際傳輸等議題，透過跨部會的立即互動跟溝通，才能找到比較多元的答案。

三、 台北市電腦商業同業公會黃法務長益豐

（一）國際傳輸可以分為三個議題：第一，國內企業想要便利的環境，因為市場主要在國外而非國內，以 ICT 產業而言，國外市場佔營收的 7 到 8 成；因此，未來法規若朝嚴謹方向調整，則產業會考慮相關修法是否會影響現行的經營，故產業會希望有彈性空間，而對於權利保障所帶來的限制之間該如何平衡，必須進一步思考。

（二）第二，在進行比較法分析時必須衡量各國產業環境與形態的差異，其他國家規範或措施，是否適合我國本身的產業環境與結構，以及我國在外貿體系下產業發展，相關層面的討論應一併納入分析與討論。

（三）第三，以我國產業結構來看，大型企業面對國外市場時，多數有能力處理國際傳輸個資的議題，但我國中小企業在相關個資處理議題則較難有相同的處理能力，例如要求企業取得認證或標準，實務上可能難以達成。目前有很多 Data center 的服務，透過 Data center 儲存個資，較常關切是否有提供額外的個資保護措施等問題。如果是彼此有業務往來的接收方，一般而言會透過合約規範處理相關問題。但如果未來將國際傳輸從「原則開放，例外禁止」轉成「原則禁止，例外開放」的話，中小型企業可能會沒有辦法因應。

四、 台灣科技產業法務經理人協會余秘書長啟民

（一）若制度上改為「原則禁止，例外允許」，衝擊面較大，因此提供下列三點建議：第一點，如果在例外允許的部分做滾動式的調整，請務必有定期檢視的機動性機制。於目的事業主管機關需要就「例外允許」即時因應時，可以運用簡報提到的適當保護措施。回到個資法第 21 條規定，目前採取「原則開放，例外禁止」制度，但可以考慮將現行條文移到第 2 項，而第 1 項則規定：「非公務機關非經完備安全維護措施且經目的事業主管機關認可，不得進行國際傳輸。」用這樣的方式規定「原則禁止」，並將相關安全維護措施，包括企業自我拘束條款、標準契約條款、行為守則、認證等 4 項列入條款裡面。而第 2 項規定：「非公務機關完備第 1 項安全維護措施後，中央目的事業主管機關仍得依下列情況限制之」並將現行第 21 條置入第 2 項。

（二）第二點，企業自我拘束條款必須針對企業業務需求，要求個資影響評估，以業界的實務為例，業者會要求資安廠商進行個資盤點，並且必須搭配員工教育訓練，不同的部門都要積極推動；於個資傳遞至其他部門時，必須經過法務長、資安長或個資長等層級的授權始得進行，因此並非所有資料都可以進行國際傳輸，只有當內部企業的自我拘束條款做好個資保護影響評估，目的事業主管機關才允許開放傳輸。此外，建議將「適法性評估」納入個資影響評估，這對於進行國際性傳輸的檢視，是很重要的部分。

（三）第三點，贊成陳理事長提及搭配沙盒機制，建議未來做制度調整時，推選智慧應用產業，譬如智慧醫療、智慧製造、智慧運輸等產業搭配沙盒。並非規避原則禁止、例外允許的制度，而是針對最新智慧應用上可能發生的問題，透過沙盒機制即時因應調整，俾利於整體數位資料經濟的發展。

五、 陽昇法律事務所鄧律師湘全

（一）國際傳輸涉及產業經濟與個資隱私保護的利益權衡，而此議題同時與專責機關、貿易條件限制有關。早期個資法由法務部主管，但簡報所提法務部 102 年 1 月 3 日函釋，針對自由權利限制跟裁量的部分並未敘明清楚，或法務部 107 年 8 月 21 日函釋，有關接收國際資料完善法規的條件，交由目的事業主管機關自行判斷。另外，國家通訊傳播委員會以函釋限制個資輸入中國，以及今年 1 月衛生福利部以函釋限制社會工作師事務所將個資傳送到中國，皆是依照個資法第 21 條第 3 款法令不完備而予以限制。

（二）立法院在 108 年 4 月 19 日林昶佐立法委員所提個資法第 21 條的修正案，採取「原則禁止，例外允許」，並且包含 GDPR 適足性的規範，內容包括：（1）傳輸地區經過評估具備適當的保護水平；（2）提供適當保護措施；（3）當事人書面同意；（4）履行契約或依當事人要求為締約前的必要措施；（5）基於重要公共利益或基於保護當事人重要利益所必要；（6）行使或防禦法律上的請求權所必要；（7）依法辦理登記且向公眾提供資訊。上述 7 點未必完善，但可作為修法參考資料。

（三）針對本次討論兩個案由，建議我國對國際傳輸應採取多數國家的立場：「原則禁止，例外允許」。因為國際傳輸不論在技術性層面到跨境的蒐集、處理或利用，對於當事人的保護並不足夠，因此必須參考歐盟國家的作法進行調整。而新法修正後產業發展產生的障礙及問題，應透過衡量後，以最小成本進行修正。另外，歐盟 2021 年 6 月 4 日新版的標準契約條款，亦可作為參考。

六、 中華經濟研究院經濟法制研究中心顏副主任慧欣

（一）簡報第 10 頁列出國際立法例比較，多數國家採取「原則禁止，例外開放」立法模式。重點並非採取何種制度，而是我國未來實施相關制度時，有無遵循國際義務的彈性？例如日本、韓國也保有相關彈性立法例，即便其國內制度是採取「原則禁止，例外開放」模式，但在配合國際義務時也不會有困難。此外，比較法國家多是「世界貿易組織」（World Trade Organization, WTO）電子商務聯合聲明倡議(JSI)的參與國，且日本跟美國彼此簽訂「數位貿易協定」（Digital Trade Agreement）、新加坡參加「數位經濟夥伴關係協定」（Digital Economy Partnership Agreement, DEPA），而這些數位協定通常要求參與者原則上容許開放，例外情形才可禁止或限制，因此這些國家如何落實國際義務，方是臺灣在修訂國內法制前應有所掌握之重點。

（二）接下來美國總統可能會公布印太經濟架構(IPEF)，而針對數位經濟標準化有其相關規則，我認為美國 IPEF 的準則不會採納較籠統的「跨太平洋夥伴全面進步協定」（Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP），而可能採取美日的「數位貿易協定」或「美國－墨西哥－加拿大協議」（United States–Mexico–Canada Agreement, USMCA），即不允許禁止業者為從事商業活動，可用電子方式跨境移轉資訊的做法。此外延伸的就是在地化(localization)問題，通常會禁止限定業者使用當地計算設施，以作為其可在境內執行業務的條件，只有金融服務業有些例外空間。

（三）法規應與鼓勵機制並行，而非法律制訂後才要求企業配合，因為企業行動絕對比政府法律進展更快且彈性大，由於數位經濟是經濟發展的引擎，所以我建議政府可透過行業公會，先發展出可提供企業或產業參考的自律準則，讓企業知道國家的政策方向，且政府應提供誘因或輔導機制。

（四）參考去年 G7 會議決議顯示各國政府也認同，並不是完全讓資訊自由流通，而是強調 data free flow with trust，在相互可信任的架構下，應讓產業在任何法制下資料都能夠互用、互通性（digital interoperability），並有彈性讓不同的法制或法規之間，能夠互相銜接或互相承認的空間為宜。誠如前述先進提到的沙盒、技術上的互通性、印太經濟架構，或數位技術標準化的國際 ISO 標準，這些都是未來要處理互通性的議題。因此，重點就是要讓產業能夠有彈性，應避免設計出一套會導致任何方式都無法取得資訊以及容許跨境傳輸的國內法制。

（五）我們現階段多從促進產業的層面討論此議題，但並非所有國家都朝向鼓勵跨境資訊、降低障礙，明顯的例子是中國、俄羅斯，其對於跨境資訊的限制越來越高，並刻意採取網路監管、防範數位貿易的保護主義。因此建議我國也宜從資訊防守面進行評估，亦即我國是否要容許這種數位貿易保護主義的國家可自由取得臺灣相關資訊？我國是否要制裁這樣的國家，是否可採用類似於現在對一些國家實施出口管制的制裁方式，建議可能要納入修法防守面的策略思考。

七、 國立陽明交通大學科技法律學院陳副教授在方

（一）贊成顏副主任提到國際經貿的因素，考量到我國國家整體的發展、國際協定的參與、國際組織對於資料國際傳輸的發展方向，我國面臨的困難是，一方面希望得到歐盟 GDPR 適足性的認定，並採取比較嚴格的立場；但相對地美國所代表的是推動資料自由傳輸的立場，進而中間產生緊張的關係。因此，我國在設定個人資料保護法律時，針對國際傳輸必須思考我國希望朝向哪個方向，或希望能兩邊都能兼顧？畢竟比較法上有些國家是兩邊都有，同時有 CPTPP 與簽署數位協議，而加拿大和日本也有得到適足性的認定，若希望兩邊都能兼顧，國際經貿因

素確實是需要思考的方向，尤其是 IPEF 的發展方向，也是我們很關注的議題。至少我國必須達到 CPTPP 或美日的方向，並清楚瞭解國際傳輸的限制保護目的，且法規限制不能在不同國家之間造成歧視，這是設計國際傳輸限制時必須要注意的。

（二）不過，避免歧視是相當困難的，若我國為了取得歐盟適足性認定，對於國際傳輸採取「原則禁止，例外開放」的立場，則在國家認定上會耗費相當大的時間與成本，若遇國際間主張歧視時，恐怕就不太容易處理，必須先思考到相關制度設計的時間與行政成本。相反地，我國現行「原則允許，例外禁止」方式，主管機關對於認定禁止傳輸之國家的壓力也非常大。

（三）第二點，國際傳輸立場的分類恐怕不能單純以原則與例外一概區分，很重要還是「結果」，多數國家都會規定一定條件，但是條件嚴格或寬鬆的程度不一。假設我國採取「原則禁止，例外開放」模式，但在管制上的程度必須進一步分析，在寬鬆情形下取得某些認證即可，而認證也有要求寬嚴的差異存在。因此，管制上的差異，對於國際經貿或廠商負擔也會有所不同，建議立場分類再進一步細分。

（四）第三點，國際傳輸的限制對於個資保護或資料安全目的並不同，若要確保人民的個人資料，不論被傳輸到哪裡，都能夠得到一定救濟的可能性，而國際傳輸的限制確實可以達到此目的。但如果是要確保資料安全的目的，則國際傳輸的限制未必有效，因為若要求所有資料都必須留在國內，從資安技術的保護上，可能反而會造成安全性維護的困難，因此國際傳輸的限制必須回歸目的探討。

（五）第四點，關於限制國際傳輸，對於產業的負面影響包括需要使用國外的資料服務的情形。但也必須考慮到，如果我國採用嚴

格的規定，確實能符合歐盟的適足性認定，而且有利於特定廠商的長遠發展，相關利益應該一併納入評估項目。

（六）我國對於國際傳輸應該採取的立場，恐怕會受到國際關係的影響，而從廠商的立場，我會比較傾向於如果要限制，程度要儘量放寬，降低廠商資料傳輸限制的成本，也可以降低國家進行適足性認定的成本。

八、 國立政治大學法律學系劉副教授定基

（一）提供以下五點意見參考：第一，建議釐清國際傳輸與資料在地化之基本概念及內涵，這兩個概念應該是不相同，所以在討論國際傳輸的限制時，是否等於採取資料在地化的政策，可以再思考。

（二）第二，各個國際經貿協定的具體內涵為何？譬如資料標準化的要求，其對於個人資料保護或國際傳輸的意義為何？經初步檢視相關協定或國際經貿要求的具體內容，似乎都還沒有直接與國際傳輸限制的規定有很明顯的衝突；反觀日本、韓國或歐盟都是 WTO 及 G7 的國家，也跟美國簽訂協議，但其本身個資法也有國際傳輸限制，因此我建議先釐清國際經貿協定具體的要求內容。誠如前面先進提及，已取得適足性認定又同時是國際經貿協定成員國的國家，此類型國家的個資法規定以及安排，是很值得我們參考的地方。簡報上提到日本、韓國之個資法是否都透過認證條款，讓參與 CBPR 的國家個資可以互通，這一點可能要再確認；另外，日本和韓國取得 GDPR 適足性認定，是不是某個程度上已（承諾）放棄用 CBPR 認證的方式進行國際傳輸，這點我建議可以再確認一下。

（三）第三，國際傳輸的限制目的為何？美國跟我國在隱私保護與個人資料保護的法制上有本質上差異，美國並無憲法承認的資訊

隱私權，且美國沒有聯邦層級的一般性個人資料保護法規。因此從我國個資法的角度來講，以基本權利保護的角度作為對國際傳輸限制的理由，保護憲法承認的資訊隱私權是一個正當的理由。

（四）第四，有關業者成本的問題，企業在個資保護上本就會有一些成本，但在討論國際傳輸的議題時，政府付出的成本反而被忽略。我國現行個資法第 21 條規定，對於政府而言相對較為輕鬆，但主要問題在於某些部會認定特定國家或地區個資保護水準不足，但其他部會對於資料傳到同一個國家時並無相同的限制，造成政府之間的邏輯不一致。如果我國未來採取歐盟的模式，政府的壓力會非常大，包含適足性認定需要評估其他國家或地區個資保護的程度、準備標準契約條款、審查大型企業的契約自我拘束原則內容等，對於政府負擔的差異應該也要納入考量。

（五）最後，國際傳輸可能要區分是資料輸出至國外或從國外輸入資料的情形，尤其在輸出的部分，臺灣以中小企業、製造業為主的環境之下，資料輸出的法律變動，對相關產業的可能影響為何？這些影響能否以標準契約條款補充？是否能透過取得當事人的同意，使資料輸出的負擔降低？綜上，建議中長期的目標還是採取「原則禁止，例外開放」的規定，對人民的資訊隱私權的保障會比較足夠。

九、 中華航空公司個資暨品質管理室標準規劃組莊組長佳勳

（一） 航空公司從實務面向而言，我們不管是資料傳輸到國外，或從國外接收個資的狀況，最主要是確保雙方的個資保護水平相同。不管是國際傳輸或國內傳輸，都會要求雙方對於傳輸或接收的資訊有相關保護措施。

（二） 國際傳輸議題對於企業來說，最主要是確保個資完善管理，而實務上常見作法是簽訂契約或標準個資保護契約條款的方式。

（三） 案由二合法要件，以華航來說，我們主要遵守 GDPR 的規定，但是我國個資法原則開放的模式，其實對我們相對彈性。不管是參考日本、新加坡或歐盟的體系，政府機關會有它的考量，不過對於企業而言，建議合法要件盡可能以原則性的方式規定較妥。

柒、會議結論：

一、 非常感謝各位學者專家的意見，國際傳輸的議題非常重要，個資法在進行國際立法例比較時，似僅我國與美國是採取「原則開放，例外限制」的模式，與其他國家採取模式並不同，而這個議題對產業界影響很大。

二、 雖然各位提供的建議不盡相同，惟均建議必須考慮我國產業發展的模式，找出對我國產業發展、國家安全及國際社會參與的最大利益公約數，修改我國個資法並保有法律上的彈性，不要變成產業發展的阻礙。

三、 本會目前尚於諮詢階段，待後續研擬草案將會舉辦公聽會，將再聽取各界的想法跟意見，非常感謝各位學者專家提供本會非常高度思考的觀點，這個議題非常的複雜、艱難，本會跟委辦單位都會一起努力，謝謝大家參與今天的會議。

捌、散會（上午 11 時 30 分）。

「個人資料保護法相關議題」第7場產學專家學者諮詢會議

會議紀錄

壹、時間：111 年 4 月 6 日（星期三）下午 2 時 30 分

貳、地點：本會寶慶辦公區 610 會議室

參、主席：高副主任委員仙桂

肆、主席致詞：（略）

伍、報告事項：（略）

陸、討論事項發言摘要（依發言順序排列）：

一、　銘傳大學公共事務與行政管理學系張助理教授志偉

（一）　關於案由一，德國現行個資法第 2 條明確區分公務、非公務機關，在合法性要件上分別以原則、例外處理，分為兩章節，並於第 6 條規定公務、非公務機關得主張或不得主張之事由，已突顯公務、非公務機關在合法性要件的差異。另外，GDPR 第 6 條第 1 項第 2 分句、第 37 條、第 27 條、第 83 條、第 51 條亦可看出差異。由於公務機關係由聯邦個人資料保護暨個人資訊自由委員會之監察官管轄監督，非公務機關則是由各邦管轄。另外在特種個人資料處理上，德國個資法第 22 條分別於第 1 款規定公務與非公務機關處理特種個人資料，第 2 款則為針對公務機關處理特種個人資料之規定；第 23、24 條針對公務、非公務機關目的外利用的容許性亦寬嚴不同。倘若我國個資法對於公私部門採取不區分章節模式，在條文設計上公私部門差異仍應納入考量。

（二）　案由二，參考 GDPR 第 4 條第 2 款規定已列出處理行為的不同型態，建議我國個資法在合法性要件、目的外利用的部分，

應針對條文進行不同安排，於合法性要件無須精細區分蒐集、處理跟利用，建議參考德國個資法就處理行為、目的外處理之立法設計。

（三） 案由三，目的相容性規範之強度將決定如何因應目的拘束原則的要求，若嚴謹操作目的拘束原則，相容性審查較為簡易。德國個資法對於目的相容性設計不同層次，要求是否需要當事人同意或其他特殊規定，才會進入目的相容性審查，亦與 GDPR 第 6 條第 4 項首先確認是否經當事人同意，再確認成員國有無特殊規定之方式相同。由於德國個資法第 23、24 條分別規定公務機關與非公務機關之目的外利用條款，最後回歸第 6 條第 4 項判斷相容性審查；若要作為我國之立法參考，應先釐清德國個資法以及 GDPR 規範內容彼此適用的關聯性，整體搭配觀察較為全面。

（四） GDPR 規範需透過各國內國法化，無法直接透過 GDPR 規定判斷各成員國的個資使用情形，仍須確認各成員國個資法才能完整適用，特別是目的外處理之概念。所謂蒐集、處理、利用乃我國個資法用語，在歐盟僅有「處理」概念而無利用階段，我國所謂目的外利用，於 GDPR 第 6 條第 4 項係指目的外處理或目的變更時的合法性要件，該規定具體化在德國個資法第 23、24 條，分別就公務機關及非公務機關作不同之規定。

二、 國立陽明交通大學科技法律學院陳教授銘堯

（一） 有關跨部門資料共享為相當重要的討論議題，包括 Big Data 或 AI 涉及大量跨公私部門資料傳輸問題，若對公私部門採取不同的立法模式，對於資料跨部門分享可能產生巨大障礙，需要重複檢視各機構資料來源、跨部門以何種方式轉化資料

等等，可能造成資料共享運作上很大的困擾，更是數位經濟最核心的議題。因此，打破公私部門框架為歐盟 GDPR 重要目標，促進資料在歐盟各國自由流通。從資料流通角度思考，所有機構應遵從相同原則，對於資料主體而言，不會認為在公部門或私部門的資料受到不同程度保護。

（二） 案由二，同意將處理與利用整合，目前於學界之討論，「處理」為相對性的概念，例如資料仲介（data broker）之商業模式係蒐集資料加以整理並授權他人檢索，對於此類業者而言，重點在於資料編輯，而資料處理本身依其商業模式，就是利用，在此情況下，處理之行為定義已相對化，例如許多資料仲介之處理、利用，可指各種的行為態樣，在未來或許可以讓法規架構模式更為簡單，意即認處理為一種利用方式。

（三） 案由三，關於「特定目的」建議在既有法律規定透過解釋即可，至於何謂目的內外利用，可透過相容性檢驗作為區別，使文字闡述更清楚。

三、 萬國法律事務所謝律師祥揚

（一） 關於區分公務及非公務機關，贊成陳教授前述建議，基於保障數位人權觀點，無論任何處理者，理論上當事人期待其個資受到相當程度的法律保障。公務機關因執行法定職務或依法使用個資，於相關法律已有所規定，因此公務機關及非公務機關區分之必要性可再斟酌。跨部門利用個資在實務上經常發生，例如學術單位與醫院相關研究單位，究竟如何界定行使職權？此情形造成公私機構之間解釋困難，應思考是否仍有區分必要。

（二） 然而，目前我國係公私二元區分體系，若「個資法」在此前提下進行大幅調整，需要具備法制調整的強大決心；其次，

既有國家司法實務或法律規範，涉及本次會議提綱中所提出的私經濟行為時，區分公私二元論所衍生既有法律或司法實務見解應如何調整；若適用相同規範應評估公私二元制度之影響及處理（例如公務機關救濟程序為訴願、行政訴訟；非公務機關則有後續民事訴訟），整體制度面皆須考慮才能更完整個資法架構。

（三） 案由二，現行實務操作不易向當事人說明處理跟利用的區別，參考相關立法例後可適當整併，尤其一般業者並不僅為蒐集目的而蒐集個資，一般均有處理或利用需求，故區別處理或利用的實益為何，應再多加斟酌。而風險性質從資訊流動的概念而言，若蒐集是資訊的節點，處理、利用假設都由同一人持有，或仍在同一範圍內，於風險變化小之情形，是否仍有區別必要性？實務常見蒐集後直接轉包其他業者進行資料處理分析並由第三人持有，其風險變動較大，從資訊流動與風險評估角度，針對行為另行規範，更有利實務運作。

（四） 關於目的解釋方式，無論是透過歐盟的相容性檢驗，或簡報第 24 頁所提函釋引用合理關聯性之概念，就實務業者之立場，需要明確的答案。蒐集目的與利用目的類似又不太類似時，須以司法案例或行政函釋以佐證規範可期待性、可理解性，以及如何操作，若司法院或主管機關已熟悉相關操作則較易透過法院判決或實務案件發展理論或分析基礎，作為我國個資法修法參考。

四、 世新大學法律學院戴副教授豪君

（一） 案由一，公務及非公務機關是否區別，過去曾有考慮是否引進控管者跟處理者的概念；其次，應考量其他相關法律草案，包括數位發展部之「資料治理法」，若更改分類後，「資料

治理法」是否同步調整？此次修法移除公務與非公務機關的區隔之時機是否合適？建議可訂立特別規定，例如 GDPR 對於特種資料或 DPO 之指定，即針對公務機關特別規定。

（二） 案由二，蒐集的概念比較明確，處理、利用在實務上不易區別，誠如陳教授所述，新興技術之處理、利用較難區隔。我國可採用與歐盟立法例較接近的處理方式，把蒐集、處理跟利用整合，至於用詞部分可再討論。

（三） 案由三，歐盟針對特定目的外利用有三種處理方法，第一種如同我國之「當事人同意」；第二種為目的相容性檢驗，需與原始目的相容；第三種則是正當利益條款，例如銀行的信用貸款跟帳戶利率隨著信用調整，第二年雖然當事人未再申請信貸，但是依照過去一年來的銀行紀錄，銀行將重新評估第二年是否提供較優惠的貸款額度、利率，此案例符合目的性相容的原則；又例如，歐盟正當利益的指導原則指出，若銀行客戶未主動的提出貸款申請，但是銀行預先就銀行資料分析，主動行銷提供貸款額度跟利率，不能主張正當利益。前者已申辦貸款，僅評估第二年利率，為目的相容原則；後者是申請帳戶，未主動申請貸款，而銀行自行評估貸款額度，不能主張正當利益。

（四） 目的相容性原則可在特定目的嚴格規範下提供其他路徑，但若要同時引進正當利益條款必須明確區別二者：正當利益是處理之合法要件；目的性相容則是在判斷是否得為特定目的外利用。

五、 台灣科技產業法務經理人協會余秘書長啟民

（一） 「電腦處理個人資料保護法」已區別公務機關及非公務機關，若要改變規範分類，應一併解釋，甚至進行法規影響評估，

例如「數位資料治理法」及「資通安全管理法」。若修法之效益大於負面衝擊，則應考慮立法技術問題，轉換過程中各法律相應部分將產生許多衝突，例如國家通訊傳播委員會（NCC）在推動數位匯流相關法律時，「電信法」、「廣播電視法」、「有線廣播電視法」、「衛星廣播電視法」亦有變動，NCC 曾考慮在數位匯流相關法案通過到執行階段會進行行政法規的調整，作為橋接。

（二） 又例如電子簽章法之立法目的係為電子商務，因實施電子化政府而納入公務、非公務機關之共同規範，又公務機關可公告排除適用事項，造成很多私法行為之電子商務無法推動，然而「電子簽章法」至今未再修法。以美國為例，其採取技術中立並未特別強調技術，但對公務機關則有特別要求，認為公務機關之安全度較高，可運用較複雜技術。

（三） 案由二，贊成前面幾位學者專家建議，尤其處理與利用界線趨於模糊，難以分辨，例如自動化運用的情況。

（四） 案由三，若要以相容性解釋，例如「合理關聯」之判斷依據，建議參考個資法施行細則第 12 條第 2 項安全維護措施的標準，以及比例原則。例如一人公司即使實施安全維護措施，仍無法適用網路公司標準，此時比例原則就相當重要，因此更建議將相容性解釋作成指引（guideline），類似個資法施行細則 12 條第 2 項。

六、 東海大學法律學院范姜教授真嫩

（一） 日本近年修法目的係為使資訊自由流通、更易合理利用，促進形成數位化社會，不僅發布「數位化社會基本法」，也成立「數位技術部」。日本將個資法之三法合一，公務機關（行政機關、獨立行政法人、地方自治機關）制定於第五章，但

仍有不同要件。日本特別對學術研究機構規範（包括公務機關與公務機關的學術研究機構、公務機關與非公務機關的學術研究機構），其以學術研究為目的時，資料流通不受特定目的的限制，可作目的外的利用，惟該資料利用對當事人權利或利益有損害之虞則禁止為之。而匿名化後得為目的外利用，因其以當事人同意為原則，一旦匿名化就不受當事人同意的要件拘束，但對匿名化資料之提供須有完整制度。

（二） 我國是否適合參考日本之立法模式，應考量我國政策方向為何。我國個資法第 15 條所謂經當事人同意或對當事人權益無侵害之規定過於寬泛，在資力不對等情況下，歐盟、日本論者多認為不符合當事人同意之要件，因當事人是否在自由意思下的同意被高度質疑。一般而言，非公務機關蒐集個人資料多是基於契約關係以當事人同意為原則，例外規定只有三款。日本現推行實現數位化社會或者智慧城市，民眾個資保護仍是其重視之議題，然並未影響到日本成為 IT 大國的目標。

（三） 案由二，若依我國目前個資法第 2 條規定，網際網路平臺對資料的蒐集、處理、利用，無法明確區分。蒐集、處理、利用，建議可用「處理」一詞取代，實務上少有只進行蒐集的情形，即使直接交付他人也常屬於利用階段。日本也是使用「處理」一詞，對於個人資料處理業者以「保有」一詞另外規範安全維護之義務。其「利用」分成兩個部分，一個是目的外的利用，另一個是提供第三人利用。以我國實際案件為例，網路拍賣平臺消費者向消費者文教基金會申訴，消基會行文給該網站認為其違反公平交易法，而公平交易委員會通知平臺有人申訴，將申訴人地址和電話號碼一起提供，屬於蒐集、處理還是利用？因涉及行政處罰條文不同，然本案確

實難以分辨，因此建議統一為「處理」。

（四） 案由三，以日本個資法為例，若與原目的有合理關聯性，就不屬於目的外利用。所謂合理關聯性有兩個條件：其一，一般社會通念認為有合理關聯性；其二，且為當事人可得預見之範圍。若兩條件皆符合，即認為非特定目的外利用，跟原特定目的有合理關聯性。日本對於特定目的無明文規定，應依照民法觀點，未違背公共秩序、善良風俗即可。若蒐集目的雖合法，但該利用資料行為會引起或助長不法行為者，則禁止該目的之蒐集。例如：在法院公告欄上公告破產者個資或有罪判決個資，被蒐集製作成破產者地圖以供一般人查詢，日本認為此蒐集行為會引發不法利用，且會助長偏見或歧視，故以命令要求下架該網站。

七、 東吳大學法學院萬助理教授幼筠

（一） 歐盟很強調 DPO 責任並由其進行決策，例如公務機關或非公務機關等分類疑慮，在歐盟可直接諮詢 DPO。現在數位形態很多委託他人蒐集、處理或利用個資的情形，被公務機關委託之非公務機關，依個資法第 4 條規定，視同委託機關，但本身也需符合非公務機關的角色，造成很多執行上的困擾。

（二） 因此，將公務機關、非公務機關進行整合，並非以公務、非公務機關分類其權利義務，而是以該機關之能力或權利義務來討論公務、非公務機關的責任，非公務機關則應確認其目的事業機關。現今數位時代大型數位處理者（FB、Google、Amazon 等)並無明確目的事業主管機關，所受監理程度很低，卻是處理資料的大宗。以 Google 而言，是電信、電商、金融等，若進行區分，會有多個公務機關監管，又包含很多跨境資料處理的問題。建議規範主體不必細分，但權利義務要有

所分別，其他法規如「資通安全管理法」、「電信管理法」等皆須配合調整。

（三） GDPR 重視隱私影響評估（Privacy Impact Assessment, PIA），以蒐集、處理、利用劃分個資生命週期，係因三階段風險不一樣。其中處理的風險相對較低，處理係利用的一種特殊形式，若有 PIA，可由 DPO 約束該資料再利用之狀態。建議我國應搭配 DPO 設置，否則未來獨立監理機關需要作出許多函釋處理爭議。歐盟自從 WP29 工作小組轉為個人資料保護委員會後，直接與 DPO 溝通，無須透過大量函釋處理爭議。

（四） 案由二，近期歐盟修訂「人工智慧法案」，關於人工智慧之道德、倫理審查，應符合歐盟人權規範，而審查的目的、方法跟技術，與當初蒐集個人資料的特定目的不相同，故歐盟個人資料保護委員會與歐盟人工智慧委員會互相交流相容性審查方法，為歐盟數位單一市場或數位國家保留彈性空間。歐盟所採取方式值得我國參考，並配合 DPO 協助推動，以確保行政程序不再複雜，避免造成法遵上的困難窒礙。

八、 國立政治大學法學院劉副教授定基

（一） 案由一，建議先檢視公務機關及非公務機關在規範上有哪些地方需要有差別，例如：資料運用合法要件、是否強制設置 DPO 等，再判斷是否需要分章、體例上是否方便閱讀，或是否會破壞法律體系。至於是否仍需定義規定，以及公務或非公務機關認定等問題。只要在特定事項二者仍有區分實益，問題必然存在。現行個資法針對公務機關規定於第 15 條至第 18 條，第 15、16 條為合法要件，第 17 條可刪除，第 18 條專人專責規定，移至安全維護事項統一規定或許更清楚，個人認為似乎沒有再將公務機關、非公務機關分章規定的必要，

重點在於個別的規定上，哪些部分公務機關須特別規定。

（二） 案由二，考量實務上資訊運用的情況（尤其人工智慧），蒐集、處理、利用難以完整區分，因此現行法區分三階段的模式建議簡化處理，名稱為運用或處理皆可。至於研究團隊提到其他國家將對第三人的利用單獨列出，其特色似乎僅強調提供給第三人風險較高，所以合法要件更嚴格，不知道除此之外，是否有其他原因？如果僅因風險較高，建議並無必要單獨列出，因仍有其他安全維護的要求，較贊成蒐集、處理、利用簡化成單一的態樣，類似 GDPR 的 Processing 即可。

九、 淡江大學公共行政學系涂助理教授予尹

（一） 第一、二案由係立法技術問題，若就規範主體的規範模式討論，其實各國各自有不同規範的方式，應思考為何區分。以實證法檢視規範主體是否要區分公務機關及非公務機關的問題，可比較個資法第 15、19 條（公務機關、非公務機關之個資蒐集、處理），以及個資法第 16、20 條（公務機關、非公務機關對於個資之利用）。第 16 條與第 20 條的規範內容非常接近，第 15 條跟第 19 條的規範雖有差別，仍能加以整合。整體而言，在實證法層次上並非無加以整合的空間，在立法論上討論如何規範主體訂定的模式，若將個資法視為普通法，先討論區分差別是否有一定程度的影響性，再區分何時公務機關於何環節有特別加以規範之必要，再討論是否設置專章、甚至專法。同一筆個資，若由公務機關蒐集或處理，最後由非公務機關利用，例如 eID 規範的模式是由公務機關蒐集，並且建立 eID 有關的資料系統，非公務機關可能大規模利用，是否訂立非公務機關利用模式的合法性或豁免要件等規範。

（二） 案由二，行為區分可比較個資法第 15、16 條，以及第 19、20

條，特別是後者僅在 19 條第 3 款有差異，19 條第 3 款的也可以被其他條文解釋所涵蓋（當事人權利無侵害），區分的意義有限。以個人資料自主或自決的角度，無論蒐集、處理或利用，對於個人來說都有一定的程度、規模的個資侵害，若個資法作為普通法，無特別區分必要，但若為特別法層次，以專章或專條的層次討論，各情境就必須加以思考。例如釋字 603 號解釋末段提及，若要建立大型資料庫而蒐集個資，必須要明定蒐集的目的，以及目的外利用的方式等，即有必要以特別法的方式規定。同理，於 AI 或演算法為個人資料的處理跟利用之情形，處理、利用幾乎相同，故於 AI 或演算法、人工智慧蒐集、處理、利用個資之情形，亦可能要以特別專章或專法規範。

（三） 案由三，特定目的之解釋係如何區分目的外與目的內的議題，研究團隊的簡報資料屬於其中一個方向，另外亦有許多的模式可參採，包括歐盟 GDPR 第 5 條第 1 項第 B 目，若為達成公益、科學、歷史、統計的目的，所為的進階處理（further processing），不應視為不符合原始目的，建議我國可參此模式劃分目的內、外。任何規範模式在解釋上仍會產生爭議，必須累積相當的個案，才能得到更明確清晰的標準，但也不能完全期待由司法機關或法院累積案例，行政機關也必須要有一定的能量作出相關的指引，目前個資法欠缺專責獨立機關，會使個案累積標準的一致性難以掌握。

十、 理律法律事務所曾律師更瑩

（一） 贊成劉老師的意見，關於案由一討論公務機關及非公務機關的條文是否合併，應倒過來先確認哪部分須有差異，例如第 15 條是否搭配第 19 條、第 16 條是否搭配第 20 條應表達清楚。又例如第 15 條第 3 款公務機關蒐集之合法事由是對當事人權益無侵害；第 19 條第 1 項第 8 款非公務機關蒐集之合法事由

也有對當事人權益無侵害之規定。實務上，公務機關較敢主張對當事人權利無侵害，因為公務機關的特定目的有公益性質，但是非公務機關卻較不敢主張此事由。

（二） 案由二，實務上有些情境確實有處理跟利用難以區分的狀況，例如客戶會主張內部使用屬於處理而非利用，但部分函釋認為內部處理也可能構成利用；反之亦同。例如去識別化屬於處理還是利用？加上演算法、AI 更易混淆。事實上處理跟利用，在個資法第 19 條、第 20 條有很大的區別，於其他規範區別則較小。例如：第 8 條告知利用地區，卻未規範告知處理地區，最近許多中央目的事業主管機關訂定或修正安全維護辦法，要求業者於國際傳輸時要告知處理地區，與母法不一致。建議先評估在我國個資法蒐集、利用的合法事由是否一起考量較有意義，因為第 7 條第 1 項和第 2 項，蒐集的同意跟目的外利用的同意，其要件完全不同。

（三） 案由三，同樣應先確認第 19、20 條是否合併，再進一步列出合法事由，以及是否引進歐盟相容性判斷。歐盟相容性的分析非常完整，但不易操作。技術上，歐盟的合法事由較無緊急概念，但我國第 20 條有為免除當事人的生命、身體、自由或財產上危險之規定，參考立法說明是類似緊急避難，例如從路倒的路人口袋拿出健保卡交給醫院，屬合法事由，以避免身體、生命遭到危險。而目的外利用之規範，若僅採歐盟的相容性判斷則無法應付緊急事由，因此整個體系皆需確認後才能討論是否引進歐盟相容性判斷。

柒、會議結論：

一、 非常感謝各位專家學者，本次三個討論議題範圍很廣，此為第一輪的討論，彙整大家意見後，第二輪將再次諮詢專家學

者的意見，相信會提出更好的方法論。

二、 關於案由二，整併蒐集、處理、利用之概念，較無太大異議，但若要整併為一個行為，仍要注意個資法以外之相關法令可能受到的影響。

三、 關於案由三，若現行法令或函釋有關目的外利用規定，可進行更完整、合理之論述，使其更明確，則修法未必為唯一路徑。

捌、散會（下午 4 時 40 分）。

「個人資料保護法相關議題」第8場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 5 月 20 日（星期五）上午 9 時 30 分

貳、 地點：本會寶慶辦公區 610 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、Open Data 聯盟彭會長啟明

（一） Global Data Barometer 為國外的一種評比方式，在 Data Governance 方面評比各國資料運用情況，而 Global Data Barometer 中之 Data Governance 有項目為「可攜權、被遺忘權」，我們那時請教之法律學者認為我國無相關權利，故 Data Governance 分數評為全球第 20 名，參考本次會議資料，我國部分判決有類似觀念，顯示目前我國屬於灰色地帶，以資料之完整性而言，建議將可攜權、被遺忘權等權利明確訂定。

（二） 近期因應疫情所建立之社交距離 APP 應屬於被遺忘權的議題，雖其為開源軟體（open source），但處理過程中並沒有法令可完全支撐。若要執行 GDPR 的被遺忘權，應有相關程序，例如經第三者驗證、資料定期檢核，若我國有 GDPR 辦公室，則應符合該監管原則。雖有論者稱其為開源軟體，未留存任何資料，可是若當事人確診上傳資料進行距離比對，該 14 天仍會存有藍芽距離資料，須有單位澈底執行當事人的被遺忘權，故有訂定相關法令之需要。

（三） 因資料可攜權目前尚不明確，在推動開放銀行（Open Banking）上亦受影響。若將資料可攜權明確化，有助於帶動產業，若個資法修正速度有限，建議亦可先透過政策推行。

（四） 目前實務上，無論 open data 或大數據使用的方式，立法皆仍需一段時間，其中溝通過程相當重要，建議可舉相關案例促進民眾理解，避免相關權利實際應用之落差，以利民眾分辨資料可攜權或被遺忘權之概念。

二、台灣科技產業法務經理人協會余秘書長啟民

（一） 增修法律涉及之任何權利，均須考慮民眾的接受度，建議透過漸進方式，令民眾逐漸有感，例如以電信門號可攜之實際運作，結合資料可攜權的概念，或自動化決策要件等，在應用面上慢慢被民眾接受，也有利於彭會長所提之資料共享觀念。

（二） 澳洲即係以漸進方式，自電信、能源等面向推進，保障個人權利行使與公共利益，此模式可供我國參考。建議我國得以特定產業為漸進式推動，例如電信、金融產業。

（三） 被遺忘權一直有爭議，英文所稱刪除權為 delete，被遺忘權則為 erase，而 right to erasure 的情境為後台資料皆清除，delete 的情境則為電子化部分仍保有副本。後台建立欄位的資料，係由系統自動輸入欄位，因此實踐 erase 所需技術面很重要。例如學校推廣部的學員一旦登記後將成為潛在校友群，曾有學員要求行使個資法上的刪除權，但該系統設計中有部分欄位無法消除，學校電算中心後續僅能重新檢討推廣部招生要求填寫之欄位，以完全貫徹被遺忘權。又例如刪除各類型 APP 的會員資料，部分系統後台資料將儲存於手機，當事人重新下載 APP 時，該會員資料會重新連結，如何使

系統不自動帶入原有欄位資訊是技術上要考慮的問題。

（四） 被遺忘權常見議題之一，即搜尋引擎本身屬蒐集或是處理？例如中國大陸之法院判決認為搜尋引擎非蒐集資料，而僅蒐集連結(link)，故要求搜尋引擎將連結點去除。另建議我國若增訂被遺忘權，亦應考慮公益事由，否則當事人目前自我救濟之唯一方式，僅能以改名作為唯一途徑。

三、台灣雲端物聯網產業協會吳副主任委員漢章

（一） 贊成將資料可攜權納入我國個資法，並建議依循歐盟 GDPR 之相關規定。因為本協會大部分成員為國內製造業，許多業務已涵蓋歐盟部分的規範，故歐盟 GDPR 規範對產業界不陌生，而且已陸續導入相關規範。

（二） 有關資料可攜權是否針對特別應用領域限制，因為資料可攜對產業界相當重要，產業的立場希望不特別限制。舉例而言，醫療產業的部分，衛福部推行新一代國際醫療資料交換標準（Fast Healthcare Interoperability Resources, FHIR），此標準從監管機關推行，若我國個資法能納入可攜權作為搭配，整體環境將相當完整，我國科技界與醫療界就可將資料輸出至類似體系之國家。

（三） 經濟部目前推動中小微企業雲端運用 SaaS（Software as a Service），鼓勵我國許多資服產業朝此領域發展，建議透過法規引導企業採取正確的做法，提升我國之競爭力，並使國內使用者（local user）受到法規保障。

（四） 目前電子病歷交換為 B2B 模式（business-to-business），係由醫生取得當事人同意後，由醫生操作；而目前國發會推動的 MyData 為 B2C（Business to Customer），較符合現行政

策，健康醫療若非敏感資料，無論係本身醫療行為、遠距醫療、甚至保險，其實較容易找到使用案例。

四、 國立陽明交通大學科技法律學院陳教授銘雄

（一） 若要促進大數據與 AI 發展，可攜權是必要的。可攜權最初係民眾尋求某種數位服務，給予其一種轉換數位服務的可能性，但可攜權有更積極的意義，可將資料移轉後，轉為其他大數據，將使 AI 和大數據的應用更為便利，亦能促進產業發展。而可攜範圍主要爭議點在於，資料控管者從當事人所蒐集的資料透過演算系統所得之衍生資料，是否為可攜權範圍，則有疑慮，因可能涉及營業秘密或其他權利歸屬爭議，故建議可攜範圍限於從當事人所獲得之資料。

（二） 關於被遺忘權，其與刪除權兩者有所差異。資料控管者對於資料存有正當理由時，始得保存資料，若不再有正當理由，則當事人擁有刪除權；而被遺忘權係即使正當理由存在，但若當事人有更值得保護的利益，兩種利益平衡後，當事人可行使被遺忘權。我國個資法第 19 條第 1 項第 7 款概念較接近此利益衡量概念。歐盟 *Google Spain v AEPD and Costeja* 被遺忘權案中，Google 擁有正當利益，但該利益為商業利益，而新聞媒體刊登報導的人係屬受新聞自由之保護範圍，因此該案中原始新聞報導並未被遺忘，但 Google Link 係基於商業利益，故可被遺忘，這是兩種不同利益平衡的結果。此類利益衡量判斷，涉及我國對被遺忘權要採取列舉的規定，或是原則可被遺忘、例外可不被遺忘等，兩種不同立法模式應進行評估。

（三） 建議應思考民眾希望擁有被遺忘權之原因，依我國個資法，保存理由不存在之資料應予刪除，惟觀察各國發展，反而應

特別考慮例外狀況，第一種態樣，控管者原先保留的理由消失，但欲進行二次利用，例如學術研究、基於公衛或其他公共利益之利用。第二種態樣，控管者仍有利益，但當事人有更值得保護的利益。建議可針對不同樣態列出一般性條款，或先採取列舉方式，例如前科資料，屬個資法第 6 條的特種資料，然而在司法院的法學資料檢索系統以人名檢索相關資料，皆會持續顯示，此部分為我國需要正視的議題。

（四） 可攜權最重要的部分，為其應以通常可判讀格式儲存，惟我國個資法目前並無此要件，但此部分涉及資料經濟產業政策。產業界認為可蒐集的資料較以前更多，故產業界樂觀其成，特別是新創數位平台。因此，應評估民眾要求提供資料時，對產業發展的影響。此外，區塊鏈與可攜權、被遺忘權之間的關聯性，亦是一個議題。

（五） 可攜權對資料控管者賦予一定義務，但需要行政機關建構其他具體規則才能落實，因此可考慮立法模式上採取由中央主管機關根據產業個別制定，此立法模式如「食品安全衛生法」，其規定某些類型的業者必須要有自主檢驗室；又例如「藥害救濟法」規定藥害救濟的範圍是否包含醫療器材，可由行政機關視實際情況而定，給予行政機關裁量空間。故可採取訂定可攜權一般條款之立法模式，要求控管者採通用格式並賦予一定之提供義務，再由各機關制訂具體之規定，使中央主管機關有法源依據推動政策。

五、銘傳大學公共事務與行政管理學系張助理教授志偉

（一） 可攜權之立法係為競爭法之目的，其核心意涵為減少被鎖定於特定社群軟體、影音串流、網路信件或保險等服務，當事人可對於控管者主張將其個資以可用方式、數據可讀方式交

付予當事人，並應可移轉至其他控管者。德國學者強調資料可攜權本身不是資料保護的權利，而較偏向政策、競爭法甚至網路規範，與個人資料保護的原始意涵不同，因此在GDPR 施行前，其他國家個人資料相關法規並無此權利。

（二） 因歐盟有數位市場管制的企圖心，資料可攜權屬於新興權利，但多數人不會向法院主張資料可攜權，或因多數單位會直接提供資料，故實務上司法爭訟較少。贊成我國訂定可攜權，以宣示對網路、影音串流平台、社群媒體規範的立場，建議應結合「數位市場法」或「數位服務法」較為完整，而非僅在個資法脈絡下討論。

（三） 有關可攜權之限制，歐盟 GDPR 和德國法皆有相關條款。歐盟 GDPR 第 12 條第 5 項第 b 款所稱，明顯無理由或造成控管者過度負擔，亦屬限制事由，此部分未訂於 GDPR 第 20 條，而係規範於 GDPR 第 12 條，可提供立法參考。

（四） 被遺忘權係屬於兩項權利之結合，歐盟 GDPR 第 17 條第 1 項為純粹刪除權，第 2 項才屬於類似歐盟法院 2014 年提出之被遺忘權。當資料已公開後，當事人有權依 GDPR 第 17 條第 1 項向控管者要求刪除個人資料，而控管者遇有第 1 項的情況下，有義務進一步告知其他控管者當事人欲行使被遺忘權。贊成於我國個資法之刪除權增加被遺忘權之要件，考量被遺忘權會涉及到言論自由、公共資料庫檔案建立的公益性等，故被遺忘權非絕對權利，必須透過個案利益衡量。

（五） 歐盟 GDPR 第 20 條可攜權的內涵包括請求將個資以機器可讀之形式交付給另一控管者，此部分為我國個資法所無之權利。入法意涵係賦予控管者該法律義務，並參考 GDPR 規範係無償提供，若未造成過大耗費，其有義務整備，將機器可

讀之資料交付他人。GDPR 第 20 條另一要件，係基於當事人同意或契約，而且資料處理必須自動化。

（六） 搜尋引擎業者不負責審查資料內容的正確性，內容正確性係基於個資法上的更正權，此部分僅為更正錯誤資訊的部分，而被遺忘權亦不包括此面向。不建議將被遺忘權或刪除權限定在特定領域，歐盟法或德國法是開放權利內容，並例示部分具重要的價值應衡量之情形，同時內國法可另外補充。德國聯邦憲法法院在 2019 年曾兩次處理被遺忘權案例，一次有理由、一次無理由，可參考具體個案操作及相關因素，例如時間久遠、復歸社會需求等要件，此部分建議應納入規範。另外，可攜權是否於特定哪些領域先進行，應僅牽涉該領域之可讀性設計而已，整體產業之共通要件應無太大差別。

六、淡江大學公共行政學系涂助理教授予尹

（一） 我國現行個資法尚無資料可攜權之概念，因就個資法第 3 條觀之，資料沒有移動性，與可攜性較相關的是請求製給複製本、請求查詢、閱覽等權利，都較單向，尚無得請求將資料自不同控管者中移轉之權利。

（二） 若未來要規範資料可攜的概念，在具體情形上會有個案差異，不同業務領域(例如電信、金融等)會有不同之資料可攜規範，其傳送通用格式亦相對重要。而個資法作為一般性法律，尚難針對細節規範，可能須回歸個別法律體系規範，並由相同業務的業者透過協商，建立資料移轉的方式，現行制度上可參考電信號碼可攜服務。

（三） 可攜權於具體操作係經當事人請求，將個資從 A 業者透過通用格式移轉至 B 業者，但實際應用上會由 B 業者以當事人代理人的身分，向原本資料控管之 A 業者請求資料移轉，

此情形應如何擔保其代理係經過當事人同意，且因不同業務有不同的個案細節，可能更適合在相關特別法律進行規範，若於個資法規範，則應為一般性之資料可攜。法律若限制資料可攜時，應描述基於何種事由得限制資料可攜權利之行使。

（四） 被遺忘權的部分，歐盟 GDPR 第 17 條條文為 Right to erase（Right to be forgotten），但我國個資法之刪除權為第 11 條，特別是該條第 3 項規定，而其但書條文「但因執行職務或業務所必須或經當事人書面同意者，不在此限。」之問題在於，何謂「因執行職務或業務所必須」，若主管機關認為個資為執行業務所必須，就可拒絕刪除，則刪除權之限制繁多，必須特定目的消失、期限屆滿，還須資料控管者判斷執行業務無必須。因此目前我國的刪除權受到高度限縮，且我國的刪除權不等於被遺忘權。

（五） 2014 年 *Google Spain v AEPD and Costeja* 的判決，主要有兩個意義：1.特定目的消失，可能要參照時間因素，原目的隨著時間經過可能不存在；2.請求刪除的資料控管者屬於大規模以個資處理或利用為業，如新聞媒體或搜尋引擎業者的情況，Right to erase 擴展為 Right to be forgotten 才有現實的意義。建議先思考我國個資法第 11 條第 3 項應如何修正，並先專注於刪除權的討論，才有進一步與歐盟被遺忘權接軌之可能。

七、大恆國際法律事務所李律師荃和

（一） 針對法院實務訴訟可能遇到之問題，提供討論的方向。被遺忘權或可攜權在我國現行法尚無請求權基礎，故立法會面臨之問題，首先是要件，有關被遺忘權之要件，參考簡報第 16

頁所提臺灣高等法院 106 年判決之衡量標準，例如資訊目的、社會意義、要求刪除與公益是否有關、是否為公眾人物等，確實應考量上述因素，但大部分不應列為被遺忘權之法定要件。觀察法院相關判決，似將權利存在或權利得以主張的要件，與人民主張權利時法院應審酌何種限制條件等，決定其有無理由。

（二） 臺灣制度可能涉及執行面的障礙，搜尋引擎或社群網站媒體幾乎在國外架設，甚至為國外公司，且在我國沒有分公司，法院即使判當事人勝訴，似乎也很難執行。可攜權也有類似問題，我國刑事偵查要調閱 Line 或 Facebook 紀錄皆很困難，即使函詢國外公司，通常也遭拒絕提供，無論刑事案件或民事案件，即使該對話紀錄或通訊過程可能對案件相當關鍵，請求法院或檢察官調閱皆遭拒絕提供。再者，我國年輕族群使用中國 APP 的比例高，涉及對岸或國防問題，執行面將會更複雜。

（三） 刪除權或被遺忘權，兩者有差異，原則上得連結個人特徵或辨識之資訊，多數為正確的資訊，例如身分證或病歷，或是相關新聞，亦有可能於搜尋時附帶搜尋出錯誤、不相關資訊誤導，存有刑事誹謗或不實的問題，但無對象性可言，因 Google 僅提供搜尋結果而非施行誹謗，不在個人資訊刪除範圍。例如搜尋律師跳出關鍵字懲戒，但其從未被懲戒過等，建議被遺忘權亦應討論是否處理此問題。

（四） 被遺忘權係憲法上權利，而立法如何落實，無法以隱私權概念推導，因資訊可攜並非憲法上權利，與隱私亦無直接關聯性，資訊是否可攜，與資料如何利用之概念不同，部分國家將其歸類為競爭法，應思考保護的法益為何、是否需要以法律保護？權利之承認有其必要，然而因涉及資訊傳輸、保存、

格式等問題，若太寬泛承認權利，但其配套或後續執行面有所不足，反而傷害權利本身。故若要承認資訊可攜，應進行準則性的立法，在個資或主要的基本法做準則性規範，而細部規範須考慮各產業領域的特殊性，在個別法規(例如：醫療法規定之病歷)具體規定。

柒、 會議結論：

一、 有關可攜權，我國現行法似未有類似規範，此權利對於將來發展 AIoT，如電信、銀行等相當重要。澳洲係規範於消費者保護法，類似 MyData 的概念，若將來於我國個資法規定，許多專家建議使用原則性規範，至於適用不同領域者，建議以專法方式處理，又可攜權涉及實務操作面的成本課題，尚有資料傳輸、格式通用性等較複雜議題待進一步處理，本會議已建立初步共識方向。

二、 有關被遺忘權部分，是否要先釐清刪除權再處理被遺忘權，也涉及技術操作面，是否僅能刪除表面資料，或完整使資料被遺忘等實際操作課題，因涉及成本極大，將納入個資法後續修法討論。

三、 本次會議為第一輪的諮詢，非常感謝資策會對議題的深入研析，後續蒐集意見後，結案報告將進行綜整，提供將來法規調適之方向，未來仍須經過數輪的討論與諮詢，讓條文更具體與細緻化。

捌、 散會（上午 11 時 30 分）。

「個人資料保護法相關議題」第9場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 6 月 20 日（星期一）下午 2 時 30 分

貳、 地點：本會寶慶辦公區 610 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、東海大學法律學院范姜教授真媺

（一） 有關「近用權之權利限制」，建議修改為「近用權之行使要件」，以避免誤解為係對基本權之限制。有關個資法第 10 條規定適用包含公務機關及非公務機關，惟參考日本個資法目前雖已三法合一，仍對於公務機關與非公務機關區分不同章節加以規範。另若當事人請求自己的個人資料，我國現行個資法第 10 條與政府資訊公開法第 18 條第 1 項有明顯落差，反觀日本個資法對於公務機關的部分，將政府資訊公開法之整合問題亦納入考量，對於請求提供個人資料之排除理由，幾乎與政府資訊公開法規定相同。

（二） 另有關我國現行個資法第 10 條之例外規定，規範過於籠統，例如兒童的個人資料，可能由法定代理人請求提供，惟當法定代理人與兒童利益相反時(例如家暴事件)，應如何處理？個資法是否對於法定代理人請求兒童個人資料之情形，將有利於兒童權益之要件納入考量，以因應受虐兒或家暴事件之特殊性？又如日本在非公務機關規定當對於本人生命、身體、

健康、生活、財產有損害之虞者，則不得提供，此情形是否包括我國第 10 條但書規定？另有關公共秩序維護、警察權行使、司法訴訟相關業務等，均規定在日本的政府資訊公開法得不公開之事由，我國是否有相應規定？至有關限制近用權行使方式或頻率，因涉及基本權之限制，建議應更加慎重考慮。

（三） 有關更正權之限制，個案上曾發生當事人認為處分書理由中關於其個人資料有誤，要求行政機關更正處分書的理由，此涉及行政機關對於個案事實的裁量權以及當事人對於他人之評價是否可要求更正之問題。參考日本有關更正權規定，倘係為達成利用該個人資料目的之必要範圍內且屬「事實錯誤」之情形，始得更正，此規定同時可避免評鑑制度或人事評議制度被破壞。

（四） 有關刪除/停止蒐集處理利用權之限制，涉及個資法第 19 條舉證責任問題，以歐盟被遺忘權的舉證責任為例，歐盟及日本的看法不同，換言之，對於可否請求刪除有兩種舉證責任，其一係請求人須證明資料不刪除將對個人權益有重大影響，其二係控管者拒絕則應證明不刪除所維護的公共利益相較個人權益更為優先。對此本人認為若由被請求的控管者負舉證責任，對於當事人應較有保障。

二、國立陽明交通大學科技法律學院陳教授銘雄

（一） 有關近用權之權利限制，我國個資法第 10 條對於公共秩序或司法訴訟有無適用餘地，仍有評估空間。因為第 10 條提及妨礙公務機關執行法定職務，或有妨礙非公務機關的重大利益，若涉及非公務機關的營業秘密、司法訴訟等問題，又或第三人重大利益包括司法訴訟或未成年人資料，這些情況

在我國應仍有適用餘地。

（二） 近用權實際上所面臨之爭議問題有以下幾點：其一、當個資同時含有他人個資時，如近期新北兒童猝死案請求公開錄音檔之爭議，則應如何評估近用個資之原則或例外事由？此亦涉及舉證責任及有無第三方審查之問題。其二、關於限制近用權行使方式與頻率確有涉及成本問題，例如病人通常都需要繳費，才能取得病歷，又如多數國家規定免費查詢亦僅限一次。其三、近用權於共享個資情形之適用餘地？例如當機構將所擁有資料與其他機構共享時，當事人得否要求原先蒐集機關告知有關共享的情況？或於可能涉及營業秘密之情形下，當事人可要求之範圍為何？等均須納入考量。

（三） 有關更正權之權利限制，除非其他國家有特殊理由，否則目前我國似乎並無特別需要與國際規範有所不同。

（四） 有關刪除/停止處理利用權之權利限制，在大數據時代如何取得個別當事人積極同意有所困難，多數國家予以限制的情形大概都會與資料共享或大數據利用有關連性。

（五） 從科技發展來看，去識別化資料與未去識別化資料在法律地位上應有所區隔，否則機構將缺乏意願加密儲存資料，更不利於資安。以美國 HIPAA 中 Limited Data Set 去識別化已接近完全去連結的程度，此時加上其他條件，如簽訂契約並禁止再連結等，即可未經當事人同意作為學術研究利用。

（六） 另以「聯邦學習」機器學習技術為例，以該技術運用資料時，資料沒有離開機構，亦無資料共享(data sharing)之情形，資料運作過程中，使用者看不到資料，此涉及隱私權本質之探討：被看見之資料才會被保護，還是使用資料就要保護？此亦涉及歐陸以人格權之角度，美國則以合理隱私期待的角度，

我傾向以科技發展之角度出發，於個人資料沒有被看見之情形，應得限制當事人的選擇退出權。

三、南臺科技大學財經法律所郭助理教授戎晉

（一） 有關近用權之限制，針對有無必要明定公共秩序維護、警察權行使、司法訴訟相關業務為限制要件等議題，雖為目前國際立法例之共通作法，但重點在於我國如何劃定底線。從立法論觀察，個資法作為個資保護的基本法，限制事由宜應以一般性或通案性質事務較為合適，因此公共秩序維護可評估納入第 10 條但書；若已明確屬於特定部會或有專門對應之特別法，如警察權行使、司法訴訟相關業務宜由相關部會或特別法處理。

（二） 另關於個資法第 10 條但書之請求對象同時包括公務機關與非公務機關，參考個資法第 8 條第 2 項第 2 款，建議第 10 條但書第 2 款規定調整為「妨害公務機關執行法定職務或非公務機關履行法定義務」。而公共秩序維護在解釋上是否得納入公務機關執行法定義務，參考個資法第 16 條目的外利用有考量公共利益的概念，建議宜區別並明文規定在第 10 條但書。

（三） 針對特定資料類型或業務型態之限制，是否均適合規定於個資法？應考量個資法作為個人資料保護普通法之基礎，若特定資料存在重大保護利益，應優先評估規定於特別法為宜。如以兒童虐待資料概念作為近用限制事由，衛福部於 2019 年針對兒童權利公約發布首次國家報告，對於公約第 16 條隱私保護即列出從憲法、民法、兒少法、個資法等 15 部國內法律，將產生國內是否已有對應兒少保護立法的問題，而較適合由兒少保護立法處理。

（四） 針對有無必要限制近用權行使方式或頻率？由於個資法第8條已明確要求應告知當事人關於權利行使的方式，至於方式合理與否則由主管機關判斷，原則上應依第5條誠實信用方法為之，在私法關係上亦應符合民法第148條第2項之規定，爰無特別規定之必要。

（五） 有關更正權之權利限制，目前多數國家未有特別規定，且國內實務經驗上建議無相應修正之需要。

（六） 有關刪除/停止蒐集處理利用權之限制，對於學術研究得否限制當事人行使刪除權，因涉及憲法法庭健保資料庫案，建議待大法官立場表明後再進一步討論。而合法利益應傾向於當事人或控管者，從實務操作角度兩者差別不大，關鍵在於當事人更需保護抑或控管者更須利用之舉證責任，建議可維持目前國內作法。

（七） 關於資訊科技是否使特定資料無法或難以刪除，是否參考其他國家允許改採停止處理利用等其他措施？首先應確認對於「刪除」之具體標準為何，究屬物理上或邏輯上(例如去識別)之刪除，對此歐盟亦尚未明確表態；其次為考量特定技術造成無法滿足「刪除」標準時之因應作為，在討論上即有以去識別化、區塊鏈等技術作為可行方式，又或修法將此情形列為刪除權的豁免事由。至有關刪除權等事後控制權之限制措施，目前應無其他需調整事項。

四、中央研究院法律學研究所吳副研究員全峰

（一） 有關近用權的權利限制，對於公共秩序維護、警察權行使、司法訴訟相關業務等等，假設並無違反公共利益時，基於警察權行使限制近用則有疑義。為避免造成過度限制，主要重點應放在權衡的判斷標準是否公開，而且必須要有適當的準

則可以供參考，而非直接透過類型化作為限制要件。

（二） 關於是否限制近用權行使之方式或頻率，涉及成本或行政程序所產生之耗費。依據醫療法申請病歷，並未對申請的次數或期間有限制，美國亦僅有限制免費近用之次數。然對於合理時間間隔的限制，可能會造成權利的過度限制，在處理上必須更加注意。

（三） 有關更正權，不單純是資料正確性之要求，歐盟法院在討論過程中亦有認為更正權可能影響後續權利的行使。因此在訂定更正權之限制，建議不應單純以資料正確與否作為唯一的判斷依據，必須進一步考慮若為限制，是否造成後續權利之侵害。

（四） 有關刪除權之限制，GDPR 規定在科學或歷史研究目的下得對刪除權為某種程度的限縮，但仍需為利益衡量之判斷。GDPR 第 89 條第 1 項要求應符合資料最小化原則處理，同時優先使用匿名化方式處理資料。因此在限制上，是否有利益衡量之規定，衡量限制拒絕權可能產生之影響，為歐盟相對我國有較細緻的規定。另有關「當事人更需要保護」才可以停止利用或「控管者更需要利用」才可以不停止利用等兩種做法，不論採取何者，重點均在於利益衡量之標準。至有關資料難以或無法刪除的情形，假設立於資訊自主權之角度，必須以停止處理利用方式代替刪除，則應在蒐集當初向當事人明確告知，使當事人得預期行使刪除權之方式；建議亦可參考歐盟「暫時性限制」之規定於釐清相關利益衡量前，控管者暫時不能利用該資料，以暫時保障當事人權益。

五、萬國法律事務所謝律師祥揚

（一） 首先，權利限制與侵權行為之排除侵害請求權，在實現或面

臨的障礙是否相同？如請求刪除權時，係依據刪除權本身或其他權利遭侵害時所得行使之排除侵害請求權，如名譽權被侵害或被遺忘權等人性尊嚴的層次，建議先釐清。

（二） 其次，權利本身性質為何？近用權、更正權、刪除或停止處理利用權均含有主客觀性質，於設計權利與限制時，應考量非公務機關如何履行其義務。第一種情形為當事人行使權利並被實現；第二種情形為違反相關規定時，主管機關依個資法處以行政裁罰或命改善；第三種情形為當事人請求被拒絕，向法院尋求救濟，此時法院於個案審理時可能需判斷非公務機關有無實現義務的期待可能性。以更正權為例，請求更正學歷、性別或涉及第三人部分時，非公務機關如何確認正確性並實現權利。

（三） 近用權及更正權之部分，實務上觀察當事人之所以行使近用權或更正權，是否係為實行其法律之其他權利，因此在考慮權利與消極事由時，建議也要考量是否有其他權利得行使更正權或近用權。

（四） 另個資法作為普遍適用規範之情形，特定資料較適合透過個別法律或其他規範作為行為準則。如擬於個資法將權利行使之限制事由於各種類型個資的適用情形均一併納入考量，會有掛一漏萬的可能。

（五） 至於近用權行使之成本問題，為能確保當事人近用權得有效實現，建議應規範在請求後幾天內完成，並搭配合理的權利限制，譬如基於相同事由或已答覆之請求，應由當事人自行負擔成本。而更正權常涉及主觀判斷，有無資料正確的問題亦一併考量由何者負舉證責任。刪除權限制則除了學術研究、公共目的之外，可能還要考量言論自由與資訊權、大眾知的

權利，而「刪除的方式」在符合「消失」的合理範圍內應有其他方式可以選擇。至於限制措施有無需要其他調整事項，建議在事後由司法機關或行政機關在調查有無違反個資法時，透過比例原則操作該限制是否合乎比例。

六、消費者文教基金會黃董事長怡騰

（一） 個資法第 10 條僅列出三種行使權利的限制條件，於立法體例上有類型化不足之疑慮。例如當申請人為法定代理人時，即可能產生第 10 條第 3 款第三人利益的問題，相對於其他國家立法體例，似乎立法上有更周延之必要。

（二） 刪除與停止處理利用之類型上不同，個資法第 11 條第 3 項、第 19 條第 2 項將刪除與停止並列，第 11 條第 2 項僅有停止處理利用，顯然立法者認為刪除與停止處理利用為不同類型，但如何決定為刪除或停止處理利用並未明文規定。「刪除」與「停止處理利用」係屬不同之權利，建議應分別規範，惟個資法第 11 條第 3 項將此兩項權利並列，似有討論之空間。

（三） 刪除有時遇有難以執行、成本過高等情形，因此建議有其他替代措施並為更細緻之規範。另建議在權利保護原則上，由拒絕請求或個資利用者負舉證責任，以落實權利保護。

七、財團法人國家實驗研究院國家高速網路與計算中心張主任朝亮

（一） 以電腦技術的觀點，「去識別化」並非一個非常精準的界定，程式設計者能夠設計使程式運作時無法看到加密資料，是否屬於去識別化，仍有疑義；現在電腦加密技術越來越進步，可以讓使用者不必解碼即可處理資料，廣義上亦屬於去識別化。

（二） 有關區塊鏈資料不能被消除之議題，事實上也是技術問題，

假如最初設計區塊鏈有預見要更改資料，即可設計一套系統以利將來可做更動。另外對於儲存資料，事實上現在很多技術要物理銷毀是不可能，因為可能已被網站複製或電腦備份。因此是否應思考制定個資電子儲存方式的法律，規定使用何種方式儲存，當合乎規定的儲存方式即等於保護個資，可能為較實際的做法。

八、理律法律事務所曾律師更瑩

（一） 有關個資法第 10 條與政府資訊公開法間之衡平問題，以新聞實例為例，新北市消防局案之受害者家屬請求消防局提供通聯紀錄，新北市表示依個資法規定拒絕提供，但涉及該案接聽電話的公務員個資能否提供？依個資法第 10 條規定必須有妨害國家安全、外交、軍事整體國家重要利益，要求提供單一消防員的個資似未符合上述事由。又提供消防員個資似乎不至於妨礙公務機關執行法定職務，或妨礙機關、第三人之重大利益。但若依政府資訊公開法第 18 條，規定當公開或提供有侵害個人隱私時，政府得限制公開或不予提供，因此仍然有權利衡平之判斷。

（二） 於私人公司之客服電話與消費者發生爭執，消費者向公司索取電話紀錄時，則尚難依個資法第 10 條、個資法施行細則第 18 條不予提供，因為員工個資似乎並未達到重大利益，則公司得否未經員工同意提供個資給消費者存有疑義。因此於上述案例，非公務機關宜有更多近用權的限制條件。

（三） 關於更正權之限制，實務上處理較少見，但有時候企業蒐集資料，企業給予員工考績或客戶評價等，是否亦屬於更正權之範圍？建議修法時應納入考量。

（四） 有關簡報第 17 頁針對特定蒐集處理利用合法要件之刪除/停

止蒐集處理利用權之權利限制比較表，我國「權利行使要件」以個資法第 19 條非公務機關蒐集之資料取自一般可得來源，且當事人有更值得保護之利益，與歐盟、英國、德國之「權利限制要件」以控管者對資料有「具說服力的正當利益」或司法訴訟、司法請求有關，此兩項對應比較，似有未妥，因所對應歐盟、英國、德國之規定涉及公權力行使，以及我國第 19 條所無之「正當利益」，兩者相較之下似不對稱，建議以第 19 條合法要件逐一比對其權利限制要件，較為合適。

（五） 關於刪除權之限制，當個資無法刪除時應如何處理？個資法施行細則制定時，科技界曾提及有些資料無法刪除，法務部認為切斷連結點，達到使任何人均無法查找之目的即可。因此建議可朝此方向為「刪除」之定義，使科技與人權保護取得平衡點。

九、台灣數位健康產業發展協會楊理事大德

（一） 關於近用權之限制，因目前個資法第 10 條但書所列舉之項目過於空泛，故有必要於該條但書增加條件限制。個資法雖為基本法，多數條文僅作原則性規範，但當規範太過抽象時，實務上恐難以操作，故建議如上。

（二） 關於是否規定特定個資之近用權限制，如僅規定兒虐資料是否會發生掛一漏萬之情形，個人不認為必然如此，因此建議仍有例示規定之必要，因為目前各相關法令規範並未十分縝密，如透過基本法產生例示的效果，舉出幾個重要的法域有哪些情形應排除近用權，並補充「如有其他法律特別規定者，從其規定」，當可解決實務上規範密度不足，以及前述掛一漏萬的疑慮。又近用權行使方式與頻率是否宜予限制，參照個資法第 14 條「公務機關或非公務機關得酌收必要成本費

用」規定之意旨，也是反映使用者付費的立場，因此，為避免近用權造成公務機關或非公務機關負擔過高成本，宜合理限制以避免資源濫用。

（三） 關於更正權之限制，與會者普遍共識為個資擁有者應有權基於維持資料正確性，而得要求公務機關或非公務機關更正錯誤個資，但問題可能在於如何認定個資的正確性。曾有新聞報導歐盟案例一位戶籍資料年齡 70 歲男子，主張其生理年齡僅為 50 歲，故訴請法院命行政機關更正其年齡資料。因此資料的正確性如存有判斷空間，而非全然可由當事人主觀自行認定時，宜考慮個資更正執行的可能性，以及由誰判斷資料正確性之問題，例如是否可由中立客觀第三者加以判斷、在判斷正確與否前，是否可先給予當事人相關保障措施等，宜一併納入考量。

（四） 關於刪除/停止處理利用，第一點有關科學研究之限制建議參考歐盟方式，透過廣泛性框架管理，由第三方監督較為妥適。第二點關於舉證責任，個資法第 19 條針對非公務機關取自一般可得來源的情況，要求當事人負有較高舉證責任以證明資料有受保護的價值，始得限制非公務機關利用，此衡平性之考量，是否宜參考歐盟法（由資料持有者負舉證責任）調整，應視歐盟法之規範與背景、立法理由再做比較，不宜貿然比照辦理。第三點關於技術上無法刪除，可能包括技術可行但耗費過高，等同客觀上不可行，因此需考慮法律上有無期待可能性。最後關於刪除權的事後控制，建議得訂定暫時狀態假處分的機制作為緩衝，避免對資料控管者與當事人造成執行困難。

柒、 會議結論：

一、 各位專家學者均認為現行法對於當事人近用權之限制似過於簡略，爰應更細緻化規範。而公務機關與非公務機關是否須作區別，涉及實務運用、科技演進、產業與個資保護及資料運用之間衡平的課題，因亦涉及其他場次之討論議題，本會將綜整各個議題，納入各界意見。

二、 需要思考如何於資料保護與資料運用之間取得衡平，目前全球分為歐盟 GDPR 與美國 CBPR 兩個體系，美國希望資料跨境流通運用，考量不同的思考重點與範疇，臺灣需要選擇適合自己國家發展的個資法，作為將來法規之調適。

三、 感謝今日各位專家學者與會，提供本會非常寶貴之意見與建議。

捌、 散會（下午 4 時 55 分）。

「個人資料保護法相關議題」第10場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 7 月 25 日（星期一）上午 9 時 30 分

貳、 地點： 本會寶慶辦公區 B136 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、國立陽明交通大學科技法律學院陳教授銘雄

（一） 有關豁免情形，從各國立法模式觀察，應係與該國對法律保留程度的要求有關聯。若部分政府行為已有其他相關法律規定時，普遍會認為不需適用個資法，此涉及立法技術之問題。

（二） 其次，比較各國豁免情形時，必須考慮該國本身對於特定事項是否已訂定相應法令，如 1970 年代美國已針對政府蒐集個資的行為制定法律，日本亦針對公務機關蒐集個資訂定專門的法律，因此有豁免情形的規定。而國內因科技偵查法尚未通過，否則可能導致監視錄影的疑慮，若予以豁免即可能發生法律真空的狀態。

（三） 第三，現行豁免規定對於公開場所的豁免係特殊狀況，臺灣目前已開始針對特定領域制定法律，比方跟蹤騷擾防制法即屬針對公共場所管制的規範。接下來需思考 AI 科技的興起，即使可能在公開場所拍出模糊的照片或馬賽克處理，但透過 AI 技術進行還原後亦可能會涉及隱私。又無人載具多為公開場所蒐集的資料，是否亦應納入規範，為政策面應考量的

問題。國外對於豁免情形規定的前提，通常都有其他法律予以規範，因此個人對於擴大豁免的範圍持較保留的態度。

（四） 有關域外效力，同意應擴大效力至境外，而不僅限於我國公務機關或非公務機關，只要涉及我國國民的個資，則不論公務機關或非公務機關之國別，建議均應納入規範範圍。尤其臺灣與鄰近國家之密切關係，多牽涉跨國個資之蒐集，故應納入規範。

二、輔仁大學法律學系翁副教授清坤

（一） 有關豁免情形，歐盟及多數國家均無特別規定，我國似亦無規範必要。於公開活動中蒐集、處理、利用而未與其他個資結合的影音資料之規定，是否得制止一般民眾於公開遊行錄影之行為，尚存有疑問。

（二） 個資法第 51 條第 1 項第 2 款是來自美國法以當時之科技，對於公開場所並無隱私的概念，但是現在透過感應器、監視器蒐集之影像不但儲存成本低且可永久保存，又可藉由網路無遠弗屆傳播，使過去公開場所豁免適用的邏輯逐漸改變。美國雖然長期以來認為公開場所沒有隱私，但後來經判例突破這個觀念，逐漸認為車子被安裝 GPS 有形成剖析的可能性，亦構成侵犯隱私。另外大法官在釋字第 689 號解釋，認為記者之拍攝、監視應限於社會通念之合理範圍內，故肯認公開場所亦存在隱私。

（三） 承前所述，刪除本條文不代表公開場所禁止錄音錄影，而應回歸法律上的利益權衡。目前這種公共隱私概念尚在發展中，反而個資法第 51 條第 1 項第 2 款之適用造成很多阻礙，在數位時代來臨前的運作邏輯雖然行得通，但少數人可能為達成特定目的將錄影上傳，使該影像可能對當事人產生長久影

響。又現在新聞媒體對於行車紀錄器拍到的街景、人像、車牌多會馬賽克處理，所給予的保護程度反而較法規要求更高，因此其實可再斟酌本條之必要性。

（四） 其他關於政府行為、基本權之豁免，可參考國外之細部規定，但是否均需置於個資法處理可再斟酌。建議我國後續宜考慮是否進一步類型化、細緻化的規定。而監視器的問題例如臺北市政府、臺中市政府有訂定地方自治規章，因此個資法需否針對監視器作特別規範可再斟酌。

（五） 有關域外效力，我國個資法規定對於中華民國國民在境外之行為亦適用我國個資法，相較其他國家為獨有的立法，惟國外分行、分公司等機構需否同時遵守當地個資法規及我國個資法，其必要性得再斟酌。又以臉書為例，雖在台灣沒有分公司，但國內有幾百萬個使用者，需否仿照歐盟、加州 CCPA 之境外效力規範，但即使有明文規定，在執法層面上卻十分困難，如何偵測境外實體蒐集歐盟公民或居民的資料，又是否確實遵守 GDPR，在數位時代需面臨相當大的挑戰。

三、銘傳大學公共事務與行政管理學系張助理教授志偉

（一） 有關豁免情形，個資法第 51 條第 1 項第 1、2 款規定，建議比照歐盟規定，納入「專為家庭生活」之要素。現行第 51 條第 1 項第 1 款似乎仍有爭議，若在臉書設定公開權限，可能無法主張第 51 條此項事由，因此需將要件明定清楚。德國法即強調此一特定要素，以避免家庭生活、工作職場等資料混合運用，例如通訊錄夾雜個人或公司之資料，則無法援用豁免條款。另建議將第 2 款規定刪除，除考量歐盟、德國法均無此規定，公眾隱私權的概念在德國法亦承認公開場合仍有自我決定的空間。

（二） 有關部分政府行為的規定，理解上並非豁免，而是因為大部分已另有專法規定，甚至於外交事項上，德國法提及即便無專法，仍回到歐盟基本權憲章第 8 條規定。因此立法時，建議考慮我國個資法對應到哪些法律，若無其他法律能承接個資保護的功能，則建議豁免條款應謹慎制定。

（三） 關於私法行為的部分應非豁免，而應為合法性要件，依 GDPR 第 6 條規定契約或類似契約行為屬合法性要件，並非一開始即排除 GDPR 之適用。而基本權類型的部分，GDPR 第 85 條為開放條款，授權各成員國於言論自由等事項訂定個別條款，因此這部分難以設計為豁免條款的立法。

（四） 關於公開場所的影音資料，如同上述第 1 款之說明，建議刪除。依德國法第 4 條特別規定監視錄影設置，對於公司等私領域設置監視錄影器需否規範，主要以勞雇關係作為考量因素。因此，此部分是否僅規範公部門或私部門之勞雇關係，係立法政策的考量。

（五） 有關域外效力，在 GDPR 第 3 條第 2 項本身為競爭法條款，其要件主要包括提供服務與商品給歐盟境內人民，及監控歐盟人民的個資運用，始適用 GDPR 規定。惟此涉及實力問題，我國是否有能力做到如同歐盟實施強大拘束力管制境外公司，以現況來說，在執行面恐有困難，但作為宣示手段，未嘗不可。

四、南臺科技大學財經法律研究所郭助理教授戎晉

（一） 有關豁免情形之先決問題，連帶涉及整部個資法之立法論。在國際立法例包括三種豁免形式：整部法案豁免、部分章節或條文豁免，及特定適用條件豁免。目前個資法第 51 條類似 GDPR 第 2 條為整部法案豁免，GDPR 第 85 條則為不適

用特定章節之規定，惟我國許多法條有但書或免除規定，在立法論結構上類似 GDPR 的部分條文豁免情形。至於個資法第 51 條第 1 項兩款事由需否合併，建議上考量因適用對象有所區別，在適用前提上不同，故不宜合併。

（二） 其次針對個別條款需否調整，第 1 款之「自然人為單純個人或家庭活動之目的」，係參考歐盟立法所訂定，近期諸多國家如巴西、中國、泰國均有仿效納入，但巴西特別將家庭活動改為「非經濟（non-economic）目的」，因此得根據國家狀況作適度調整。關於第 2 款規定，監視器規範所要考慮者，還涉及資料開放、資料監理等面向，也會觸及政資法、通保法等規範，應通盤考量為宜。若保留此條文，建議應強化適用條件，考慮是否應限於公共利益或基於職業的需求。

（三） 針對新聞、學術、藝術、文學之目的，較常於國際立法例列入豁免條件，泰國對此加上「僅出於符合職業道德或公共利益」此一前提要件。另外在刑事犯罪或刑事偵查的部分，也擴張到司法審判的概念。而涉及勞動或職業活動的目的，今年 6 月加拿大國會於新法草案亦加上其必須為相關個資處理行為之「唯一目的」。因此各國在豁免條款的設計上，多會加上公共利益或唯一目的等前提適用的條件。

（四） 有關域外效力，是否仿效歐盟立法例，擴大域外效力之適用範圍，我在兩年前曾於政大法學評論發表文章，採取保留見解。第一個原因，是關於我國個資法之完備程度，如專責機構、資料跨境傳輸規範、問責機制、處罰規定等；第二個原因，是域外效力條款之設計，必須顧及個資保護與經濟發展的平衡，藉由立法方式強化保護規範之餘，是否將阻礙國際經貿乃至於創新科技的發展。若要採納域外效力條款，建議採歐盟模式，如泰國、巴西、中國均有大幅度仿效 GDPR。

（五） 至於在國內個資法完備程度，除了專責機構、跨境傳輸外，歐盟基於經濟吸引力，也包括歐盟本身的執法能力得透過競爭法達到實質控制。如從國際經貿、個資與產業發展之衡平角度，域外效力條款過嚴是否導致外商離開，且實際操作上執法權有無協商能力或其他認定標準，包括域外的監控、商品服務的提供等，均應納入考量。

五、中央研究院歐美研究所何副研究員之行

（一） 有關豁免情形之個資法第 51 條第 1 項，同意郭老師的看法，若認為該項為豁免條款，建議須限定範圍，並建議再更細緻化，譬如明確界定單純個人與家庭行為。一些政府行為之豁免情形，以英國對於政府監控或反恐活動為例，由於已有其他法律規範，因此排除個資法的適用。我國若針對政府行為予以豁免規定，須考慮政府行為是否有相應之法規範。

（二） 另外第 51 條第 1 項第 2 款所謂公共場所、公開活動有無合理隱私保護期待，當時立法參考美國法之立法例，未預見大數據與 AI 時代，因而單純將隱私限於私密空間。但近年美國法院提出馬賽克理論，已不再以空間場域劃分。因此建議刪除此規定，避免在大數據時代產生許多困擾。若暫時無法刪除，建議考慮制定於公共場域裝設監視器之相關規範或指引。以目前對隱私保護的期待，多以當事人有無合理期待可能性作判斷。對於監視器之規範，英國幾乎每輛公車上都有 CCTV，但在乘車時即會告知，此反映民眾對該場域可能的隱私合理期待。

（三） 有關域外效力，與前面幾位先進想法相似。GDPR 由於域外效力的關係，類似全球標準，但背後有許多政治、經濟因素的考量。因為歐盟的市場足夠大，有經濟實力在背後支持，

但我國是否效仿，取決於市場的力量，否則實益不大，反而可能帶來限制。在 GDPR 剛通過時，臺灣許多銀行即考慮關閉倫敦分行，以避免違法遭受鉅額罰鍰，因此在探討域外效力的問題時，並非僅有法律設計，也必須考量我國政治經濟的背景與競爭力。

六、台灣科技產業法務經理人協會江監事國泉

（一） 有關豁免情形，應特別考慮所豁免的政府行為，是否多增加細部定義。因為若豁免政府行為，某種程度上可能產生風險，司法行為亦同，均有可能使人民生活有被大幅監控的風險。並建議個資法第 51 條第 1 項第 1 款家庭活動目的宜作更細部定義，第 2 款公開活動蒐集、處理或利用與其他資料結合的影音資料，在定義上並不詳盡，宜刪除第 2 款。

（二） 有關域外效力，認同中研院何副研究員的意見，歐盟域外效力具有與美國經濟競爭的內涵。2010 年 Facebook、Amazon 或其他線上平台的興起，使歐盟察覺到網路無國界所產生的經濟競爭風險。我國個資法並無類似 GDPR 第 3 條第 2 項對境外實體的域外效力規範，但我國個資法是否納入該規範，須考慮是否有實力執行，否則僅留於文字的規定。因此建議視執法實力，在立法設計上予以調整。

七、國巨法律事務所蔡律師文玲

（一） 有關豁免情形，由於個資法第 51 條第 1 項第 1、2 款規範主體不同，因此不建議兩款整併。第 2 款在實務上常遇到很多公司或團體，舉辦公開活動時會留下現場拍照或攝影的活動紀錄。如無本款豁免，於實務上會有相當多困擾(例如：蒐集時必須向當事人履行告知義務)，因此實務上確實有此豁免

條款之需求。

（二） 很多 AI 科技針對大數據分析或人臉辨識，包括便利商店的螢幕會拍攝消費者臉部，或街道上行人在公開場所的活動，這類影音活動資料可能有後續利用，作為商業開發或與其他個資結合，也確實會監控到一些個人社會活動。因此如要保留本條規定，在處理 AI 技術上針對臉部資料的蒐集，這部分適用的條文應再作討論。

（三） 有關監視器議題，除了街道之外，多數裝設目的為保障居家安全，以目前個資法第 51 條第 1 項第 2 款之解釋，包括辦公室的監視器或居家環境等公共區域的監視器，依照通說對於隱私權見解係以有無合理隱私期待作為判斷標準，權衡公共利益或個人利益保護。目前像警察職權行使法有針對經常發生犯罪的地方設置監視器，如果個資法要針對監視器特別規範，建議盤點檢視目前現有法規，以避免產生適用疑義。

（四） 有關域外效力，贊同前面先進的看法，雖然國外對於境內人民服務活動或持續監控有規範的必要，但應考量後續執行之可能性。

柒、 會議結論：

一、 各位專家學者建議研究國外立法例時，因為各國可能有其他相關法律的考量，不能僅直接比對法條差異，且個資法許多條文亦需考量科技技術之發展。此外，也涉及法律、經濟、執行等層面，很多條款也涉及到國際傳輸的問題。每位專家學者從自身專業給予不同的思考觀點，從法條的規範延伸到一個國家政治、經濟的影響，而歐盟因為其市場地位作為規則的制定者，主導許多數位時代的法令。

二、 由於法條制定須考慮諸多因素與層面，若刪除個資法第 51 條第 1 項第 2 款，相關之經濟行政成本、對利害關係人之影響等，亦應一併納入考慮。本次為第一輪議題的個別討論，待所有議題討論完畢後會作橫向的綜整，進行第二輪綜合討論，納入各界相關意見思考。感謝今日各位專家學者與會，提供我們非常寶貴的意見與建議。

捌、 散會（上午 11 時 30 分）。

「個人資料保護法相關議題」第11場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 8 月 24 日（星期三）下午 2 時

貳、 地點：本會寶慶辦公區 513 會議室

參、 主席：高副主任委員仙桂

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、東海大學法律學院范姜教授真媺

（一） 111 年憲判字第 13 號判決可能是讓我國個資法制更完整之契機，至於獨立監督機制應解釋為監督機制或監督機關，基本上機制的範圍較大，可能包含歐盟、德國、英國的做法。但仍建議有設置獨立監督機關之必要，日本於 2015 年修法後設置個人資料保護委員會，在此之前同我國均採行各機關首長主管制，然而各機關首長未必對個資法有足夠專業知識，又如有無違反個資法、資料去識別化是否達到匿名化、假名化之程度等，均難以迅速判斷也影響機關執行效率。

（二） 有關獨立專責機關須為二級或三級機關，重點應在於能否獨立行使職權(預算、人事獨立等)。日本個資委員會係採合議制，因個資保護涉及多方面利益衝突，除個資當事人外，亦涉及公共利益，需透過獨立專責機關維持公平性，作衡平判斷。且為維持委員的獨立性，委員之免職應具有法定事由，亦有任期之保障。

（三） 另日本個資法近期修法納入公務機關，由於委員會等於內閣府之外的府外機關，基於三權分立，委員會對公務機關僅有勸告或建議之監督權限，並未包含進入實地檢查等調查權。關於人員編制，除了具公務員身分之人員，亦包括不具公務員身分之資安技術人員或產業從事人員等，此方式有助於推行個人資料保護與管理制度。

二、淡江大學公共行政學系涂助理教授予尹

（一） 首先，雖然 111 年憲判字第 13 號判決提及欠缺個人資料保護獨立監督機制部分有違憲之虞，但十多年前司法院大法官釋字第 603 號解釋就已提及針對指紋採集的組織及程序等相關事宜應進行檢討。而憲判字第 13 號判決再次提及獨立監督機制的必要，但解釋文及理由書均表示將此保留給主管機關相當的立法形成自由。

（二） 考量健保資料庫是衛生主管機關非常重要的政策執行工具，建議將獨立監督機制分為兩部分討論，其一係衛生或健保相關法規應強化獨立監督機制，其二係以個資法的立場，現行監督權限有關調查權及處分權之機制是否已足夠獨立。檢討上難免會涉及現行的組織型態，思考上可以分為三個層次：首先應有專責機關；其次，若專責機關獨立性不足，考量設置獨立機關；第三，獨立機關應為二級或三級？

（三） 另一個角度觀察，若仍以行政院作為行政權最終負責者，難以認為獨立性可以完全逸脫行政一體的範疇。假如二級機關之獨立性亦有疑義，則以三級機關為前提所設計的獨立機制更無法予以期待。從法制面而言，獨立性使該機關與最高行政機關保持一定的距離，若為相當中央二級的獨立機關，其委員組成須經立法院同意，則可認有較高的獨立性。

（四） 最後關於獨立機關在組織法設計的重點，其一為委員的任期保障；其二為委員的任免事由，尤其是法定免職事由的規定；其三為任期交錯制。立法者對此有相當空間，在立法形成階段針對獨立機關委員的任免，訂定相關要件與機制設計，保留相當的立法自由。

三、 中央研究院歐美研究所何副研究員之行

（一） 大法官在憲法判決中表示希望建立獨立監督機制，而該判決的客體是健保資料庫，所以多數人將此解釋為對健保資料庫本身的運作、組織程序、資料釋出，及儲存對象做出獨立監督的規劃與監理之規範。因憲判字第 13 號判決採嚴格審查標準，若解釋上將獨立監督機制解讀為應成立獨立監督機關，或許如此的立法形成更妥適。

（二） 以組織面而言，贊成應具備專責及獨立性。目前國發會為個資法的解釋機關，但之後的獨立專責機關必須扮演與政府協調的角色。因為政府其實是最大的資料控管者，而獨立專責機關必須在功能上發揮調查職權，特別是在行政指導、調查、處分的權限維持其獨立性。

（三） 以英國為例，幾年前英國的國民保健署(NHS)與 Google DeepMind 簽署資料分享協議有違反個資法之虞，資訊委員辦公室(ICO)便主動介入調查，其後提出行政指導，使該協議逐步修正。ICO 並非合議機關，但仍扮演制衡政府此一龐大資料控管者的角色，有效帶領行政部門為合法之資料治理。

（四） 通常獨立機關受理民眾的申訴後，將發動其調查權，於調查結果後做出一定程度的處分。但目前我國個資法的裁罰力道不足，即使成立獨立專責機關，亦可能無法達到嚇阻性。而

歐盟強調獨立監管機制配合高額罰鍰，因此除了機關的組織程序及功能、運作層面外，建議罰鍰的部分應一併修改。

四、國立陽明交通大學科技法律學院陳教授銘雄

（一） 憲判字第 13 號判決採取嚴格審查標準，係由於審查標的為特種個資，若為一般個資的情形可能未必相同。因此憲法判決要求衛福部應設置獨立監督機制，但不見得必須修法。然而從國家發展的角度，為因應國際潮流，確實可藉由此機會強化我國個資保護機制。

（二） 其次是憲法判決並未提及「專責」的要件，僅要求獨立監督機制，因此事實上也許可以透過結合既有機關達成。另一問題是我國之所以未設有獨立專責機關，主要考量部會有數量上限之規定，所以從既有機關尋求較適合者亦為一種方式。再者，公務機關與非公務機關可否由不同機關監管？例如監察院的國家人權委員會層級較高且獨立，可監督公務機關；非公務機關則可考慮由公平交易委員會監督，參考 GDPR 或部分國家的個資法，本質上帶有公平競爭的色彩。假使以此做組織上調整，至少可解決部會數量總額的問題，而且公平會、監察院本來就具有調查權限。

（三） 至於其他部會可否另外設置個資監管機構？以英國為例，除了 ICO 之外，在 NHS 下亦設有個資保護委員，雖然不見得具有獨立性，但其優點在於各部會對業管之個資特殊性更加瞭解，反而很難期望一個委員會掌握所有部會的個資型態。而各部會所設機關應採合議制或獨任制？此問題不妨交由各部會自行決定，若為三級機關則建議採獨任制，因為獨任制權責集中，在執行面上較有效果。

（四） 最後關於獨立機關的功能，其一為制定法規，其二為執行法

規，亦可思考此兩種功能是否必須置於同一機關。參考其他國家的經驗，法律應盡可能簡化，不需有太多標準，避免不同機關的法令互相衝突。若有獨立專責機關將可以簡化這些問題，但獨立性為一種相對性概念，如何盡可能提升其獨立性，才能對各部會所管資料進行某種程度的限制。

五、台灣科技產業法務經理人協會江監事國泉

（一） 憲判字第 13 號判決表示從個人資料保護法及相關法律規定整體觀察，欠缺個人資料保護的獨立監督機制，對個資隱私權保障不足，而有違憲之虞，但並未強調該獨立監督機制是屬「專責」。由於該判決係針對個資法第 6 條特種個資，在蒐集、使用上本來就有相當程度的門檻，而本次判決可作為設立獨立專責機關的契機。但是否所有法令包括個資法、健保法都必須作大規模的修訂？為避免耗費過多資源，建議可再進一步考慮。

（二） 另外我國個資法有規定公務、非公務機關對於個人資料的蒐集、利用之違法事由，及有相應之裁罰。承何副研究員所說，我國個資法所訂的罰鍰額度相對較低，產生之嚇阻效果亦較低。由於非公務機關的範圍十分廣泛，假如未能設置一個獨立專責機關，無論執法或裁罰方面可能有相當問題，因此認同陳教授的意見，或許可交由公平會承擔在非公務機關對個資蒐集、處理或利用的監督。

（三） 最後，關於獨立專責機關應具備哪些機制，英國、德國採獨任制，日本、韓國則採用合議制。考量獨任制同時具有執法、裁罰權限，且必須同時監管公務機關與非公務機關，在執行面上可能會有困難，因此比較傾向採取合議制的方式。又目前我國各中央目的事業主管機關在行使權限的過程中，難免

會有相衝突之處，如採獨任制可能在處理各機關之間的執法衝突上會耗費較大心力，因此採取合議制的獨立監督機關會較適合我國當前的發展。

六、輔仁大學法律學系翁副教授清坤

（一） 長期觀察全世界多數全盤適用個資法的國家，幾乎都設有獨立專責機關，譬如 GDPR 第 51 條對各會員國之要求。另外其他立法比較周延的國家如日本、韓國、加拿大、澳洲、新加坡、香港、澳門等，亦均有專責機關處理個資保護。而觀察我國個資法與其他國家個資法並無太大差異，最大不同在於沒有專責機關。由於個資法充滿許多不確定的法律概念，且個資法的相關權利可能與他人基本權益或公益產生衝突，因此如何在不同價值之間取捨，就可能需要透過專責機關解釋才能有效適用。

（二） 再者，我國個資法解釋機關從法務部到國發會，可是實際上配置的專責人員有限，執行之事務也有限，相較國外落實個資法之程度相去甚遠。因此從國際趨勢觀察，我國目前已經制定個資法，下一步就是執法程度應達到國際水準。有關處分權、調查權相關問題，大部分國家其實於個資法有詳細規範，如英國、加拿大、香港等提及當個資侵害的受害人申訴時，主管機關應如何處理，根據何種狀況發動調查或停止調查等。

（三） 至於令狀的問題，我國個資法提到主管機關得至非公務機關的實地場所進行檢查，而澳洲則要求應取得法院許可，如同我國刑事訴訟法的搜索應有法院令狀，包括指定場所、期間等。而能否對公務機關進行裁罰，譬如愛爾蘭的資料保護法第 141 條第 4 項即有規定。另外我國個資法的罰鍰相較業者

所獲取的經濟利益明顯過低，建議修法亦應提高罰鍰額度。

七、南臺科技大學財經法律所郭助理教授戎晉

（一） 關於專責機關的部分，可將目前國內遇到的問題分成兩個面向，其一是如何符合國內期待，另一是如何符合國際的看法。在憲法判決中要求一個獨立監督機關，但國際上要求專責。在 2001 年「資料保護暨隱私委員國際會議」（International Conference of Data Protection and Privacy Commissioners）針對「個人資料專責機構認定要項」（Accreditation Features of Data Protection Authorities）提出四款認定上的基本要求，包括法源依據、自主性與獨立性、符合國際通認標準、賦予適當權力，在具體認定上比較像開放式條件，但無論歐盟、國際隱私組織均有一套認定標準。

（二） 參考韓國過去訂定與電信網路相關之個資利用法規(即「情報通信網法」)，由韓國的 KCC 相當於我國國家通訊傳播委員會所主管，但後來被認為該法僅適用特定行業，所以之後又制定一體適用的個資法，因此目前韓國有兩個個資保護主管機關，其一為韓國個資保護委員會，另一為韓國的 KCC，均被國際承認為個資保護主管機關。因此其實重點應在於機關有無適當的獨立性及執法程度。

（三） 香港的隱私公署承襲歐盟本身 commissioner 的概念，但後來除了獨任的 commissioner 之外，也列了三個助理的 commissioner，因此有做一些調整與折衷。回到國內，以任期保障來說，如公平會、NCC 的委員均有任期保障概念，對於保持機關的穩定性、獨立性相對較容易。又參考各國法制，採取合議制的國家較多，如巴西、泰國、澳門等。其中泰國借鏡日本的方式，委員設有常任及非常任，得聘請社會賢達

擔任類似兼任的委員，又特別要求數位經濟與社會部常務次長擔任副主委，屬於相當特殊的設計。

（四） 關於獨立專責機關的調查權，GDPR 第 58 條第 1 項至少包括三種態樣，即違法行為之調查、通常情況下之業務檢查、特定資格准否之審查。國內類似立法如公平法、消保法，也有類似當出現違法情事時實施行政檢查的規定，但是否能對應 GDPR 第 58 條之規定，可能必須依機關的行政調查權限作評估。又機關得否委託其他機關行使權限，我國行政程序法已有類似機關之間相互委託的規定，但當專責機關成立後，除了能否委託其他機關行使權限，亦應考量其他機關可否委託專責機關協助執行稽核檢查。

（五） 最後關於處分權，得否裁罰公務機關，基於行政一體原則，在整個行政架構下可能產生左手罰右手的疑義。或許可參考韓國設立行政 ADR 機制，即「個人資料爭議調解機制」，國內亦有類似概念如金融消費者保護法下的金融消費爭議評議，使民眾得先向相關事業進行申訴，作為一種調解機制以降低專責機關之負擔。

八、理律法律事務所曾律師更瑩

（一） 在憲判字第 13 號判決的協同意見書提及，由於健保資料庫案的爭議在於衛福部作為健保的主管機關可以解釋法令，又可以使用健保資料庫，即公務機關自身同時有解釋或管理的權限，產生球員兼裁判的問題。假如由另一機關解釋個資法適用於健保資料的處理，此時方有獨立性存在。因此判決所提的獨立監督機制，未必為專責機關，而是要避免球員兼裁判的爭議發生。

（二） 假使法規制度將管理與監督的權限區分，在發生個案爭議時，

由另一機關作出類似裁決，比如五權分立下由監察院擔任，則憲法判決提到缺乏獨立監督機制的問題即有可能解決。以個案性、專案性的組織進行監督與調查，而非常態性的設置，亦可避免耗費太多時間及資源。

（三） 目前我國個資法分散由各個中央目的事業主管機關監管，而因金管會對金融機構高度監理，若將來設立個資法的獨立專責機關也有權監管金融機構時，則必須考慮各機關權限分立的問題。又倘若獨立監督機關層級不夠高，可能無法與金管會制衡，則從個資法的角度上很難發揮作用。因此獨立機關需要具一定位階、權限，否則難以期待其獨立性。最後考量國內文化，獨任制可能較易承受壓力，合議制則相對容易推行、達成目標。

柒、 會議結論：

一、 關於獨立專責機關的設立，憲法法庭於憲判字第 13 號判決表示因隨著當代科技進步，針對政府蒐集的個資在組織及程序上應有必要防護，避免不當的洩漏或濫用，譬如公共利益如何判別就可能需要獨立專責機關處理。至於獨立專責機關為二級或三級，將留待行政院考量各項利弊得失，但仍應符合本次憲法判決要求的規範，之後將依可行性再為歸納與分析。

二、 由於本次憲法法庭已表示將獨立監督機制的設計保留立法形成空間，針對此項議題，將再投入更多資源做相關規劃，因此議題除涉及個資法整體修正外，尚包括相關機關的設置，未來將持續深入探討。感謝今日各位專家學者的與會，提供非常寶貴的意見與建議。

捌、 散會（下午 4 時）。

「個人資料保護法相關議題」第12場產學專家學者諮詢會議

會議紀錄

壹、 時間：111 年 10 月 3 日（星期一）下午 2 時

貳、 地點： 本會寶慶辦公區 513 會議室

參、 主席：高副主任委員仙桂(楊參事淑玲代理)

肆、 主席致詞：（略）

伍、 報告事項：（略）

陸、 討論事項發言摘要（依發言順序排列）：

一、國立陽明交通大學科技法律學院陳教授銘雄

（一） 從制度欲達成之目標觀察，美國未訂定刑事罰係因其個資觀念與他國不同，未將個資以基本權看待。又雖各國之行政罰鍰上限之規定不同，惟行政機關裁處時在一定額度內具有裁量空間，例如歐盟 GDPR 雖訂定高額罰鍰，但個案中對於中小企業則未必處以過高的罰鍰，建議應給予行政機關有彈性的裁量空間。

（二） 贊成設置獨立專責機關後，將公務機關納入裁罰範圍，可彰顯獨立機關之意義。而關於非公務機關的代表人、管理人或其他代表權人是否裁罰，由於多數國家要求機構內應設置個資保護長，對相關人員已有一定規範，即使未規定於個資法，亦可能已規定於其他法規。

（三） 部分國家裁處行政罰原因為機構內部法遵不足，如未能證明事故發生後已建立完善機制符合法遵要求，則會連續處罰至改善為止。促使產業逐步提高個資保護標準，並非一步到位，

此種機制可使整個社會提高個資保護程度。至於刑罰的問題與行政罰存在連動關係，當行政罰的處罰力道已足夠時，則刑事罰相對可減少。除非是行政罰無法解決的問題，才需要使用刑事手段解決。

二、臺北大學法律學系曾教授淑瑜

（一） 首先，行政罰之罰鍰需否加重，應考慮裁罰基準，以及比例原則。若過去並未訂定裁罰基準，則重點在於將來如何訂定該基準。其次，行政罰法第 26 條規定同時處以行政罰及刑事罰時，以刑事罰優先，因此行政罰如何加重的意義不大。另外行政罰得未待訴願決定即執行，但刑事罰則可能耗費數年之久，緩不濟急無法達到效果。

（二） 個資法第 48 條為行政義務的違反，如履行義務則不裁罰；而第 47 條則是因已破壞法秩序所以先予處罰，為避免損害擴大與恢復法秩序，故規定仍須命改正。至於需否將公務機關納入處罰之對象，因並非僅有非公務機關才可能外洩個資，公務機關亦可能發生濫用、侵害、洩漏個資的情形，因此基於平等原則贊成應納入公務機關。

（三） 行政罰之罰鍰額度如採資本額、當地營業額等作為標準，針對營利社團法人並無問題，惟非營利性之財團法人(例如醫院)恐難以適用此標準，建議應妥善訂定相關標準。以刑事罰而言，倘以意圖營利之不法所得作為標準，在計算犯罪所得即需花費許多心力，因此建議廣泛針對不同型態之主體訂定標準，而不以資本額或營業額為限。關於針對代表人等之處

罰需否回歸行政罰法第 15 條，考量原本就已有規定，在適用上應不會有太大問題。

（四） 個資法上的刑事罰基本上為洩漏機密之態樣，刑法第 132 條訂有洩漏國防以外秘密罪、第 317 條訂有工商秘密罪且針對公務員或非公務員均有處罰，第 318 條之 1 及之 2 則針對利用電腦洩漏秘密罪有加重處罰之規定，因此個資法應係針對保護特別法益的部分規定，並以意圖得利為目的。又 105 年刑法訂定沒收新制，由於個資法的刑事罰屬於財產利益的犯罪行為，沒收不法利得可填補作為其他保護個資的來源收入。

（五） 於需否處罰過失犯，在刑法理論上主觀存有意圖，客觀上即無過失。建議針對不同犯罪態樣做出區隔，並在基本故意、過失態樣外，另附加意圖營利之加重態樣。如採取「以其他不正手段或方法取得他人處理之個人資料」作為刑事罰之客觀要件，建議應明確規定以避免產生不確定法律概念。關於刑事加重處罰部分，刑法針對 5 年內再犯者有累犯之處罰規定，因此較不建議增訂結合犯或接續犯之規定。

三、 台灣科技產業法務經理人協會余秘書長啟民

（一） 依個人參與經濟部商業司、工業局、中小企業處行政檢查之經驗，在限期改正階段多半都是查核、輔導然後命其改正，但業者改正程度有限，經濟部基於輔導立場通常最多裁罰 2 至 4 萬元。在實務上觀察 165 反詐騙專線的週期，可能前案才因個資外洩命限期改正，改正過後經過一定週期，165 專

線又接獲通報，究是否為同一根因，業者若為此主張必須負舉證責任，因此事實上限期改正在執行上存在很多困難。

（二） 近年推廣個資保護並納入資訊安全，包括隱私權政策、設立資安委員會、教育訓練，並要求執行弱點掃描、滲透測試、社交工程等。個案有時業者未採行上述措施，但在作成處分前已決定改正，主管機關可能就會難以決定是否裁罰。建議應於裁罰前，透過主管機關之積極抽測、查驗以督促業者合規。

（三） 至於公務機關須否列為裁罰對象，個人認為應一視同仁，並考量資通安全管理法多側重公務機關，從資通安全角度更應結合個資法規定，且應保留限期改正的規定。而個資法第 50 條針對非公務機關負責人、代表人的裁罰，實際上有些企業主會因此而加強重視，所以仍有一定的嚇阻效果。針對裁罰金額，是否依違反行為按次連續處罰，在實務上運用的次數並不多。

四、國際通商法律事務所余律師若凡

（一） 目前罰鍰額度對許多公司並無嚇阻作用，因此，裁罰金額確實有提高的空間，但重點是裁罰額度如何衡量。歐盟等國家有以全球營業額或訂定高額的罰鍰，倘若我國仿效歐盟的罰則，可能導致外商退出我國市場。然而罰則過輕，也可能導致大眾對法遵的不重視，建議可參考新加坡以當地營業額作為標準。

（二） 至於是否先命限期改正，同意前面先進看法，確實主管機關在過程中會遇到許多困難或成本，但針對有裁量權限的規定，

優點是雙方可以有比較多的討論空間。因此在行政罰的考量，若訂定較高額度的罰鍰且不以限期改正為先行程序時，主管機關應提供更多個資法遵的指引、辦法或解釋，使業者在事前、事後有透明的標準可自行做法遵評估。

（三） 針對刑事罰的部分，從業界來看非常具有威嚇力，即使一年以下有期徒刑也比幾千萬行政罰鍰的風險更高，考量個資法的目的應是期望業者履行法遵義務，而非讓業者不敢嘗試創新，故認為以行政罰為主可能較為妥適。另外刑事罰納入過失行為，可能會對業界造成很大的寒蟬效應，建議僅針對惡意行為處罰較為妥適。若是僅針對惡意行為處刑事罰，則可考慮不以被害人提起告訴為追訴罪責。

（四） 關於刑法的工商秘密、妨礙電腦使用、妨礙營業秘密等罪，與個資法規範並不相同，因此需思考個資法的刑事罰，如回歸刑法概念解釋，罪責是否相當以及有無配套措施。很多個資外洩情形是業者無法查明事故原因，致主管機關也難以進行裁罰。觀察其他國家，如發生大規模個資外洩，會要求業者通報主管機關，並在期限內提出報告由主管機關審核，而非直接處以行政罰或刑事罰。

五、中興大學法律學系林教授昱梅

（一） 關於行政罰的部分，無論以嚇阻作用或取締成本為考量，贊成不以命改正為先行程序。個人認為應使非公務機關投入個資保護之法遵成本，而非僅仰賴主管機關的行政指導。在數位轉型時代，建議將資訊隱私權、個人資料自主權內化為非公務機關的法遵成本。

（二） 中央、地方機關均為行政罰法第 3 條之行為人，如環保事件得裁罰行政機關，罰鍰金額甚至有依照行政罰法第 18 條第

2 項計算不法利得者。若公務機關違反個資法義務，應如同非公務機關受有裁罰，但公務機關不具營利性質，故在裁罰基準或裁處額度上應有區別。在法定裁罰金額為定額或比例的問題上，機關常以初次違規或第二次以後的違規行為作為裁量基準，較少以違規情節輕重作為判斷，建議納入個資外洩筆數、個資風險高低或業者規模大小等作為裁罰考量因素。

（三） 訂定罰鍰額度應符合比例原則，建議採固定額度且有最高額及最低額的規定模式，輔以行政罰法第 18 條第 2 項不法利得計算。應注意者為，若採營業額或資本額界定業者的規模，業者為避免受高額罰鍰，可能自行調降資本額，而營業額相關計算資料在行為人支配領域較難蒐證，若以稅務資料的所得一定比例可能較為可行。

（四） 關於個資法第 50 條規定裁罰非公務機關之代表人等，考量代表人可影響業者支出法遵成本的意願具有一定的影響力；另因行政罰法第 15 條規定與個資法第 50 條不同之處在於，行政罰法的併同處罰限於故意或重大過失，在主觀要件的門檻較高，且上限為一百萬元罰鍰，故建議保留個資法第 50 條的規定。

（五） 關於刑事罰，行政罰法第 26 條規定一行為不二罰，且採刑罰優先原則。行政罰與刑罰，目前採量的區別說，認為刑罰較重，建議依謙抑原則，運用行政罰對業者處以超過其成本之罰鍰以收預防效果。立法政策上可先考量資通安全管理法或刑法妨害電腦使用罪章等的適用，不宜在個資法擴大刑法規範，如附加告訴乃論的規定，是否會導致以刑逼民的情況，宜一併考量。又關於接續犯如何處罰，個資外洩案件不見得為蒐集、處理、利用行為的串聯，而是短期間內重複發生多次的情形，建議在立法政策上，亦可參考交通違規透過距離

或時間擬制行為次數的模式，以利實務運作。

六、淡江大學公共行政學系涂助理教授予尹

（一） 關於個資法第 47、48 條行政罰規範模式，法條本身並未規定「應」處或「得」處，第 47 條規定處 5 萬到 50 萬以下並令限期改正，該限期改正是否須以處罰鍰作為前提要件，即產生疑義。故未來修法除了思考限期改正與罰鍰的順序問題，在「應」或「得」處的問題亦須解決。再觀察個資法第 47、48 條不同的規範模式，可能是立法者為區別秩序罰與執行法。針對命限期改正，屆期未改正按次處罰之規範邏輯，效果較接近行政執行法的怠金性質。最高行政法院 105 年庭長聯席決議，提到按次處罰為秩序罰而非執行罰，建議未來可朝向此方向修法。又依司法院大法官釋字第 604 號解釋，提及以舉發次數當作違規次數為合憲，但須注意比例原則及明確性原則的問題，建議若訂定裁罰標準之法規命令應有明確授權的依據。

（二） 至於是否裁罰公務機關，早期認為可能有左手罰右手的問題。但多年以來，特別在環保法規部分多有處罰行政機關的情形，建議公務機關亦應在個資保護付出一定法遵成本。又如運用行政罰可以達到一定效果，則並不需處以刑事罰。但在特定情形如為彰顯行為的惡害，或該行為的不法程度較高時，運用刑事罰也未嘗不可。

（三） 至於美國 CPRA 無刑事罰，所有違規行為皆為民事或行政罰部分，其原因係美國法有關隱私相關權利內容保障方式，係從各州普通法的民事侵權態樣逐漸堆疊概念、範圍及侵害類型，故以民法規範 CPRA 的消費者個資保護事宜。但美國 HIPAA 關於醫療個資外洩有處以刑事罰的規定，因此本質

上仍應視立法政策決定。

七、南臺科技大學財經法律所郭助理教授戎晉

（一） 關於行政罰的思考，應視所欲達成之目的及討論基礎為何。首先，個資法之行政義務有哪些？其次，違反行政義務之行為態樣有哪些？第三，當發生違反義務的情形，主管機關為主動或被動知悉？均牽涉行政罰是否需有命改正的規定。若要求需先命改正，則應思考其與行政義務連動之關係，國內許多法規不乏有類似改正前置之要求，例如消費者保護法第56 條針對違反消費資訊的部分，規定經主管機關通知改正，逾期未改正再處罰。

（二） 此外，需否採改正前置規定，應先將個資法的行政義務類型化，檢視哪些違反行為有改善可能性。又參考泰國個資法第90 條新設的個資委員會有權處行政罰鍰，在認為適當時可先命改正後發出警告，保留主管機關行使權限的彈性。而日本之所以罰鍰最高僅有 10 萬日幣，因日本實務上以公告名稱作為解決方法，一旦主管機關進行調查或將名稱公告被新聞揭露，對於業者的商譽有很大的衝擊影響。而關於是否裁罰公務機關，日本今年 4 月公布 PPC 例行性檢查，已納入20 家公務機關。基於公務機關與非公務機關應處於平等立場，贊同處罰對象納入公務機關。

（三） 至於罰鍰的裁罰基準，如採現行固定額度做法，現行法最高罰 50 萬元明顯不足以產生嚇阻的功能。國內以銀行法最高得處 5000 萬元罰鍰，與韓國可處 4 億韓圜、泰國 500 萬泰銖，均明顯高於現行個資法的罰鍰額度，但應往上調多少是另一問題。若採歐盟全球營業額的模式，可能超過主管機關得控制的情形，在認定上恐有困難。若臺灣採取全球營收之

標準，則係以法律實體作為責任範圍限縮，或完全以全球所有營收比例換算罰鍰？參考中國、巴西以境內管轄範圍的營收為準，相對全球營收較容易認定，且建議亦可仿效歐盟在最高金額及全球營收擇其高的模式。

（四） 針對是否裁罰非公務機關之代表人，國際上中國大陸採用此一方式。行政罰除罰鍰之外，是否有納入其他行政罰之可能性，觀察其他國家有採暫停特定營業行為，例如巴西規定可命暫停與個人資料運用相關的系統操作。而我國行政罰法第2條對於其他種類行政罰明定限制、禁止行為處分、剝奪或消滅資格、影響名譽或警告性處分等，建議可作為設計行政罰之參考。

柒、 會議結論：

一、 針對本次議題，在行政罰的部分可以觀察到各國行政罰鍰額度有明顯差距，刑事罰部分有些國家並未規範，各國在刑罰的構成要件及刑度上皆有不同。而關於個資外洩的問題，目前個資法並未規定通報主管機關之義務，在去(110)年行政院成立個資保護執行聯繫會議，請各中央目的事業主管機關於其依個資法第 27 條授權訂定之安全維護辦法中訂定通報主管機關之義務，作為修法前的因應方式。此外，我國個資法除了罰則之規定外，第25條亦有禁止蒐集、處理或利用個資，與命刪除、沒入或銷毀個資，以及公布非公務機關違法情形及其姓名或名稱與負責人等相關規定。

二、 感謝今日各位專家學者的與會，提供本會非常寶貴的意見與建議，後續本會將會針對相關規定進行整體評估。

捌、 散會（下午 4 時 20 分）。

附件二、專家學者訪談相關記錄

中央研究院何之行副研究員訪談

壹、訪談資訊

一、　訪談主題：歐盟合法處理要件及假名化

二、　訪談日期：110 年 11 月 24 日（三）

三、　訪談地點：中央研究院歐美所 304 研究室

四、　訪談人：周芷瑄副研究員

五、　受訪者：何之行副研究員

貳、訪談內容

一、訪談提綱

（一）GDPR 之合法處理要件（lawfulness of processing）共分為 6 種，其中有關同意（consent）及正當利益（legitimate interest）在適用上存有疑義。近年國際論壇上已開始廣為討論同意是否不應該再被視為主流的合法處理要件。實務上控管者廣泛運用同意作為合法處理要件已造成民眾同意疲乏（consent fatigue），以及大量資訊被阻擋（content blockage），致使民眾無法取得所需資訊，並限制取得資訊之機會，且增加民眾負擔。因此今年 APEC 會議已經開始討論正當利益的可行性，試圖讓正當利益成為合法處理要件之主流。

（二）然而，許多企業認為運用正當利益要件處理資料時，判斷正當利益要件之適用性較複雜且使用正當利益要件處理資料法遵風險較高，因此英國政府在 2021 年 9 月的公眾諮詢文件

《資料：新方向》（Data: A new direction）中建議，UK GDPR 修法時應制定一份廣義的正當利益制式清單（exhaustive list），當符合本清單所列利益時，控管者即得免於進行衡平測試（balancing test）。換言之，當前 GDPR 有關正當利益之規定仍有改善討論空間，請問您對於英國政府所提出的方案有何看法？在我國《個人資料保護法》架構下，您認為我國是否該將正當利益納為合法處理之特定情形，又是否需參考英國政府所提出的方案？

二、何之行副研究員回覆

（一）目前業界大量使用同意作為合法處理要件造成同意疲乏現象，但當事人個人資料自主權（autonomy）之尊重為 GDPR 立法目的，因此雖有同意疲乏現象，同意應維持主流，因向當事人取得同意是為了達到透明度（transparency），確保資料控管者已將應揭露給當事人的事項完整、正確、全面告知當事人，使當事人清楚明白資料控管者如何處理其個人資料，避免產生資訊不對等之情形，並非增加民眾負擔。無論在 GDPR 或我國《個人資料保護法》架構下，唯有實際上真的無法取得當事人同意，如時間成本、行政成本過高，才得使用其他合法處理要件，我國還未有獨立個資監管機關前，可避免國家成為最大的資料控管者。

（二）然而，為試圖解決同意疲乏現象以及同時尊重當事人個人資料自主權，可考慮是否在我國《個人資料保護法》中將正當利益納為特定情形之一並得參考 GDPR 相關規範。GDPR 正當利益已存在於我國《個人資料保護法》第 6 條第 4 款，雖然不是將「正當利益」獨立為特定情形。《個人資料保護法》第 6 條第 4 款係公共利益條款，且涵蓋利益衡量概念，所列舉出的醫療、衛生或犯罪預防目的都是公共利益高的目的，但是我國僅含利益衡量概念，對公共利益的判斷沒有真正

要求做利益衡量。

（三）反觀，GDPR 對科學研究開設例外條款（scientific research derogation），其中 article 9(2)(j)特種個資例外條款有三要件：公共利益、適當安全維護措施、會員國立法授權。但每個歐盟會員國在施行（implement）本條款時不一致，不同會員國的監管機關對本條款有不同詮釋，產生法規適用性之落差，未達到 GDPR 為一致化歐盟個資保護法之目的。但大致上可統整為四種公共利益，各自有利益衡量的差距：

1. 非常重大公共利益（substantial or significant public interest），有時間空間急迫性，如 COVID、SARS 防疫。
2. 重要公共利益（important public interest），如健保資料庫建置（public health insurance data base）有重要價值但無時間空間之急迫性。
3. 普通公共利益（general public interest），如學術研究，但牽涉眾人之學術研究及因學者興趣而進行的學術研究公共利益層級不同。
4. 低程度或無公共利益（low or no public interest）。

（四）層級化的公共利益模式（layered public interest model）使不同層級之公共利益對應到不同層級之同意要求：COVID 防疫是非常重大公共利益，得限制沒有退出（opt out）權或不需取得當事人同意；健保資料庫是重要公共利益可以給予當事人退出的可能性；普通公共利益則需搭配退出的可能性甚或明示 opt in 同意。

（五）我國學術討論正研議是否應將公共利益類型化，在英國，公共利益是資料處理的適法基礎但必須符合利益衡量的標準，較少如同我國用公共利益涵括所有情形而無利益衡量或無其他限縮條款，目前《個人資料保護法》中除了同意以外的特定情形，其實都太廣泛，應該增加利益衡量來限縮。

（六）如正當利益要寫入《個人資料保護法》中，建議做為次於同意的特定情形（supplement），且規定不得太廣必須限縮。實際做法得參考 GDPR 正當利益規定，將正當利益要件寫入《個人資料保護法》成為特定情形的一種，以較廣義的文字敘述正當利益要件，但是因為我國無獨立個資監管機關對正當利益進行詮釋，以避免再次出現與目前公共利益相似的狀況，立法者可在《個人資料保護法施行細則》限縮，明確制定正當利益要件，其中包含利益衡量。我國可考量英國公眾諮詢文件中建議的廣義的正當利益制式清單（exhaustive list）是否可寫入《個人資料保護法施行細則》做為限縮正當利益要件的方式。

（七）英國公眾諮詢文件提出的廣義制式清單，太廣義且較不清楚，第 g 項將假名化及匿名化之個人資料列入制式清單中，然而這與 GDPR 要求相反，英國 ICO 應較難同意；第 h 條將機構內研究或是商業研發用的資料列入制式清單中，代表之後每間公司幾乎可以使用這條規範毫無阻礙處理個人資料再也不用取得當事人同意，與 GDPR 之立法精神相左。因此，我國可以參考英國的公眾諮詢流程，但英國廣義的制式清單不建議參考，反而如我國要制定一份制式清單須限縮且明確。

（八）最後，對正當利益要件之限縮，應該還需在我國《個人資料保護法》中加入 GDPR 兼容性判斷（compatability test），個人資料必須在特定目的內蒐集、處理、利用，資料二次利用必須在新舊目的兼容情形下。亦可參考 the Finnish Act on the Secondary Use of Social and Health Data (552/2019) ，芬蘭用立法的方式，即最簡便的方式，規定特定目的外二次利用資料不需再次取得當事人同意。

（九）綜上所述，如我國決定將正當利益納為個人資料蒐集、處理、利用之特定情形，公務機關與非公務機關選擇正當利益作

為特定情形必須符合《個人資料保護法》正當利益條款、《個人資料保護法施行細則》正當利益限縮條款，以及《個人資料保護法》兼容性判斷。

三、訪談提綱

（一）GDPR 將「去識別化」分為「假名化」（pseudonymisation）及「匿名化」（anonymisation），我國《個人資料保護法》有關「去識別化」之定義，依據法務部函釋及法院判決均認為係「處理至無從識別特定當事人」，即相近於 GDPR 有關匿名化之概念。觀察近年國際個人資料保護法制趨勢，發現已有愈來愈多國家將假名化之概念納入該國個人資料保護法規。

（二）然而我國《個人資料保護法》目前未明文規範假名化之概念，恐造成未來在國際交流與其他國家隱私保護法制規範銜接上產生斷層，請問您對此一問題之看法為何？

四、何之行副研究員回覆

（一）當前我國去識別化的定義較不清楚，法務部函釋之解釋應更明確。最簡單及直接的解決方式是建議直接在我國《個人資料保護法》中說明假名化資料為個人資料，加入 GDPR 假名化、匿名化的概念及架構，使公務機關或非公務機關即便採取假名化措施依然須遵守《個人資料保護法》下的個資保護要求。

（二）目前實務上，我國許多組織採取加密或是 barcode 的假名化方式，且組織認為這即是符合我國《個人資料保護法》去識別化之要求，不需要取得當事人同意即可直接蒐集、處理、利用當事人個人資料，但事實上並不符合《個人資料保護法》之要求。假名化概念放入《個人資料保護法》後，公務機關或非公務機關使用假名化個人資料時依然必須符合一種特定情形才得蒐集、處理、利用當事人個人資料，以生醫資料為例，公務機關或非公務機關必須取得當事人同意，才能合法蒐集、處理、

利用假名化後的個人資料，這種方式較符合國際認同的資料保護原則。

（三）另外，假名化資料納入《個人資料保護法》可確保跨境資料傳輸個人資料符合 GDPR 水準，對我國取得 GDPR 適足性認定甚為重要。以便於理解，常以《人體生物資料庫管理條例》中的「以非去連結方式」的概念來解釋假名化，假名化之去識別程度係非完全去連結，但如我國《個人資料保護法》要納入假名化，其定義該以哪些文字呈現，有待商榷。

臺北醫學大學全球衛生暨發展碩士學位學程蔡奉真主任訪談

壹、訪談資訊

一、　訪談主題：我國個人資料保護法未來修正建議

二、　訪談日期：111 年 1 月 20 日（四）

三、　訪談地點：臺北市大安區基隆路二段 172-1 號（臺北醫學大學大安校區）

四、　訪談人：李宗儒副法律研究員、蔡紫亘副法律研究員

五、　受訪者：蔡奉真主任

貳、　訪談內容

一、 訪談提綱

（一）我國於 2010 年，參考 1995 年歐盟資料保護指令、德國聯邦個人資料保護法第 13 條及奧地利聯邦個人資料保護法等外國立法例後，最終考量我國社會與經濟環境之特殊性，將《個人資料保護法》（以下簡稱「個資法」）第 6 條規定修正為與德國和奧地利等國不同，使個資法「特種個人資料」限於病歷、醫療、基因、性生活、健康檢查及犯罪前科等 6 種類別，並於個資法施行細則第 4 條進一步定義。然而，近年來隨著人臉識別應用、穿戴式裝置等新興科技的應用，而蒐集臉部、指掌紋、聲紋等個人資料，基於人權保障之目的與我國司法院大法官解釋第 603 號意旨，有關保護個人資料當事人之權益，想請教蔡奉真主任以下問題。

（二）我國現行個資法第 6 條之「特種個人資料」之定義與範圍，是否有進一步擴張之必要性，如納入「生物識別資料」？

（三）若須擴張，則除「生物識別資料」，哪些個人資料建議亦應納入「特種個人資料」之定義？

二、蔡奉真主任回覆

（一）因為科技的進展會遠快於法律的進程，若僅是因為科技調整法條內容，將造成每過一段時間即需調整法條內容。故以大架構來說，由於我國係屬歐陸法系國家，應思考歐陸法系在面臨科技發展需要如何做滾動式的調整。

（二）而所謂的敏感性資料係屬於文化字眼，並非完全是科學字眼。誠如方才所述，非敏感性的個人資料，也有可能識別特定個人，所以「敏感性資料為何敏感」則係有一個時空背景，特別是以現在的科技，會變成不僅可以從資料中去識別個人，甚至會識別到個人背後的相關背景，故以目前來說此部分才係須要區分的原因。

（三）若要朝資料只要可以識別到個人，就全面性的管制保護，未來是可以討論的，但就目前法令來說，識別出來的特種資料是非常生物性的，不純粹是社會生活的相關資訊，因此以現階段來說，在尚未清楚的界定敏感性的定義，及為何須區分特種個資及一般個資的情況下，則不宜貿然去調整將一般個資及特種個資一視同仁。而所謂的保護，也須了解到本土民情，例如說大眾是否意識到哪些種類的資料係個資而需要受到保護的狀況在將本土風情了解的更透徹之情況下，後續較易推動修法的進程。

（四）針對因為科技的發展造成可以到識別到個人的資料範疇擴大，若將其放入生物識別資料並非不行，後續可以透過解釋的方式，擴大生物識別資料的定義範疇，因此建議直接在特種個人資料的範圍放進生物識別資料，後續內容可以透過施行細則和函釋再擴充。現在許多法律皆會遇到科技發展會搭不上法律的問題，且台灣為高科技發展國家，故在法律訂定後，後續解釋的空間上，應可以考慮更加彈性，讓範圍可以有機會解釋得更寬廣。

（五）此處「納入」有種列舉的意涵，但依科技發展的角度，希望能朝不須更動到母法的規定，而採取例示或具有未來能夠再擴充的方法，擴大規範範疇。

二、 訪談提綱

（一）我國有關因學術研究而蒐集、處理及利用個人資料之規定，規範於個資法第 6 條第 1 項第 4 款、第 16 條第 5 款、第 19 條第 1 項第 4 款，以及第 20 條第 1 項第 5 款。有關「學術研究」之具體內涵，參照司法院釋字第 380 號解釋及其協同意見書、法務部 2015 年 7 月 2 日法律字第 10403508020 號函釋，所謂「學術研究」，係指針對有系統而較專門之學問中的特定主題，作深入且有系統的探討或研查，以發現事實，形成理論並付諸應用。惟上述說明均屬抽象之法律概念，尚難遽定其範圍及認定標準，仍宜依具體個案分別認定之。對此，以下想針對我國個資法關於「學術研究」的相關規定，進一步請教蔡奉真主任。

（二）綜觀各國法制，個資法有關研究之相關規定可分為「研究」、「科學研究」及「學術研究」之規範用語。規定「研究」（research）之國家，包含美國、新加坡及菲律賓；而歐盟、英國、德國及韓國則以「科學研究」（scientific research；wissenschaftliche Forschung；과학적 연구）作為個資法規範用語；而我國及日本則係以「學術研究」（学術研究）作為條文用語。對此想請教：我國個資法是否需調整「學術研究」之法律用語？

（三）承上，由於現今巨量資料產業蓬勃發展，有論者因此認為：我國個資法所稱「學術研究」過於限縮，而應進一步擴大至產業研究的應用，因此想請教您：我國個資法「學術研究」之法律用語，是否應擴張至產業研究的應用，或於個資法另立產業應用之機制？

（四）個資法中之「學術」或「科學研究」既屬於不確定法律概念，對此想請教：「學術」或「科學研究」的相關定義，應留於主管機關規範，或個資法有清楚定義之必要？如要定義，應否以符合特定研究方法或倫理標準之研究為限？

三、蔡奉真主任回覆

（一）以歐陸體系來看，個人針對其資料有其自主權，個人權益是最大的，無論是否關於公益，非經個人同意前，理論上是不可動的。健保資料庫的特殊性，係在進入資料庫時，針對後續的使用是否得到當事人同意，進一步產生了之前健保資料庫案的爭議，畢竟健保資料庫裡的資料，最初蒐集的目的並非為了學術。因此目前的狀況來看，學術利用在蒐集之資料時皆須通知同意，則後續在使用時可能會較無疑慮。

（二）而在生物資料庫方面，其在規範在利用上是較清楚的，且針對利益回饋之規範也是較清楚。就本題來說，針對字眼的使用，我覺得是還好，可是依資料公益使用來講，資料是否會對個人隱私造成侵害，是否會有一個資料守門員來控制，這就牽涉資料當事人的保護責任要誰負擔。所以，是否從「學術研究」改成「科學研究」，我認為是可改可不改，此不是最重要的，因為台灣人對於所謂公部門的信任度大於私部門，所以當寫成科學研究，大眾皆會連想到係從公部門連結出來的研究。故在此處，文字上並非如此重要，若改成科學研究也可，因其看起來所涵蓋的範圍較大，但並非如此急迫。

（三）資料若未識別到個人時，則不應過分的箝制。因個資法的所規範目的，是為了保障個資當事人不會被任意識別，所以當資料利用上，並不會識別到個人時，或不牽涉特定個人時，則不需要去過多的限制。可是，今天大部分的爭議會落在：銷售個人資料的層面，例如生物資料庫，若係以公益出發的角度去「出售」資料，就須有一個利益回饋的機制。但此題

並未區別資料來源是公部門還是私部門，故先以資料係從公部門或以公益模式得到來出售的角度，可以參考現在生物資料庫的相關規範。

（四）不過我想討論的另一個問題是：像今天的智慧手錶，也可以蒐集到很多生物性的資料，準確度也達到一定程度了。這個時候因為此資料的來源並非出於公益，在今天這題的討論上，好像比較沒有討論到，可是我認為此處應要更受監督。我這邊所說的需要受到監督指的是：相較於現今巨量資料庫資料來源大多是公部門，規範上係僅限於學術利用，而私部門因為可能較少受到同樣的關注，在資料的應用上會走得更前端，反而是我覺得更需要把關的地方。

（五）所以統整來看，針對產業利用資料有兩條路，一為政府來的資料被產業拿來開發利用，另一為商業自己蒐集而開發利用，台灣依目前來說較多的利用狀態係屬前者，資料庫和資料都是公部門居多。而針對後者來講，台灣的社會情況會呈現一個很矛盾的狀態，在台灣的社會大眾在意重點不一定是「我的資料不要被洩漏出去」，而更多的是「會對我造成多大困擾」。很多權利的想像是有文化背景的，若以資料源頭來講，資料擁有者如何使用資料，透過資料研發下一個產品，若其未將資料外洩造成傷害係沒有問題的，就像敏感性資料透露出來給廠商，如果可以改變病患舒適度的產品，那未嘗不是一個好的利用方向。在這樣的利用情境，我們在「當事人同意」的階段就必須把關，而不允許未經同意而濫用資料的狀況，可是在同意之後之利用，則或許不須太過去壓縮。

（六）以管制層面來講，若在前端有通知和同意的狀況下，則在後端的管制則即可以放寬，而台灣在個資的立法上，我們目前看到的是「管制鬆緊不一」的狀態，也就是說雖然法規範不斷地細緻化，但管制模式和手段並沒有跟上，這個是在修法

之外，如何訂定更細緻的執行方式，是我認為除了修法之外，特別需要去重視的一點。

（七）學術和科學並不容易區分。另有關倫理標準和管理上，IRB 的存在一定有必要，但現在要求的越來越細，因為倫理審查的範圍寬廣，連觀察性實驗現在需要經 IRB 審查。可是，有一個疑問是：若產業在利用時，沒有伸手跟公部門要資料時，是否有辦法透過 IRB 審查達到把關？此部分針對倫理審查的範圍則須再考量。

（八）其他對於我國個資法相關觀察與建議，我認為資料治理應該要更宏觀的來看，資料跨區域及跨國的傳輸已屢見不鮮，那台灣在個人資料保護法還是以自己可以掌握到的範疇為想像，此觀點可能無法與世界接軌。目前以台灣的狀況來說，僅是參考外國立法例，卻忽略了立法背後的系統，此處是跟不上科技的發展與需求，應更宏觀的來看如何跟國際接軌，即個資暴露風險的討論上，應更關注全球的趨勢發展。因為現在較大的問題，在規範的架構和模式，會造成實務上的爭議無法落入法規範的窘境。

（九）從今天的題綱來看，在科學發展所產生的問題上係較多的，但在台灣個資法的問題，不全是來自科技，亦有來自管制執行不力的問題。若在科技發展的前提下，法制如何跟上，此為制理模式的問題，各國都在看有無滾動式修正和調整的方式，使其可以更快的跟上科技發展的速度。但台灣所遇到的問題大多都是與管制執行不力相關。針對執行不力的狀況，必須強調：「零風險」這個概念，在現今科技發展的狀況下，幾乎是不可能達到的。因此如果制定的管制規範，內容要求零風險，就可能會不利科技發展。

國立臺灣大學法律學院李建良教授訪談

壹、訪談資訊

一、 訪談主題：個人資料保護法相關議題研析之被遺忘權修法與法制建議討論

二、 訪談日期：2022 年 4 月 13 日（三）

三、 訪談地點：中央研究院法律學研究所 9 樓所長室

四、 訪談人：陳咸蓁研究員、賈忻蓉副研究員

五、 受訪者：李建良教授

貳、訪談內容

一、訪談提綱

（一）綜訪談提綱所述，我國《個資法》目前針對被遺忘權並無明確規範，參考其他多數國家如歐盟、英國、德國、美國、新加坡及澳洲個資法令皆有相關規範；而日本則無此規定；另韓國自取得 GDPR 適足性認定後，已於 2021 年 9 月提出相關修正草案。

（二）依您的專業觀點，我國《個資法》未來應否增修或不增修相關權利規範？而比較法上建議應以哪些國家為主要參考依據？理由為何？該如何衡平我國《個資法》避免人格權受侵害，以及促進個人資料合理利用間之立法目的？

二、李建良教授回覆

（一）從三個層面觀察，首先從立法與否角度觀之，GDPR 第 17 條的被遺忘權是一個有完整規定，包括請求積極要件、例外情形的成文法，故以法繼受的角度，轉換為我國《個資法》中請求

權基礎適用應為可行。而引進被遺忘權規定的優點是可以具現成規範、且正在運用中的權利作為請求權基礎，就可不需再討論是否要承認被遺忘權這個問題，因為目前我國民事法院還未正式承認被遺忘權。

（二）我傾向引進如 GDPR 第 17 條遺忘權的規定，主因是我國法院對法律未有明文規定且在發展中的權利相對消極，故從立法角度而言，以現成規範加以繼受值得肯定。相對的，須留意立法的負面影響，一但被遺忘權被明文規定，將可能限縮法院的形成可能性；再者需考量未來法院是否會擴大解釋明文的例外規定，如基於公共利益之事由等，而有變向窄化被遺忘權權利內涵的負面影響，這個經驗是參考行政訴訟的資訊公開實務，人民請求資訊公開的實務重點多在於有無例外規定，法院對不用提供資料的例外有擴大解釋之情形。

（三）次從權利位階性角度觀之，應注意立法與非立法推導出的權利屬性問題。歐盟適用 GDPR 第 17 條的案例是於一般法院爭訟，代表立法後其屬性是法律賦予人民的權利，即所稱「法律上之權利」。惟法律上之權利未必是憲法上基本權利；相對的，可想像如果非透過法律規定，而係法院要承認被遺忘權，且是基於憲法保障人民的人格權導出被遺忘權，就會是憲法所衍生的權利。故透過立法者立法規定，將使被遺忘權屬性某程度被定格並產生後續該權利是否屬於憲法上基本權的問題，而須是基本權受侵害始可進入憲法訴訟。

（四）舉一情境為例，立法後有某甲依法律規定於法院提告，而法院以其為例外規定之情形而駁回，如該案窮盡訴訟救濟途徑確定，人民可否聲請進入憲法法庭進行裁判憲法審查？屆時，將不能以法官解釋法律或命令違法為由，而須是侵害原告基本權利。此時回到被遺忘權屬性問題，如被遺忘權是法定明文規定，將難以認定其當然為憲法上權利；如果是由法院依憲法保障人

格權導出的被遺忘權，主張其為憲法上基本權利就相對容易。故如欲以立法引進被遺忘權，可考慮於立法程序補足這個問題，例如立法理由以被遺忘權不只是借鑑 GDPR，而係來自憲法中人格權保障之根基，因此將被遺忘權明文化為憲法權利的明文化等等，在程序上還有很多可能性。

（五）再從權利行使的實踐機制角度，承接前述立法引進的權利屬性問題，應考量是由行政權還是民法上請求權行使。在還未有 GDPR 之前，歐盟被遺忘權有關案例[270]的訴訟過程並非逕於法院提告，而是由人民向屬於行政機關的個人資料保護委員會，請求命資料控管者刪除，經資料控管者拒絕後，始向法院提告，前述權利的行使機制因有行政權的介入類似行政訴訟。

（六）故實踐機制有兩種，一是有行政權的介入與執行、類似行政訴訟的方式，權利基礎屬性就更近於法律上權利。但如欲採行政權介入的模式，成立個資專責機關並仿法國或西班牙由行政權介入來做個資爭議處理，將產生公、私法交錯，法關係會趨於複雜。另一種則是德國模式，即是資料當事人直接向法院提出私人民事訴訟，又德國聯邦憲法法院近來有兩個關於被遺忘權的重要判決，係以民法保障之人格權為請求權基礎，而非 GDPR 第 17 條的權利。如此一來，在德國模式下，人民如敗訴確定，向憲法法院即可以人格權為救濟基礎，就沒有銜接問題。德國學說上有論者也認為 GDPR 的權利並非基本權，如使用 GDPR 的權利向聯邦憲法法院提起訴訟，必須從德國的基本法找出基本權，或如欲採用歐盟法，也須是基於歐盟人權憲章，以 GDPR 第 17 條為基礎反而有被法院駁回的可能。

---

[270] 如歐洲法院於 2014 做出判決 Case C-131/12（Google Spain v. AEPD），該案為一西班牙民眾欲要求 Google 和西班牙先鋒報刪除多年前有關財務危機之報導，經 Google 和報社拒絕，該民眾向西班牙資料保護局 （Agencia Española de Protección de Datos , AEPD）提起訴願，並經 Google 上訴至歐洲法院。

（七）立法時，應考量我國《個資法》的結構，目前我國結構分為公務和非公務機關，前者會是行政訴訟，後者則是民事訴訟，而被遺忘權又以非公務機關居多。我國雖以公務、非公務區分並分別適用行政或民事訴訟程序，但非公務機關如違反《個資法》規定，主管機關仍可以開罰，故立法亦牽涉到《個資法》須有權利如何行使之規定。

三、訪談提綱

（一）上開被遺忘權在法律適用時可能產生挑戰或調適作法，例如被遺忘權之權利行使內容、具體個案認定標準以及與其他基本權利之可能衝突。依您的專業知識與經驗觀察，考量我國現行《個資法》規定以及我國產業經濟結構，若我國《個資法》未來增修被遺忘權，對於現行司法實務與產業發展之影響為何？

（二）針對相關立法調整所產生之適用問題或實務挑戰，有無修法建議措施或其他國外借鏡參考之處？

四、李建良教授回覆

（一）第一點建議是被遺忘權有關刪除的內涵，雖說如 GDPR 第 17 條都有一些框架性的規定，但權利行使的程度為何？刪除的意涵、客體以及到什麼程度？都還是開放的問題，歐盟也持續進行有關規定討論。故我國如要引進，也應考慮已有的歐盟實踐經驗及有關判決、學說並釐清細節，將被遺忘權內涵規定的更清楚。另外有關權利的內涵、行使要件等等也涉及各國法院、司法體制的發展，不一定是較為空白的規定較有利當事人行使權利，多是該國司法願不願意承認該權利的問題。像是美國在隱私權的發展上，不乏以最高法院發展出的判例形塑權利的要件和規定。

（二）惟如一些外國法院可見的判斷標準，亦需留意其代表性及適用性。例如德國 2009 年的一個有關被遺忘權的判決（Spiegel-

Verlag Rudolf Augstein GmbH & Co. KG），德國聯邦憲法法院以時間向度衡量一般人格權與新聞自由的利益，包括隨著時間經過而資訊的重要性遞減，當事人被保護的重要性提升等，上述要件是聯邦憲法法院自行發展，由人格權創設而尚在形成中，還未定性。這些如時間向度等的判準，因尚無法數據化只能保留給司法者衡量。又因為每個案例情形各異且這些個案類型亦尚在累積，德國的判決的案例種類目前也只有兩種類型，如欲參考納入如因果關係的判準、標準等等，可能為時尚早，比較危險。

（三）此外，德國發展的被遺忘權雖以人格權為基礎，但也未完全排除資訊自決的內涵，只是資訊自決權利因為時間的經過，而其逐漸無法行使，例如重大刑案的新聞報導中，因為公共利益的緣故而無法行使資訊自決權；而當時間推移數十年，資訊的權利屬性已不同，不再是自決權的問題，「資訊自決」的屬性已受限，資料當事人在意的不是最初資料揭露、呈現與否的自決的問題，而是為何時間經過已久還要被他人知道的問題。至於退出權與被遺忘權之間的互動關係，是其根基有共通性，退出權是當事人撤回同意即不可再釋出利用，含有資訊自決之意；被遺忘權所涉的資料則往往是合法蒐集利用，但因其持續表現在外，而使人格的形象定格且被持續知悉，而 GDPR 請求刪除資料的要件之一係撤回同意，也隱含資訊自決。

（四）第二點建議是在數位時代下，資料多為數位資料，衍生出資料刪除的地域範圍是否應及於外國的問題，例如去連結之後是否要求國外也無法搜得？我國也可參考歐盟近來的一些相關判決[271]，並提前立法規定。但需留意所欲清楚規定的部分是否已

[271] 例如於歐洲法院於 2019 的判決 Case C-507/17 （Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)）中表示，世界各國對隱私權保護和網路使用者資訊自由間的法益平衡差距甚

成熟或無爭議，如實踐經驗至今仍有爭議或判準尚在形成，則仍應該開放討論，避免壓縮未來形塑的可能性。

（五）最後，仍須視立法成熟度進行立法選擇，因人民對被刪除資料的需求性還需實證研究方可得知，應留意一次性的全盤修訂是否可能使法規成為具文，也有些問題會以局部型、部門法的方式規定，如醫療方面的敏感資料等等，因較有需要故先行規定，而不是採用一般性的概括規定。至於被遺忘權對產業的影響，我認為這個規定會設有許多例外，影響還好，較屬於實踐上的問題，因其可能在國外多有爭議，但可以想像在國內是否同樣受到人民重視，會有實證研究的問題。

大，原則上 GDPR 被遺忘權的範圍應限於歐盟成員國之地域範圍。*Judgment of the Court (Grand Chamber) of 24 September 2019. Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507 (last visited Apr.18, 2022.) note [60]-[62].

國立臺灣大學法律學院李建良教授訪談

壹、訪談資訊

一、　訪談主題：個人資料保護法相關議題研析之資料可攜權修法與法制建議討論

二、　訪談日期：2022 年 4 月 29 日（五）

三、　訪談地點：線上視訊會議

四、　訪談人：盧秉義副研究員、賈忻蓉副研究員

五、　受訪者：李建良教授

貳、訪談內容

一、訪談提綱

（一）綜訪談提綱所述，我國《個資法》目前針對資料可攜權並無明確規範，參考其他多數國家如歐盟、英國、德國、美國、新加坡及澳洲個資法令皆有相關規範；而日本則無此規定；另韓國自取得 GDPR 適足性認定後，已於 2021 年 9 月提出相關修正草案。

（二）依您的專業觀點，我國《個資法》未來應否增修或不增修相關權利規範？而比較法上建議應以哪些國家為主要參考依據？理由為何？該如何衡平我國《個資法》避免人格權受侵害，以及促進個人資料合理利用間之立法目的？

二、李建良教授回覆

（一）資料可攜權的概念在實務上已有較長時間的討論，傳統案例有如手機門號的移動，而 GDPR 發展可攜權的形貌和規定也已進入相對成熟的程度。在此先釐清可攜權與被遺忘權性質上一個較大的差異，被遺忘權一定程度有憲法上人格權的根基，被遺

忘權是否立法有其利弊得失，即使不立法也可由憲法人格權推導，例如德國即是結合民法對人格權的保護憲法保障人格權發展出被遺忘權，相對而言 GDPR 則是以第 17 條明文化；但是資料可攜權則未必是憲法上的權利，很大程度是法律創設的權利，如 GDPR 第 20 條創設可攜權之規定，資料是否可攜、可移轉，有很大的立法形成空間，因而很多地方如不透過立法，要從憲法推導出一個可攜權較為困難，故其立法的需求相對較高，如評估資料可攜權具重要性，則我傾向以立法增設可攜權。

（二）再者，如以立法引進可攜權，則以法繼受以及較合於我國法體系可能性的角度觀之，GDPR 第 20 條發展出的可攜權規定實可做為繼受、轉換為合於我國條文的參考，故我較傾向是否可透過我國個資法將可攜性入法。基於上述，可攜權的議題可從以下 5 大問題討論：第一個問題是何謂可攜性，第二是誰的資料可被移轉的主體問題，第三是可攜的資料是哪些資料的客體問題，第四是如何可攜、如何移轉，第五則是誰負責移轉資料。

（三）在談上述問題前，需先理解可攜權的重要性。資料可不可以帶走，過往比如門號由契約到期的 A 手機業者移轉到 B 手機業者使用，是實體性的資料可攜的問題；現在進入數位時代，可攜權的應用範圍愈來愈廣，不再只是實體資料的移轉，牽涉數位資料的移轉。以下就以社群平台如 FB 類型的資料可攜權來理解上述五個問題較容易對應，例如 FB 有許多留言，當使用者要離開平台、關閉 FB 帳號時，是否可帶走資料？此即為進入數位和網路時代遇到的可攜權問題。

（四）首先談可攜性的權利內涵，大概可分為兩個面向，其一是當事人取得可攜性資料的取得權，促使資料可以被攜帶、離開平台時要能夠帶走，避免被鎖定的效應，故同時也涉及技術性問題；再者是資料的移轉權，包括由平台移轉至平台間的直接移轉，以及由平台給資料當事人後由當事人給別人的間接移轉。要讓

可攜權的輪廓更清晰，可透過與其他權利的比較，例如與被遺忘權的比較，這兩個權利互不排斥，我可以把資料帶走，也可以不帶走但是刪除資料。

（五）第二是誰的資料可被移轉的問題。以社群平台來說，很難說純粹屬於個人資料。與他人聊天、對話等資料可能很大部分包含別人的資料，例如與他人在社群平台上的相片等，此時涉及別人的權利如何以法律保護，也是可攜權立法規範重點。

（六）第三是可攜資料應包括哪些資料的問題。此時將涉及一個基礎問題，即平台和使用者之間的法律關係的定性，影響平台業者可否刪除使用者的資料。即使這個問題仍在發展中，且現在契約形貌與過去不太相同，一般仍會界定平台和使用者之間係私法契約關係，基本上會有某種告知同意的情形，法律關係是雙方合意。該與平台的約款亦會決定資料屬於誰，例如民法上定型化契約約款，故資料歸屬也須回歸契約約定，受平台約款限制。然而，有些資料可能基於公益理由受到強行法的規制而剝奪資料的可攜性，例如基於公共利益等理由而不予轉移資料。故何種資料可攜就有兩個基礎的法律關係，一是平台與使用者間的契約關係將用以區辨資料是否為個人資料；第二個就是所謂的強行法基於公益理由限制可攜性。

（七）應注意可攜之資料也並非皆為純粹個人資料，有可能是跟當事人有關的資料。以平台為例，所稱資料有三種，一是使用平台所需之個人資料，例如帳號的建立、密碼、姓名等，這些資料應屬核心可攜之資料；二是溝通資料，例如對話、照片和影音紀錄等非純粹的個人資料且包含他人之資料，也在可攜權的範圍；三是非主動產出而係被動取得的資料，例如使用紀錄和搜尋紀錄等等。故可知，資料可攜權概念的資料範圍並不以可識別為個人為範圍，在社群平台上更接近於是否跟當事人相關連，

如此可能無法明確與他人切割的情形乃可攜權之特性，亦為可攜權之難題。

（八）我國個資法中個人資料的定義，基本以可識別個人為主；但可攜權的資料，以平台業者為例，就有可能包含他人資料，主要在於是否與當事人相關連，而不以可識別為限，故將有立法和適用的問題，如果欲同時達到個資保護、消費者保護法和公平競爭之規範意旨，未來理論上可能應從寬認定資料可攜之資料範圍。此外，資料的範圍除了由當事人提供、產出之資料，是否應該包括被動取得的資料，例如社群媒體中別人的傳訊、使用紀錄、停留時間和位置、搜尋紀錄等等，前述也應屬於可攜之範圍。這也是我一開始所提到不屬於人格權的部分，需要以法律創設保護。

（九）第四是如何可攜的問題。可攜權如果要運作，勢必不能很明顯的切割自己與他人的資料，因而可攜的難題也在於如何保障別人的資料。因此在資料可攜的機制中，首先應先保障資料的取得，相較於傳統可攜情形如門號可攜，在數位時代中應是轉換為程式化的資料，如何程式化並依國內產業情形而定，例如GDPR 第 20 條的規定；再者是平台因應當事人的要求給資料，也就是取得權；當資料要更進一步移轉出去，如該資料包含第三人的資料，應建立第三人同意的機制，保護第三人的個資，因為第三人不見得願意一同轉出。

（十）第五是誰負責移轉資料的問題。可能移轉的方式有兩種，如前述所提由平台移轉至平台間的直接移轉，以及由平台給資料當事人後由當事人給別人的間接移轉，由誰及如何進行移轉並沒有標準答案，例如歐盟 GDPR 第 20 條可攜權的規定，是達個人資料可由一控管者傳輸至另一控管者之程度，美、澳則只要求是電子形式、不妨礙移轉，故主要應視國內產業情形而進行法律上設計。

三、訪談提綱

（一）上開資料可攜權在法律適用時可能產生挑戰或調適作法，例如被權利行使內容、具體個案認定標準以及與其他基本權利之可能衝突。

（二）依您的專業知識與經驗觀察，考量我國現行《個資法》規定以及我國產業經濟結構，若我國《個資法》未來增修可攜權，對於現行司法實務與產業發展之影響為何？針對相關立法調整所產生之適用問題或實務挑戰，有無修法建議措施或其他國外借鏡參考之處？

四、李建良教授回覆

（一）除了思考前述提到可攜權相關的五個問題之外，因其一定程度有別於過去的權利，屬於新的權利，需要思考其在既有法秩序下的定位應為何。因此，以上述法秩序定位問題為基礎，資料可攜權有多重的面貌和特性，至少有三個面向：其一可攜權是個人資料保護的一部分，讓資料具有可攜性、可被移轉對當事人來講是一種個人資料保護的強化面向；其二是消費者保護面向，可攜權也涉及消費者保護法權利的發展；其三是公平競爭法的面向，資料的移動也影響平台、企業之間的公平競爭秩序，如使用者欲從一擁有很多資料的大型平台離開時無法帶走資料，會使競爭秩序被綁定，可攜權可能產生打破市場一定程度集中的情形，涉及公平競爭的維護。

（二）可攜性將使平台業者的義務提升，需要讓資料可被帶走，促成平台間的公平競爭，並提高了個資自主性。故可攜性不僅僅是做為個人資料自主的一個面向，其重要性和複雜性也在於其帶有三個面向。現行我國個資法雖已有資料查詢、提供複製本的規定，但終究與可攜權之功能不同，其係將資料轉換為可攜資料，非僅是取得、查詢資料；且可攜權入法可打破私法契約的約定，也將影響消保法面向有關時下常見定型化契約的約定。

（三）有關權利衝突，例如前面提到建議在可攜權行使機制中應建有第三人同意的相關機制，該第三人保障機制一定要透過法律規定為宜，因以於平台間移轉對話資料為例，如無法律規定而僅交由平台自行建置運作，未經第三人同意移轉與第三人有關之資料時該第三人資料保護權利被侵犯，發生爭議即無法釐清責任、也可能阻礙第三人行使被遺忘權。

（四）在法繼受以及比較法的參考上，應留意像德國的個資保護體系，不是只有單一的個資法，在個資法之外，還有很多法律有自己個資保護相關的規定，例如較嚴格的部門法等，因而多會先視個別規定，無相關個資保護規定才回歸個資法處理。我國個人資料保護則主要透過單一《個人資料保護法》規定，像是我國在傳染病防治法在個資保護的規範就不足，建議針對傳染病防治法個別建置一套個資保護規定，並且加速更新《個人資料保護法》。

（五）另有關哪些資料可攜，受到平台約款和強行法之公益理由限制的影響，惟長期觀察下來我國公益條款常被擴大適用，應而建議立法、修法時清楚、較嚴格的訂定對限制權利行使的理由及其要件，例如德國對公益的解釋就較為嚴格。

（六）此外，GDPR 第 20 條提到的結構性、通用性、機器可讀性等條件，應留意歐盟的法律多包含有歐洲單一市場的思維，因此歐盟法會影響會員國法，例如歐盟法影響德國法，但歐盟法並不等於德國法；形式要件是否只要符合這三者，並沒有標準答案，前述問題有提到的資料可攜方式應以程式化的方式，所謂程式化是較簡化的想法，是與傳統可攜如門號可攜的對比，實際上應視國內產業情形而定。

台灣科技產業法務經理人協會余啟民秘書長訪談

壹、訪談資訊

一、 訪談主題：個人資料保護法相關議題研析之國際傳輸修法建議討論

二、 訪談日期：111 年 5 月 31 日（二）

三、 訪談地點：TEAMS 線上

四、 訪談人：周芷瑄副研究員

五、 受訪者：余啟民秘書長

貳、訪談內容

一、訪談提綱

（一）我國《個人資料保護法》（下稱個資法）對於國際傳輸規定，若參考國際趨勢改採以原則禁止、例外允許進行限制，將安全維護措施條款（例如：企業自我拘束規則、標準契約條款、行為守則、認證）列為基本要求，並以中央目的事業主管機關認可之方式，作為例外允許國際傳輸之規定，是否妥適？若是，安全維護措施條款具體內容應包含項目為何？

（二）我國若參考日本或新加坡立法例，於個資法或隱私保護相關規範中，承認 CBPR 驗證為符合我國國際傳輸合法性要件的方式之一，是否妥適？若是，政府認可對產業的影響力為何？具體該以何種形式或文字呈現較為適當？（例如：將 CBPR 驗證直接納入個資法作為國際傳輸方式之一，抑或是由個資主政機關或是中央目的事業主管機關以函釋、子法或其他方式承認 CBPR 驗證為符合我國國際傳輸合法性要件的方式之一。）

二、余啟民秘書長回覆

（一）同意應隨國際趨勢，將個資法國際傳輸規定修改成原則禁止、例外允許，而取得 CBPR 驗證可為安全維護措施之一，但是具體內容必須再加上經中央目的事業主管機關申報再進行核可。採用這樣的方式目的是建立一套主動申報機制，唯有企業主動申報，政府才可有效監管、實際執法。申報機制中的政府單位應為中央目的事業主管機關而非國發會個資主政機關，因為現行機制下，中央目的事業主管機關本已定期發函請所屬機關進行個資盤點及風險評鑑，但是並不清楚企業是否徹底落實，因此在現有中央目的事業主管機關體制下建立一套申報及核可機制是可行的，藉此，中央目的事業主管機關才能透過主動申報機制即時掌握資訊，如同金融監理科技，我國應建立個資監理科技，將目前的申報機制從紙本變數位化，打造單一資料申報平台。

（二）中央目的事業主管機關要求申報之內容，應包含對所屬產業擬定自我約束條款，自我約束條款之內容可與 CBPR 驗證規則相稱，意指，自我約束條款應包含個資盤點及個資作業流程風險評估，如同 GDPR 之 Data Protection Impact Assessement，並應納入適法性評估以符合國際要求。

（三）該申報制度除符合 CBPR 要求，應與公司治理（ESG）結合。現行法律規定公司應定期向主管機關進行董、監、股數申報，個人資料之管理應比照辦理。另外，公司治理本含有內、外稽核要求，因此若將個資保護與公司治理結合，將取得個資驗證設為加分項目是合理的且不會對企業造成過大負擔。加強自動申報之力度才可使我國政府主管機關達到有效監管及執法，確保企業真正落實法遵並提升產業個資保護水準。

（四）並不支持直接將 CBPR 驗證直接寫入個資法作為國際傳輸合法性要件之一，因為如之後需要調修，修法時間太冗長，效率不

高。反而建議將 CBPR 驗證程序、CBPR 驗證規則，這些相等同（equivalent）的概念寫進個資法，較為妥適。例如，應取得包含以下驗證程序的國際驗證…，驗證規則應包含以下驗證要件…，並列出 CBPR 驗證程序及驗證規則。因此，可以下列形式或文字呈現：「但符合下列情形之一者，得國際傳輸個人資料：取得國際驗證，並經中央目的事業主管機關產業申報之後核可。」

（五）事實上，目前無法評估政府認可 CBPR 驗證對產業是否會有影響力，因為必須先認可並實施約兩年之後才能斷定實質影響力是否為正面，並依據成效進行機動性調整。然而，影響力應該會趨向於正面，重點在於政府如何鼓勵企業將取得 CBPR 標章從企業負擔轉換成企業加分項，將個人資料保護導入公司治理應為努力目標。

附件三、國際觀測相關彙整之簡報內容

2022 年上半年度國際個資關鍵議題分享會

上半年度國際個資關鍵議題分享會

科技法律研究所
財團法人資訊工業策進會
2022.03.02

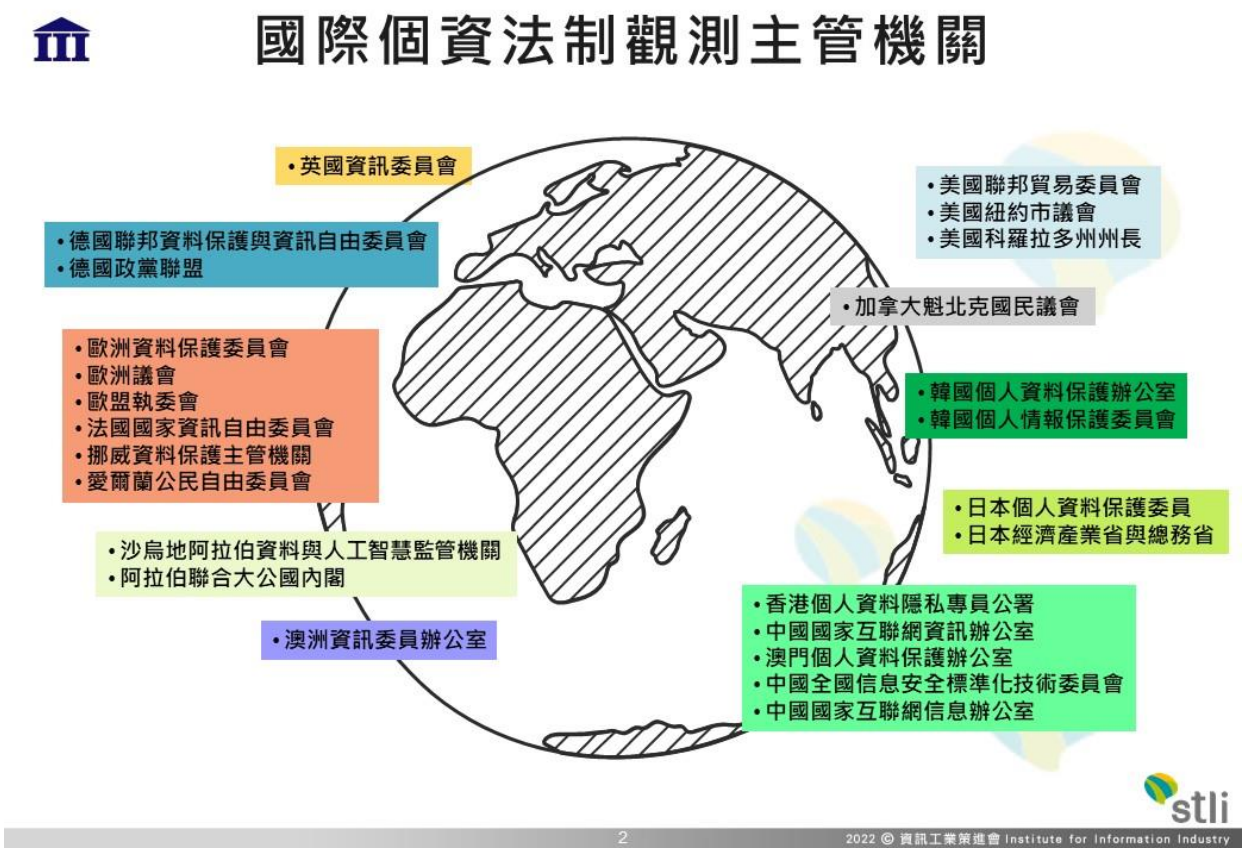
stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

資訊工業策進會 Institute for Information Industry

大綱

- 國際個資法制觀測主管機關
- 國際個資法制觀測議題綜覽
  - 1、立法修法國際動態
  - 2、資通訊領域個資議題
  - 3、人工智慧或生物識別
  - 4、COVID-19因應措施
  - 5、裁罰實務案例
  - 6、GDPR適足性認定
  - 7、國際傳輸

2022 © 資訊工業策進會 Institute for Information Industry


國際個資法制觀測主管機關
•英國資訊委員會
•德國聯邦資料保護與資訊自由委員會
•德國政黨聯盟
•歐洲資料保護委員會
•歐洲議會
•歐盟執委會
•法國國家資訊自由委員會
•挪威資料保護主管機關
•愛爾蘭公民自由委員會
•沙烏地阿拉伯資料與人工智慧監管機關
•阿拉伯聯合大公國內閣
•澳洲資訊委員辦公室
•美國聯邦貿易委員會
•美國紐約市議會
•美國科羅拉多州州長
•加拿大魁北克國民議會
•韓國個人資料保護辦公室
•韓國個人情報保護委員會
•日本個人資料保護委員
•日本經濟產業省與總務省
•香港個人資料隱私專員公署
•中國國家互聯網資訊辦公室
•澳門個人資料保護辦公室
•中國全國信息安全標準化技術委員會
•中國國家互聯網信息辦公室
stli
2
2022 © 資訊工業策進會 Institute for Information Industry

國際個資法制觀測議題綜覽
1 立法修法 國際動態
2 資通訊領域 個資議題
3 人工智慧或 生物識別
4 COVID-19 因應措施
5 裁罰實務案例
6 GDPR適足性認定
7 國際傳輸
stli
3
2022 © 資訊工業策進會 Institute for Information Industry

1、立法修法國際動態

2022 © 資訊工業策進會 Institute for Information Industry

1、立法修法國際動態(1/6)

主題摘要

美、英、加等國提出個資隱私法律相關立法及修法

- 美國科羅拉多州通過《科羅拉多州隱私法》
- 美國俄亥俄州公告《俄亥俄州個人隱私法》草案
- 英國 UK GDPR 修法公開徵詢意見
- 加拿大魁北克省、沙烏地阿拉伯、阿拉伯聯合大公國推出個資隱私新法
- 義大利《個人資料保護法》發布重大修正

英、日、法、歐針對個資隱私法規實踐修訂子法及標準指南

- 英國《匿名化、假名化和隱私增強技術指南》公開徵詢意見
- 日本《令和三年修正個資法民間部門指引案》公開徵詢意見
- 法國發布《資料保護專員指南》
- 歐盟發布《資料主體之近用權利指導方針》

2022 © 資訊工業策進會 Institute for Information Industry

1、立法修法國際動態(2/6)

美、英、加等國提出個資隱私法律相關立法及修法-1

2021.07.01 **美國科羅拉多州通過《科羅拉多州隱私法》**

美國科羅拉多州是繼加州與維吉尼亞州之後，第三個成為擁有隱私保護專法的州，該法將於2023年7月1日生效。CPA生效後，**消費者除近用權、更正權、刪除權與資料可攜權等權利外**；亦規定在資料控制者對其消費者進行目標式廣告、銷售消費者個人資料，或者將對消費者決策產生重大影響時，**消費者享有選擇退出權**。違反CPA可處最高2,000~50萬美元民事懲罰。

2021.07.13 **美國俄亥俄州公告《俄亥俄州個人隱私法》草案**

- 美國俄亥俄州副州長公告《俄亥俄州個人隱私法》（Ohio Personal Privacy Act, OPPA）草案，**賦予消費者知悉權、近用權、刪除權、資料銷售退出權及不受歧視權**。
- OPPA草案中所謂「消費者個人資料」排除：

1. 法規保護之個資（如健康資訊及紀錄、病患辨識資訊、受試者之個資及相關資訊、病患安全工作成果、個人信用等）。
2. 依法（如駕照法、家事法、醫療法等）所得個資或依法授權得使用於公衛之資訊等。

2022 © 資訊工業策進會 Institute for Information Industry

1、立法修法國際動態(3/6)

美、英、加等國提出個資隱私法律相關立法及修法-2

2021.09.10 **英國UK GDPR修法公開徵詢意見**

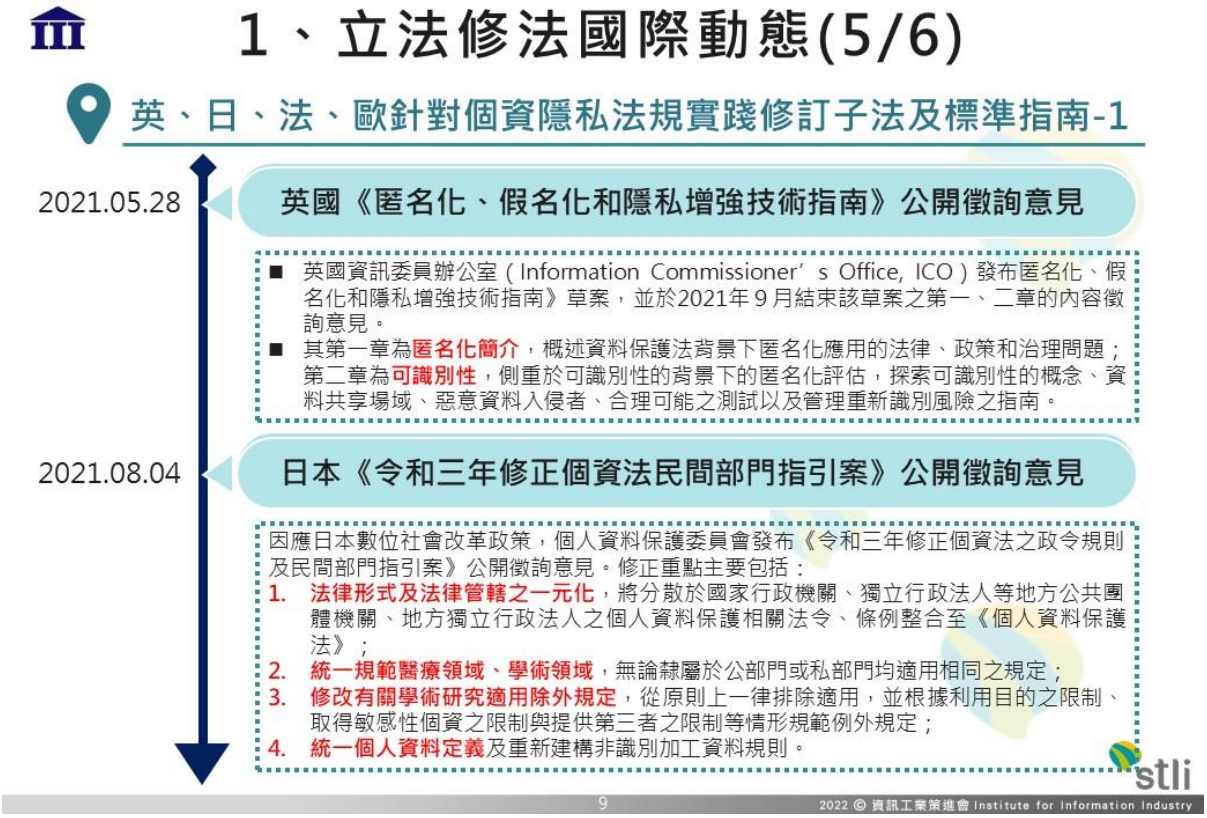
由於英國政府於2020年9月發布《國家資料策略》（National Data Strategy），其中表明要進行個資法規相關修法，因此英國文化媒體暨體育部（Department for Culture, Media and Sport, DCMS）公布公眾諮詢文件《資料：新方向》（Data: A new direction），**正式啟動公眾諮詢展開國內隱私法規修法第一步，為期10年**，修法目標係將英國隱私法規晉升為一部持續成長及值得信任之隱私法規體系。

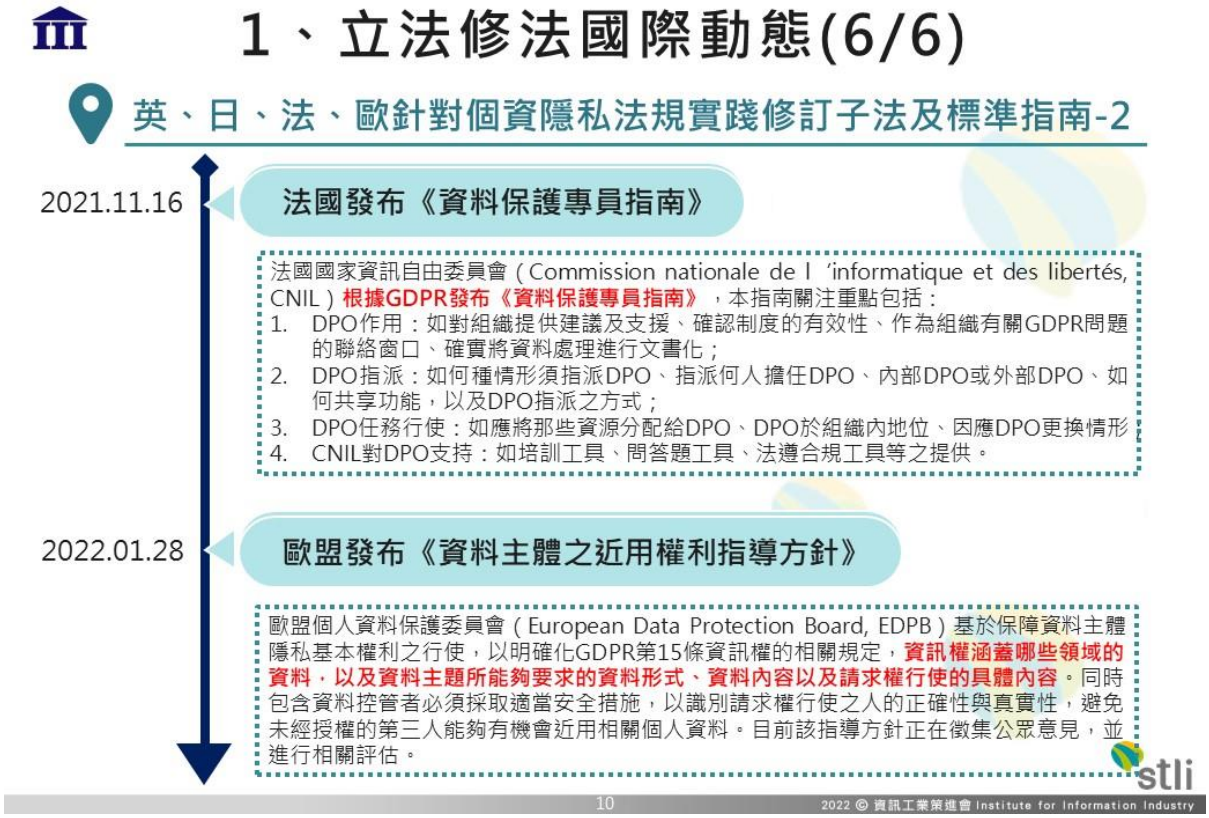
2021.09.22 **加拿大魁北克省通過《個人資料保護法》**

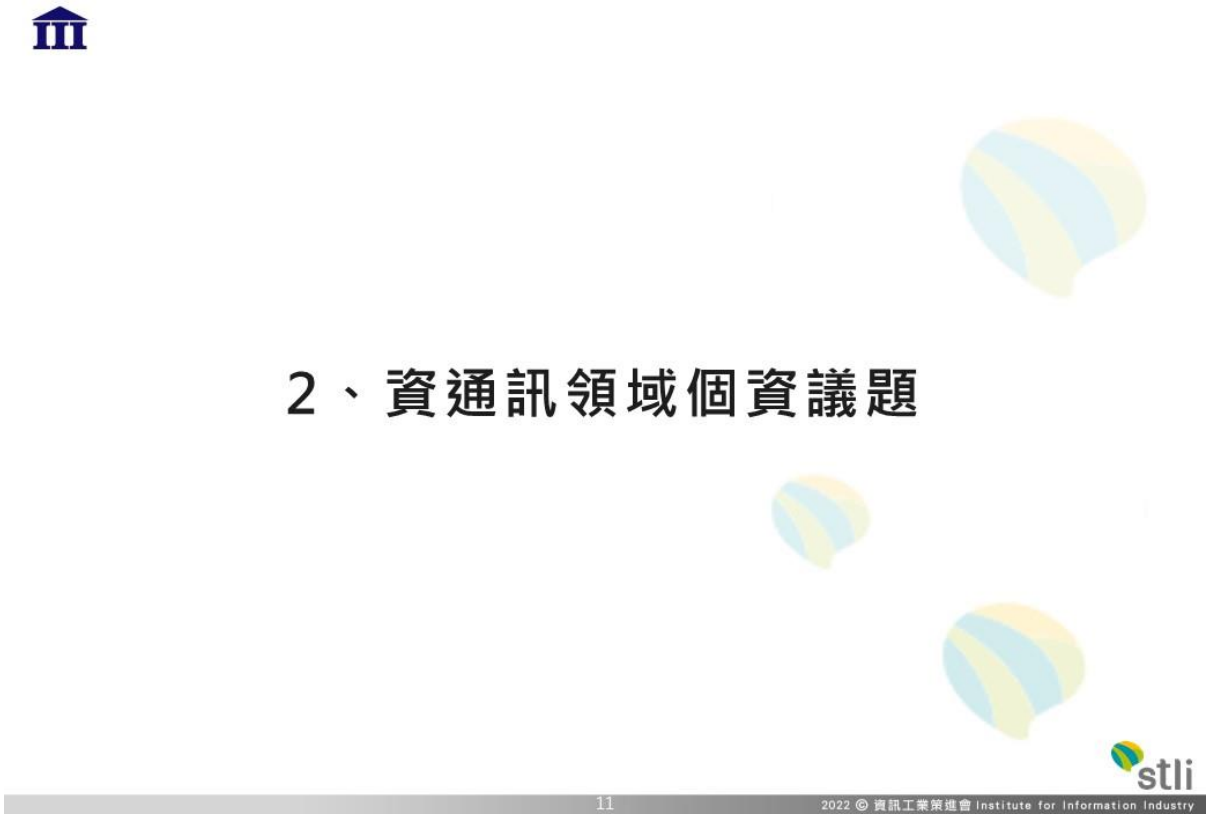
- 加拿大魁北克省通過《關於個人資料保護規定現代化法》（An Act to modernize legislative provisions as regards the protection of personal information），除了部分1年後生效及3年後生效的可攜權條款之外，大部分規定將預計於2年後，即2023年9月22日正式生效。
- 本法**規範內容包括資料侵害報告、指派資料保護專員、實施資料保護影響評估要件等規定，並擴大當事人權利**。在罰則規定上，作為行政罰之罰鍰將增加至全球銷售額的2%或個人最高處以5萬加元、企業最高處以1千萬加元之金額。

2022 © 資訊工業策進會 Institute for Information Industry

1、立法修法國際動態(4/6)
美、英、加等國提出個資隱私法律相關立法及修法-3
2021.09.24
沙烏地阿拉伯通過《個人資料保護法》
沙烏地阿拉伯通過《個人資料保護法》並於2022年3月23日施行，旨在確保個人資料隱私規範資料共享並防止濫用個人資料，以開發數位基礎設施、支持數位經濟增長的創新爲國家2030年願景目標。
2021.11.27
阿拉伯聯合大公國通過《個人資料保護法》
阿拉伯聯合大公國通過《個人資料保護法》並於2022年1月2日施行，旨在加強經濟、投資及貿易機會，以保護整個阿拉伯聯合大公國個人資料，適用於設立在阿拉伯聯合大公國境外並與阿拉伯聯合大公國資料主體相關的處理活動的資料控管者及資料處理者。
2021.12.03
義大利《個人資料保護法》發布重大修正
義大利《個人資料保護法》修正重點：
1. 擴充公務機關依職權或依公共利益處理個人資料之法律依據包含「為公共利益所執行的任務或行使公務權力」。此外，公務機關處理個人資料的合法依據可能是一般行政行為，而不僅是法律或法規。
2. 加強對「色情報復」法律保護並提升主管機關對私人性愛內容外洩之監管權。
stli
8
2022 © 資訊工業策進會 Institute for Information Industry


1、立法修法國際動態(5/6)
英、日、法、歐針對個資隱私法規實踐修訂子法及標準指南-1
2021.05.28
英國《匿名化、假名化和隱私增強技術指南》公開徵詢意見
■ 英國資訊委員辦公室（Information Commissioner’s Office, ICO）發布匿名化、假名化和隱私增強技術指南》草案，並於2021年9月結束該草案之第一、二章的內容徵詢意見。
■ 其第一章為匿名化簡介，概述資料保護法背景下匿名化應用的法律、政策和治理問題；第二章為可識別性，側重於可識別性的背景下的匿名化評估，探索可識別性的概念、資料共享場域、惡意資料入侵者、合理可能之測試以及管理重新識別風險之指南。
2021.08.04
日本《令和三年修正個資法民間部門指引案》公開徵詢意見
因應日本數位社會改革政策，個人資料保護委員會發布《令和三年修正個資法之政令規則及民間部門指引案》公開徵詢意見。修正重點主要包括：
1. 法律形式及法律管轄之一元化，將分散於國家行政機關、獨立行政法人等地方公共團體機關、地方獨立行政法人之個人資料保護相關法令、條例整合至《個人資料保護法》；
2. 統一規範醫療領域、學術領域，無論隸屬於公部門或私部門均適用相同之規定；
3. 修改有關學術研究適用除外規定，從原則上一律排除適用，並根據利用目的之限制、取得敏感性個資之限制與提供第三者之限制等情形規範例外規定；
4. 統一個人資料定義及重新建構非識別加工資料規則。
stli
9
2022 © 資訊工業策進會 Institute for Information Industry


1、立法修法國際動態(6/6)
英、日、法、歐針對個資隱私法規實踐修訂子法及標準指南-2
2021.11.16
法國發布《資料保護專員指南》
法國國家資訊自由委員會（Commission nationale de l 'informatique et des libertés, CNIL）根據GDPR發布《資料保護專員指南》，本指南關注重點包括：
1. DPO作用：如對組織提供建議及支援、確認制度的有效性、作為組織有關GDPR問題的聯絡窗口、確實將資料處理進行文書化；
2. DPO指派：如何種情形須指派DPO、指派何人擔任DPO、內部DPO或外部DPO、如何共享功能，以及DPO指派之方式；
3. DPO任務行使：如應將那些資源分配給DPO、DPO於組織內地位、因應DPO更換情形
4. CNIL對DPO支持：如培訓工具、問答題工具、法遵合規工具等之提供。
2022.01.28
歐盟發布《資料主體之近用權利指導方針》
歐盟個人資料保護委員會（European Data Protection Board, EDPB）基於保障資料主體隱私基本權利之行使，以明確化GDPR第15條資訊權的相關規定，資訊權涵蓋哪些領域的資料，以及資料主題所能夠要求的資料形式、資料內容以及請求權行使的具體內容。同時包含資料控管者必須採取適當安全措施，以識別請求權行使之人的正確性與真實性，避免未經授權的第三人能夠有機會近用相關個人資料。目前該指導方針正在徵集公眾意見，並進行相關評估。
stli
10
2022 © 資訊工業策進會 Institute for Information Industry


2、資通訊領域個資議題
stli
11
2022 © 資訊工業策進會 Institute for Information Industry

2、資通訊領域個資議題(1/5)

主題摘要

中、日、法針對資訊安全及數位轉型議題提出規範

- 中國大陸《互聯網資訊服務演算法推薦管理規定》公開徵詢意見
- 中國大陸《網路安全標準實踐指南—數據分類分級指引》公開徵詢意見
- 日本制定「數位轉型時代企業隱私治理指導手冊」第1.1版
- 法國發布數位支付與資料保護之白皮書

英、日、德、美提升電信、新聞規範以加強隱私保護

- 英國《新聞業務守則》草案公開徵詢意見
- 日本發布《電信事業個人資料保護指引修正案》
- 德國發布《電信—電信媒體—資料保護—法律》指南
- 美國對電信業客戶專屬網路資訊外洩事件加強通報規範

2022 © 資訊工業策進會 Institute for Information Industry

2、資通訊領域個資議題(2/5)

中、日、法針對資訊安全及數位轉型議題提出規範-1

2021.08.27 **中國大陸《互聯網資訊服務演算法推薦管理規定》公開徵詢意見**

- 該草案訂定利用演算法推薦技術提供網路服務之管理規範，**要求演算法推薦服務提供者以顯著方式向使用者告知演算法推薦服務情況**，並以適當方式公示演算法推薦服務的基本原理、目的意圖、運行機制等。
- 該草案適用在中國大陸境內各類利用演算法推薦服務的互聯網公司，幾乎都在監管的射程範圍內，如短視頻平台、電商平台、社交平台及餐飲外賣平台等。該草案期望透過建立全面監督管理體系，加強行業自律並落實社會監督，並建立特殊分級制度，以增加演算法推薦技術的公開透明度，保障用戶的知情權。

2022.09.30 **中國大陸《網路安全標準實踐指南—數據分類分級指引》公開徵詢意見**

- 本指南依據《中華人民共和國數據安全法》第19條訂定資料分類與等級保護系統，旨在圍繞網路安全法律法規政策、標準、網路安全及事件等主題，**宣傳網路安全相關標準及知識，提供標準化實踐指引**。
- 該指引提出個人資料、法人資料及公共資料三種資料類型的識別規則，個人資料又分為一般性、機密性、隱私性三類；法人資料則分為商業資料、管理運用資料、系統操作與安全性資料三類。此外各類資料依照公開、內部、敏感、重要、核心五個級別的資料定級規則分為1到5級，表示各類必要最低限的資安標準。

2022 © 資訊工業策進會 Institute for Information Industry

2、資通訊領域個資議題(3/5)

中、日、法針對資訊安全及數位轉型議題提出規範-2

2021.07.19 日本制定「數位轉型時代企業隱私治理指導手冊」第1.1版

- 日本經濟產業省與總務省於2020年8月制定「數位轉型時代企業隱私治理指導手冊」第1.0版，闡述企業在隱私治理應有作為；並於2021年7月制定「數位轉型時代企業隱私治理指導手冊」第1.1版，提供企業隱私治理參考。未來將持續更新本指導手冊，並適時為考量社會趨勢修訂以作為企業實踐之指導方向。
- 第1.1版相較於第1.0版，更新內容包括：

1. 提出企業管理層**應有作為之三項要求**，即闡明對隱私治理的態度、設置專門負責隱私保護人員以及實施資料衝擊影響評估等為隱私治理工作投入資源；
2. 對隱私治理重要事項的**案例更新**；
3. 根據第1.0版就企業隱私治理實踐狀況進行更新與**增加參考案例**。

2021.10.06 法國發布數位支付與資料保護之白皮書

法國國家資訊自由委員會（CNIL）有鑑於數位支付的過程中，可能會涉及資料保護與隱私安全的議題，發布《信任需付出代價：現在與未來支付方式之資料保護挑戰白皮書》，**針對數位化金融支付的議題，提供一個完整資料保護與隱私安全規劃之指引文件**，以建立良好的信任關係與環境條件。金融支付工具對於經濟利益的影響層面，包含銀行金流、交易記錄、個人交易的詳細記錄以及可識別特定當事人之相關資料，對於相關資料的去識別化程度、國際傳輸議題以及是否符合GDPR要求，在個資保護與資訊安全議題內都相當重要

2022 © 資訊工業策進會 Institute for Information Industry

2、資通訊領域個資議題(4/5)

英、日、德、美提升電信、新聞規範以加強隱私保護-1

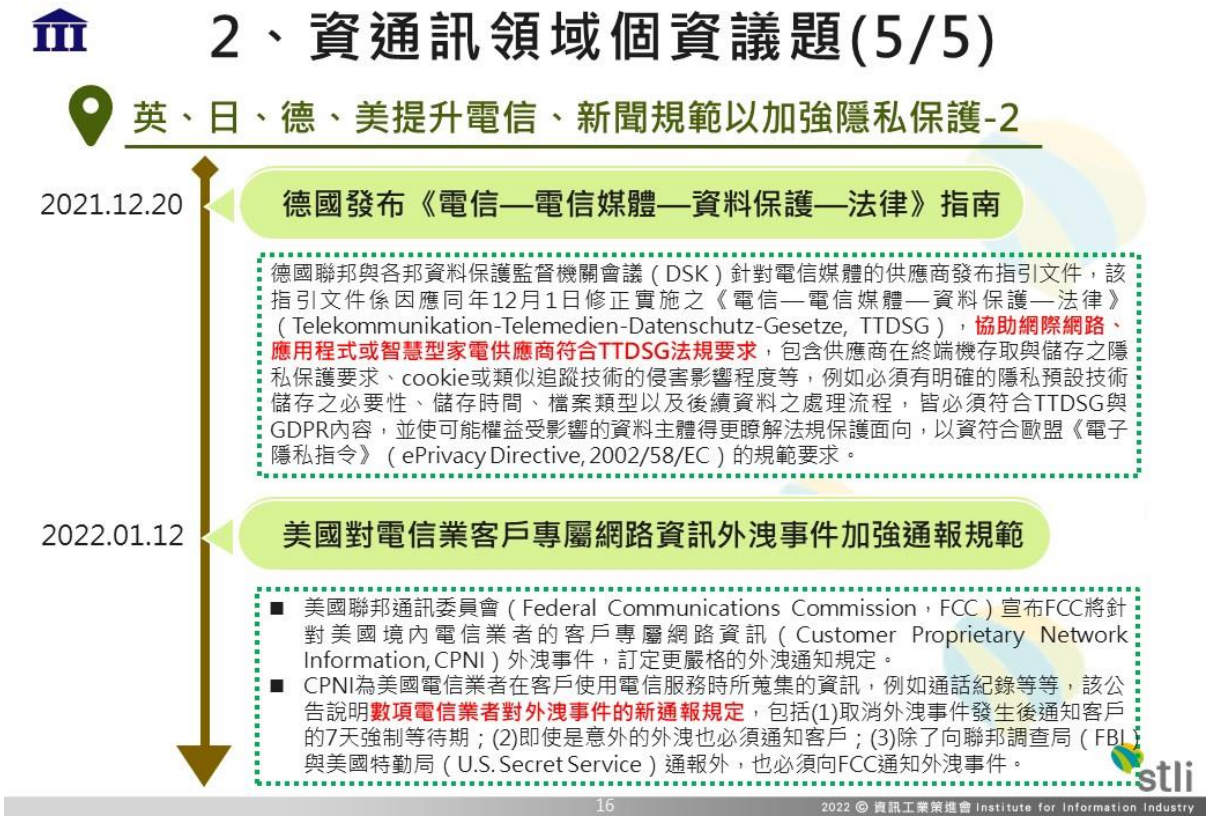
2021.10.13 英國《新聞業務守則》草案公開徵詢意見

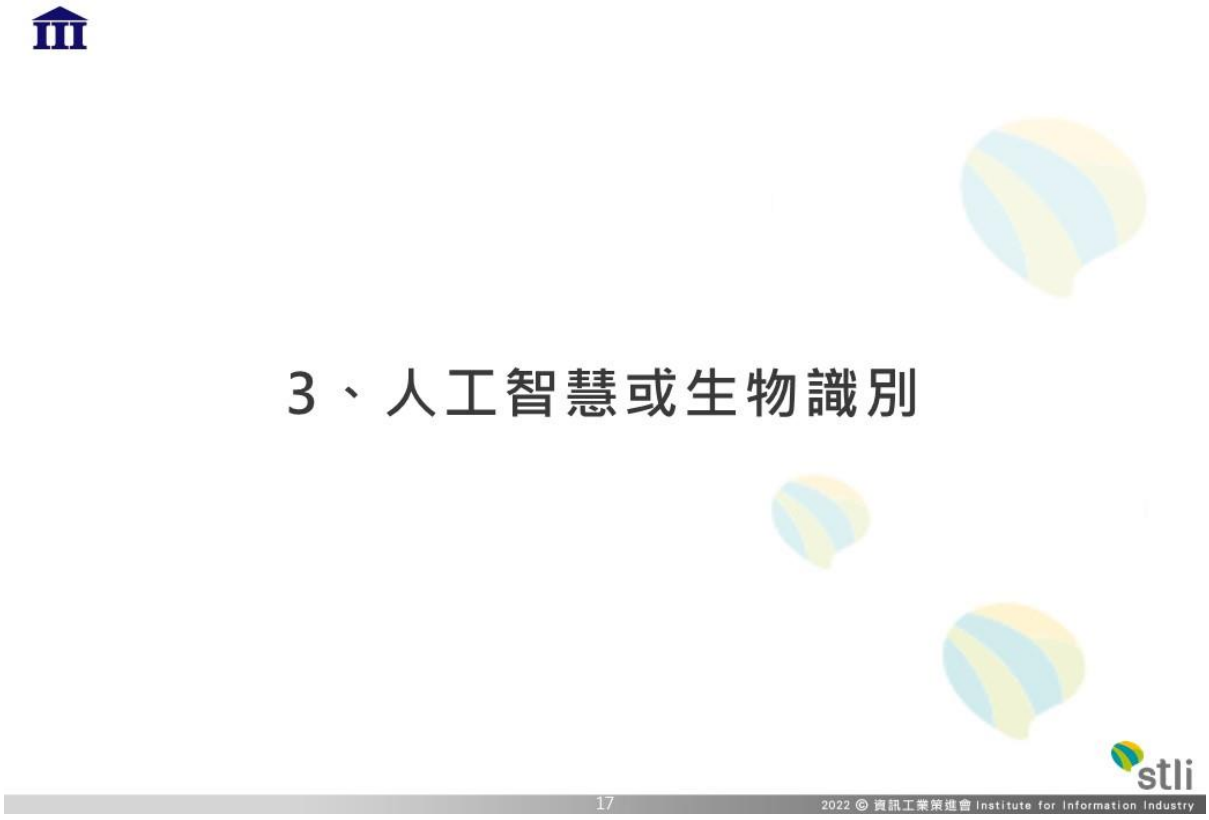
- 英國資訊委員辦公室（ICO）2021年10月13日開放關於新聞業務守則草案（draft journalism code of practice）的意見徵詢，並於2022年1月24日結束徵詢意見。此次主要徵詢**有關新聞業守則草案的意見回饋**，依《英國資料保護法》（Data Protection Act 2018, DPA 2018）第 124 條的法定條例，針對新聞目的處理個人資料之規範。
- 該草案針對新聞業者提供實用指南，分為以下部分：(1)平衡新聞和隱私；(2)證明合規性；(3)保護個人資料安全；(4)證明使用個人資料的正當性；(5)採取合理措施確保個人資料準確；(6)為特定目的處理個人資料；(7)使用適量的個人資料；(8)保留個人資料之時間；(9)明確角色和職責；(10)幫助人們行使其權利；(11)爭議與執法；(12)UK GDPR特殊豁免規定等。

2021.11.02 日本發布《電信事業個人資料保護指引修正案》

- 日本總務省於2021年11月2日舉辦「有關平臺服務之利用者資料處理審議會」（プラットフォームサービスに係る利用者情報の取扱いに関するワーキンググループ），並同時發布《電信事業個人資料保護指引修正案》（電気通信事業における個人情報保護に関するガイドライン改正骨子（案））。
- 修正案**對於平台業者、應用提供業者、網站營運業者、廣告業者等取得利用者資料之事業者**，在充分把握自身取得的利用者資料以及資料收集模組或標籤等之後，根據取得資料種類或利用目的進行通知、公布或必要時取得同意，以使利用者能夠理解。

2022 © 資訊工業策進會 Institute for Information Industry


2、資通訊領域個資議題(5/5)
英、日、德、美提升電信、新聞規範以加強隱私保護-2
2021.12.20
德國發布《電信—電信媒體—資料保護—法律》指南
德國聯邦與各邦資料保護監督機關會議（DSK）針對電信媒體的供應商發布指引文件，該指引文件係因應同年12月1日修正實施之《電信—電信媒體—資料保護—法律》（Telekommunikation-Telemedien-Datenschutz-Gesetze, TTDSG），協助網際網路、應用程式或智慧型家電供應商符合TTDSG法規要求，包含供應商在終端機存取與儲存之隱私保護要求、cookie或類似追蹤技術的侵害影響程度等，例如必須有明確的隱私預設技術儲存之必要性、儲存時間、檔案類型以及後續資料之處理流程，皆必須符合TTDSG與GDPR內容，並使可能權益受影響的資料主體得更瞭解法規保護面向，以資符合歐盟《電子隱私指令》（ePrivacy Directive, 2002/58/EC）的規範要求。
2022.01.12
美國對電信業客戶專屬網路資訊外洩事件加強通報規範
■ 美國聯邦通訊委員會（Federal Communications Commission，FCC）宣布FCC將針對美國境內電信業者的客戶專屬網路資訊（Customer Proprietary Network Information, CPNI）外洩事件，訂定更嚴格的外洩通知規定。
■ CPNI為美國電信業者在客戶使用電信服務時所蒐集的資訊，例如通話紀錄等等，該公告說明數項電信業者對外洩事件的新通報規定，包括(1)取消外洩事件發生後通知客戶的7天強制等待期；(2)即使是意外的外洩也必須通知客戶；(3)除了向聯邦調查局（FBI）與美國特勤局（U.S. Secret Service）通報外，也必須向FCC通知外洩事件。
stli
16
2022 © 資訊工業策進會 Institute for Information Industry


3、人工智慧或生物識別
stli
17
2022 © 資訊工業策進會 Institute for Information Industry

3、人工智慧或生物識別(1/5)

主題摘要

港、美針對AI運用發布法規或標準指南

- 香港發布《開發及使用人工智能指引》協助業者遵從隱私規定
- 美國紐約市立法禁止雇主使用自動就業決策工具篩選員工

歐、美、韓、澳針對生物識別技術加以規範隱私保護

- 歐洲議會提出臉部辨識及監控行為對隱私侵害問題
- 比利時發布《生物識別資料處理建議》
- 德國禁止公共場所使用臉部辨識系統並限制使用大規模監視工具
- 美國紐約市施行《生物識別技術隱私法》
- 韓國《個人資料技術性和組織性保護標準》修正草案公開徵求意見
- 澳洲公告7-11便利商店臉部辨識系統違法

2022 © 資訊工業策進會 Institute for Information Industry

3、人工智慧或生物識別(2/5)

港、美針對AI運用發布法規或標準指南

2021.08.18 **香港發布《開發及使用人工智能指引》協助業者遵從隱私規定**

香港個人資料隱私專員公署公布《開發及使用人工智能指引》，**要求科技與資料處理業者以尊重、互惠及公平的三種方式對待資料主體**；七項人工智慧的道德原則（問責、人為監督、透明度與可解釋性、數據隱私、公平、有益的人工智慧、可靠、穩健及安全），並且在人工智慧策略及治理、風險評估及人為監督、人工智慧模型開發及系統管理、與資料主體的溝通及交流，俾利香港發展區域性數據樞紐的優勢，並協助香港成為創科中心和世界級的智慧城市。

2021.11.10 **美國紐約市立法禁止雇主使用自動就業決策工具篩選員工**

美國紐約市議會通過法案**禁止雇主與職業介紹所使用自動就業決策工具篩選員工或候選人選，除非在使用該工具之前已進行偏見稽核**。該法將自動就業決策工具定義為任何發布例如分數、分類或建議等輸出的計算過程，包含透過機器學習、統計建模、資料分析或人工智慧，以實際協助或取代對自然人有影響就業決策之人工決策。如果企業不遵守相關規定則每次最高得處以1,500美元之違規罰款。該法預計於2023年1月2日起生效。

2022 © 資訊工業策進會 Institute for Information Industry

3、人工智慧或生物識別(3/5)

歐、美、韓、澳針對生物識別技術加以規範隱私保護-1

2021.10.25 **歐洲議會提出臉部辨識及監控行為對隱私侵害問題**

- 歐洲議會公布「在歐盟成員國內大規模生物識別及大規模監測行為」（Biometric and behavioural mass surveillance in EU Member states）報告。
- 由於臉部辨識屬於GDPR第9條第1項規定之「生物識別資料」範圍，因此屬於特殊種類之個人資料。該報告建議由於監視錄影設備屬於長時間、連續性且密切地監視並紀錄個人之動態資料，對於個人行動自由可能會產生寒蟬效應，多數人會畏懼監視錄影設備之場所及空間；此外，**大規模的監視行為加上事後的臉部辨識系統，若未加以嚴密地控管相關資料洩漏或外流，將對於個人隱私權利產生重大危害**。

2021.12.06 **比利時發布《生物識別資料處理建議》**

- 比利時資料保護主管機關（l 'Autorité de Protection des Données, l' APD）已將生物識別資料作為「2020-2025年戰略計畫」優先事項，並根據計畫制定並發布《生物識別資料處理建議》。在生物認證資料被排他性地保存在設備中的情形，生物認證過程能夠自主地進行而不需透過外部近用，在資料主體的操作下執行等一定條件下，該資料處理在合法依據上該當於私人活動的例外。
- 本建議**針對資安政策提出GDPR所要求組織及技術面有以下的安全管理措施**，如使用最新加密算法將生物識別資料模板進行加密、檢測不當行為、禁止外部近用、保存期間經過後應刪除，而系統及設備、軟體亦應採取適當保護措施。

2022 © 資訊工業策進會 Institute for Information Industry

3、人工智慧或生物識別(4/5)

歐、美、韓、澳針對生物識別技術加以規範隱私保護-2

2021.11.24 **德國禁止公共場所使用臉部辨識系統並限制使用大規模監視工具**

- 德國社會民主黨、綠黨及自由黨三個政黨共同協議，根據「紅綠燈計畫」（Die Ampel steht）承諾將**禁止於公共場所內使用臉部生物辨識系統並限制大規模監視工具使用**。
- 根據該協議內容，三方政黨擬於歐盟層級之上推動臉部辨識之禁止規範，相關禁令規範將於歐盟《人工智慧法》（artificial intelligence Act, AI Act）草案內討論。

2021.07.21 **美國紐約市施行《生物識別技術隱私法》**

- 美國紐約市正式施行《生物識別技術隱私法》（biometric privacy act），主要聚焦於通過**規範非公務機關對生物識別資料的蒐集、儲存、傳輸與利用**，以確保其準確、安全及保護個人隱私。
- 本法規範重點包括：

1. 禁止商業機構將生物識別資料向第三方進行銷售、租賃、交易或共享以換取金錢或其他利益；
2. 當商業機構有蒐集、儲存、共享消費者生物識別資料的情形時，應將資料處理目的揭露予消費者；
3. 提供受侵害之消費者訴訟權與法定賠償請求權，並給予違反揭露義務之業者於接獲消費者通知後有30天補救期間，若屆期未改善，消費者得請求500美元的損害賠償。

2022 © 資訊工業策進會 Institute for Information Industry

3、人工智慧或生物識別(5/5)

歐、美、韓、澳針對生物識別技術加以規範隱私保護-3

2021.08.31 **韓國《個人資料技術性和組織性保護標準》修正案公開徵求意見**

- 韓國個人情報保護委員會公告《個人資料技術性和組織性保護標準》修正草案並公開徵求意見。本次修正擬**調整「生物特徵辨識資料」之定義、蒐集告知，以及加密要求**。
- 本次修正考量將「生物資料」一詞更改為「生物特徵識別資料」以資辨別標準將用以驗證或識別個人為目的，進而進行加密的資料，明確定義為「生物特徵識別資料」，與過去未區分用途而統稱為「生物資料」一詞區分，並將應加密的資料客體，明確地限定在只有「生物特徵識別資料」，而非所有「生物資料」。

2021.10.14 **澳洲公告7-11便利商店臉部辨識系統違法**

- 澳洲資訊委員辦公室（Office of the Australian Information Commissioner, OAIC）宣布，**7-11便利商店在當地進行消費者調查所蒐集參與者的臉部圖像並生成臉部辨識資料，已違反澳洲《1988年聯邦隱私法》**（Privacy Act 1988 (Cth)）。
- 調查發現，通過7-11客戶反饋機制大規模蒐集敏感的生物識別資料對於了解和改善客戶的店內體驗並非合理且必要的。7-11便利商店此舉已過度蒐集對其功能沒有合理必要的敏感生物識別資料，從而侵害了客戶的隱私，OAIC已責令7-11終止此專案並銷毀已蒐集之圖檔及資料。

2022 © 資訊工業策進會 Institute for Information Industry

4、COVID-19因應措施

2022 © 資訊工業策進會 Institute for Information Industry

4、COVID-19因應措施(1/3)

主題摘要

英國強調疫苗接種檢查計畫、NHS測試追蹤系統隱私保護

- 英國發表聲明強制疫苗接種計畫符合《英國資料保護法》
- 英國發布《COVID-19檢驗之個資保護指南》
- 英國發布「NHS測試和追蹤建議」

德國建議監管疫苗接種登記、強化職場防疫資料保護

- 德國針對COVID-19疫苗接種資料建議採取全國性監管措施
- 德國對於工作場所內提供3G文件要求雇主應加強隱私保護
- 德國建議COVID-19疫苗接種登記應符合資料保護規定

2022 © 資訊工業策進會 Institute for Information Industry

4、COVID-19因應措施(2/3)

英國強調疫苗接種檢查計畫、NHS測試追蹤系統隱私保護

2021.09.29 英國發表聲明強制疫苗接種計畫符合《英國資料保護法》

英國資訊委員辦公室（ICO）針對蘇格蘭和威爾斯強制疫苗接種和 COVID 狀態檢查計畫發表聲明，其內容提到將由英國政府決定是否、如何引入強制疫苗接種和新冠肺炎檢查計畫且**確信其不會因《英國資料保護法》而受阻**。

2021.12.15 英國發布《COVID-19檢驗之個資保護指南》

英國資訊委員辦公室（ICO）**針對檢驗組織相關個資保護規範發布指南**：(1)進行檢驗前，檢驗單位必須清楚說明其即將如何處理個人資料；(2)進行檢驗時，必須使用官方政府應用程式且參考「疫苗接種和COVID狀態檢查指南」；(3)完成檢驗後，要依據ICO的COVID-19 hub獲取即時更新資料保護建議。

2021.12.21 英國發布「NHS測試和追蹤建議」

英國資訊委員辦公室（ICO）針對英國國家健保局之防疫測試和追蹤系統發布「NHS測試和追蹤建議」，以加強對民眾之個人資料保護，包括：(1)擴大NHS 測試和追蹤的**員工培訓**計畫，包括為不同職位特別設計的課程；(2)訂立額外的流程，並向員工**傳達政策**；(3)增加**審查機制**，例如定期審查和監控契約，以確保員工和第三方遵循協議中的流程。

2022 © 資訊工業策進會 Institute for Information Industry

4、COVID-19因應措施(3/3)

德國建議監管疫苗接種登記、強化職場防疫資料保護

2021.08.31 **德國針對COVID-19疫苗接種資料建議採取全國性監管措施**

德國聯邦個人資料保護與資訊自由委員會（BfDI）針對國內企業為避免群聚案例或造成防疫破口，要求員工或應徵者提供COVID-19疫苗接種紀錄及檢測結果，**由於涉及資料主體之高度敏感性個人資料，建議立法者應採取全國性的監管策略及管制措施**。

2021.11.22 **德國對於工作場所內提供3G文件要求雇主應加強隱私保護**

德國聯邦個人資料保護暨資訊自由委員會（BfDI）認為**受僱人提供3G文件（已接種證明、已康復證明或已檢測為陰性證明）並無具體保護措施**，為避免相關證明文件被不當使用，雇主得透過可驗證流程檢查或運用Corona應用程式方式予以追蹤，對員工隱私更有保障。

2022.01.04 **德國建議COVID-19疫苗接種登記應符合資料保護規定**

德國資料保護協會（DVD）針對聯邦政府提出COVID-19預防接種登記之強制控制措施，指出**應合於資料保護法規之預先設計**，例如透過法律或授權命令之合法性基礎，建立COVID-19疫苗接種登記平台，由各邦政府的衛生局進行登記，並得以串連德國各邦政府的接種資訊且只能用於特定目的，相關施打資訊委託予醫療專業人員予以管理，亦應與相關從業人員簽署保密協議，以取得社會人民的信任及維護資料主體之隱私權利。

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(1/6)

主題摘要

美國個資保護成效佳，各項網路個資爭議有進展

- 美國加州公布《加州消費者隱私法》首年執法情形
- 美國禁止SpyFone從事監控業務並命令刪除資料及通知
- 美國墨西哥州針對保護兒童隱私爭議與Google和解

歐盟資料保護主管機關遭批評成效不彰

- 愛爾蘭資料保護委員會遭批成效最低GDPR監管機關
- 歐盟執委會遭訴行政管理不善及未監督主管機關實施GDPR

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(2/6)

主題摘要

歐洲各國個資主管機關對科技巨頭提出裁罰

- 德國認為FB智慧眼鏡產品違法而無法於德國上市
- 愛爾蘭資料保護委員會發布FB裁罰被評為嚴重輕判
- 愛爾蘭資料保護委員會裁罰Twitter未及時個資事故通知
- 奧地利裁定使用Google Analytics cookies違反GDPR
- 法國因Google及FB未提供輕易拒絕Cookie判處鉅額罰款
- 歐盟執委會要求WhatsApp對隱私政策內容提出說明

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(3/6)

美國個資保護成效佳，各項網路個資爭議有進展

2021.07.19 **美國加州公布《加州消費者隱私法》首年執法情形**

美國加州檢察長Rob Bonta公布《加州消費者隱私法》（The California Consumer Privacy Act, CCPA）首年執法情形，**認為相關執法非常成功並促使更多加州人民行使其權利**。加州檢察長表示在收到違法的通知後，75%的企業在30天法定期間內遵守相關規定，其餘25%則是屬於調查中或尚在30天期間內。

2021.09.01 **美國禁止SpyFone從事監控業務並命令刪除資料及通知**

美國聯邦貿易委員會（FTC）禁止SpyFone從事監視業務與命令公司刪除相關資料，該追蹤軟體應用程式公司透過駭客設備，秘密取得與分享個人活動、手機使用與網路活動的資料，並出售追蹤軟體應用程式。**SpyFone缺乏基本安全措施**（例如沒有對儲存的照片與訊息等個人資料進行加密），FTC除了**禁止該公司從事監控業務**之外，還命令該公司**刪除所有非法取得資料**，並**通知設備所有者**該應用程式已被秘密安裝。

2021.12.14 **美國墨西哥州針對保護兒童隱私爭議與Google和解**

先前Google遭指控違反美國關於兒童網路隱私法律，**新墨西哥州檢察日前與Google就兒童隱私訴訟達成和解**，相關案件涉及《兒童網路隱私保護法》（COPPA），該協議將撥出數百萬美元，用於全新墨西哥州兒童，促進教育、隱私與安全。

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(4/6)

歐盟資料保護主管機關遭批評成效不彰

2021.09.13 **愛爾蘭資料保護委員會遭批成效最低GDPR監管機關**

愛爾蘭公民自由委員會（Irish Council for Civil Liberties, ICCL）表示愛爾蘭資料保護委員會（Ireland’s Data Protection Commission, DPC）是GDPR執法成效最低落監管機關。**由於跨國科技業歐盟主要據點都設於愛爾蘭，DPC是歐盟主要監管機關，其判決引領、影響其他監管機關之判決**。但愛爾蘭資料保護委員會**執法效率緩慢**，2020年愛爾蘭資料保護委員會**有98%申訴案件尚未處理**。而西班牙隱私保護委員會相比愛爾蘭資料保護委員會經費缺乏，但受理案件速度比愛爾蘭資料保護委員會快10倍。

2021.11.29 **歐盟執委會遭訴行政管理不善及未監督主管機關實施GDPR**

- 愛爾蘭公民自由委員會（ICCL）正式向歐盟監察使（European Ombudsman, EO）提出申訴，表示歐盟執委會未確實監管GDPR之實施，申訴主要分為兩部分：**(1)未建立一套監管機制定期追蹤GDPR實施之狀況。(2)未對愛爾蘭資料保護委員會（DPC）未確實實施GDPR一事進行懲罰**。
- ICCL表示，EC至今未採取調查行動，亦未對愛爾蘭啟動侵權程序（infringement procedure）。其他歐盟監管機關先前也對DPC未盡其義務提出抗議。EO表示會審核本申訴案，決定是否展開調查。歐盟資料保護監督機關（European Data Protection Supervisor）亦安排於2022年6月舉辦會議討論GDPR執法架構之重整。

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(5/6)

歐洲各國個資主管機關對科技巨頭提出裁罰-1

2021.09.10 德國認為FB智慧眼鏡產品違法而無法於德國上市

FB於各國上市Ray-Ban Stories智慧型眼鏡配置鏡頭，讓用戶拍照或錄影並透過影像應用程式編輯分享。依據《聯邦資料保護法》第4條規定，拍攝行為涉及蒐集他人個資，**而拍攝人必須取得被拍攝人同意，且隨身攜帶並發放告知拍攝行為的通知文件**，始得合法進行拍攝

2021.10.18 愛爾蘭資料保護委員會發布FB裁罰被評為嚴重輕判

愛爾蘭資料保護委員會公布將對FB裁罰2,800萬至3,600萬歐元（約9億至11億元新台幣）但業界普遍認為愛爾蘭資料保護委員會嚴重輕判，**僅判FB應更加透明化處理使用者之個人資料，沒有以保護當事人權利為主**，放任科技巨頭規避GDPR。

2021.10.18 愛爾蘭資料保護委員會裁罰Twitter未及時個資事故通知

- 愛爾蘭資料保護委員會公布針對Twitter違反GDPR一案已受都柏林巡迴法院（Dublin Circuit Court）判決同意，確定對Twitter祭出45萬歐元（約1,450萬元新台幣）罰鍰。
- 2019年1月，愛爾蘭資料保護委員會收到Twitter個資事故通知，事故事實為如Twitter保護帳號使用者在安卓系統上使用Twitter變更其電子郵件，使用者帳號會失去保護。針對**Twitter的個資事故通知方式部分，認為Twitter通知速度緩慢以及通知內容不足**，因此以違反GDPR第33條第1項、第33條第5項規定對Twitter進行罰鍰。

stli

2022 © 資訊工業策進會 Institute for Information Industry

5、裁罰實務案例(6/6)

歐洲各國個資主管機關對科技巨頭提出裁罰-2

2021.12.22 奧地利裁定使用Google Analytics cookies違反GDPR

奧地利隱私主管機關裁定奧地利一間網路服務供應商使用Google Analytics cookies之行為，違反GDPR第5章國際傳輸條款。該公司與Google之間有簽訂標準契約條款，但是奧地利隱私主管機關判定**該標準契約條款以及補充措施不足以符合GDPR及Schrems II要求**

2022.01.06 法國因Google及FB未提供輕易拒絕cookies判處鉅額罰款

法國國家資訊自由委員會（CNIL）裁罰決定，由於Google.fr、Youtube.com及Facebook.com讓使用者只透過一個按鍵就能接受所有的Cookie，而**當使用者要拒絕這些Cookie時，卻需要好幾個按鍵才能拒絕所有的Cookie進而影響同意自由**，違反《法國資料保護法》第82條規定，分別向Google及臉書判處1.5億歐元及6,000萬歐元的罰款。

2022.01.27 歐盟執委會要求WhatsApp對隱私政策內容提出說明

歐盟執委會已發函要求WhatsApp對2021版本的服務條款及隱私政策內容提出說明，並且說明是否符合歐盟消費者保護法，包含GDPR。**WhatsApp必須確保消費者清楚了解他們同意接受哪些條款以及個人資料如何被運用**，WhatsApp應於2022年2月底之前提供回覆與EC開啟正式對話。

stli

2022 © 資訊工業策進會 Institute for Information Industry

6、GDPR適足性認定

2022 © 資訊工業策進會 Institute for Information Industry

6、GDPR適足性認定(1/2)

主題摘要

韓國通過歐盟GDPR適足性認定

- 歐盟執委會與韓國發布聯合聲明表示完成適足性認定初步談判
- 歐洲資料保護委員會公布韓國適足性認定草案之意見
- 韓國正式通過GDPR適足性認定

2022 © 資訊工業策進會 Institute for Information Industry

6、GDPR適足性認定(2/2)

韓國通過歐盟GDPR適足性認定

2021.03.31 **歐盟執委會與韓國發布聯合聲明表示完成適足性認定初步談判**

歐盟初步認定韓國對於個人資料保護水準與歐盟GDPR相當，**有望成為繼日本之後，東亞第二個通過歐盟適足性認定的國家**。雙方皆認為韓國取得適足性認定將會深化雙邊貿易並開啟更多商業機會，雙方民間企業及公務機關間資料流動性皆可藉由適足性認定顯著提升。

2021.09.24 **歐洲資料保護委員會公布韓國適足性認定草案之意見**

歐洲資料保護委員表示**韓國個人資料保護法體系與歐盟個人資料保護法體系相比達到與歐盟相似的保護效果**（essentially equivalent），並建議韓國適足性認定最終的判決中應載明韓國執法或情報公務單位在何種情形下可以依國家安全目的再處理資料（onward transfers）並應受哪些限制。

2021.12.17 **韓國正式通過GDPR適足性認定**

本次適足性認定範圍**排除韓國因宗教活動、政黨提名候選人處理之個人資料，以及金融機構信用資料傳輸的適用**，因歐盟認為韓國金融委員會作為信用資料的監管機關專責不足，仍需透過標準契約條款（SCC）進行國際傳輸。另外，本次談判僅涉及歐盟人民個人資料移轉至韓國國內，因此韓國針對PIPA提出第二次修正案，其中也包括適足性制度相關條文。

2022 © 資訊工業策進會 Institute for Information Industry

7、國際傳輸

2022 © 資訊工業策進會 Institute for Information Industry

7、國際傳輸(1/3)

主題摘要

英國因應國際資料傳輸協議加強跨境傳輸規範

- 英國針對國際資料傳輸協議及個資跨境傳輸指引修正草案公開徵詢意見
- 英國公布UK GDPR認證方案幫助企業遵循UK GDPR規定
- 英國回應國際資料傳輸協議聲明以支持英國數位經濟政策

中國大陸公布子法、美國簽訂資料流通協議

- 中國大陸《數據出境安全評估辦法》公開徵詢意見
- 美國與澳洲針對重大犯罪取得境外資料簽訂跨境資料流通協議

2022 © 資訊工業策進會 Institute for Information Industry

7、國際傳輸(2/3)

英國因應國際資料傳輸協議加強跨境傳輸規範

2021.08.11 **英國針對國際資料傳輸協議及個資跨境傳輸指引修正草案公開徵詢意見**

英國資訊委員辦公室（ICO）指出**國際資料傳輸協議**（International Data Transfer Agreement, IDTA）**將取代英國現行採用的歐盟標準契約條款**（SCC），成為英國確保跨境傳輸資料保護品質的契約工具，並要求組織在沒有充分決定的情況下將英國以外的個人資料傳輸到其他國家時應盡之職責。

2021.08.19 **英國公布UK GDPR認證方案幫助企業遵循UK GDPR規定**

英國資訊委員辦公室（ICO）公布已審核通過**英國三部UK GDPR認證方案**（certification scheme），推行認證主要是**協助組織確實落實UK GDPR法遵**，進而提升消費者對其產品或服務之信任。

2022.02.02 **英國回應國際資料傳輸協議聲明以支持英國數位經濟政策**

英國資訊委員辦公室（ICO）回應文化、媒體和體育部（DCMS）制定國際資料傳輸協議（IDTA）聲明、歐盟執委會國際資料傳輸附錄（Addendum），**幫助確保個人資料從英國轉移至未通過適足性認定國家時，組織有能夠使用IDTA或附錄作為資料傳輸工具。**

2022 © 資訊工業策進會 Institute for Information Industry

7、國際傳輸(3/3)

中國大陸公布子法、美國簽訂資料流通協議

2021.10.29

中國大陸《數據出境安全評估辦法》公開徵詢意見

- 中國大陸國家互聯網資訊辦公室《數據出境安全評估辦法》公開徵詢意見，特別針對資料跨境傳輸做進一步規範。本辦法規範個人資料或重要資料**在跨境傳輸資料前，組織應完成兩項審查—自評及資料出境安全評估**。
- 下列事項為進行資料出境安全評估時，國家網信部門會考慮之項目：資料傳輸之合法性及必要性、第三國之個資法體系、資料量、資料種類、資料敏感度、個資事故之風險、資料當事人之權利及利益是否被保障、跨境傳輸契約之完整性等。

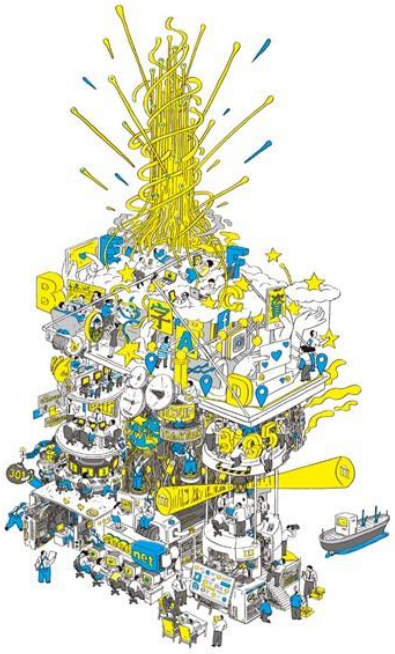
2021.12.15

美國與澳洲針對重大犯罪取得境外資料簽訂跨境資料流通協議

- 美國依據其於2018年通過之《釐清境外合法利用資料法》（Clarifying Lawful Overseas Use of Data Act，CLOUD Act）與澳洲簽訂協議，**以利雙方針對重大刑案向通訊服務提供者取得境外電子資料**。
- 此協議確保雙方可即時取得電子資料，包括儲存於主流社群媒體等電子資料，以防範、偵測及追溯重大犯罪如兒童性暴力、隨機攻擊、恐怖主義及透過網路破壞重大基礎建設等，協議內容亦同時就美澳共同的隱私權利和公民自由價值妥善保護。

stli

2022 © 資訊工業策進會 Institute for Information Industry



1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13策進 e-Taiwan / m-Taiwan 14精進5G智慧科技創新應用 15支援文創與設計產業奠基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉無線寬頻環境
19協助產業拓展商機並強化資安防護 20數位轉型化育者

THANK YOU

stli

2022 © 資訊工業策進會 Institute for Information Industry

2022 年下半年度國際個資關鍵議題分享會

下半年度國際個資關鍵議題分享會

科技法律研究所

財團法人資訊工業策進會

2022.09.07

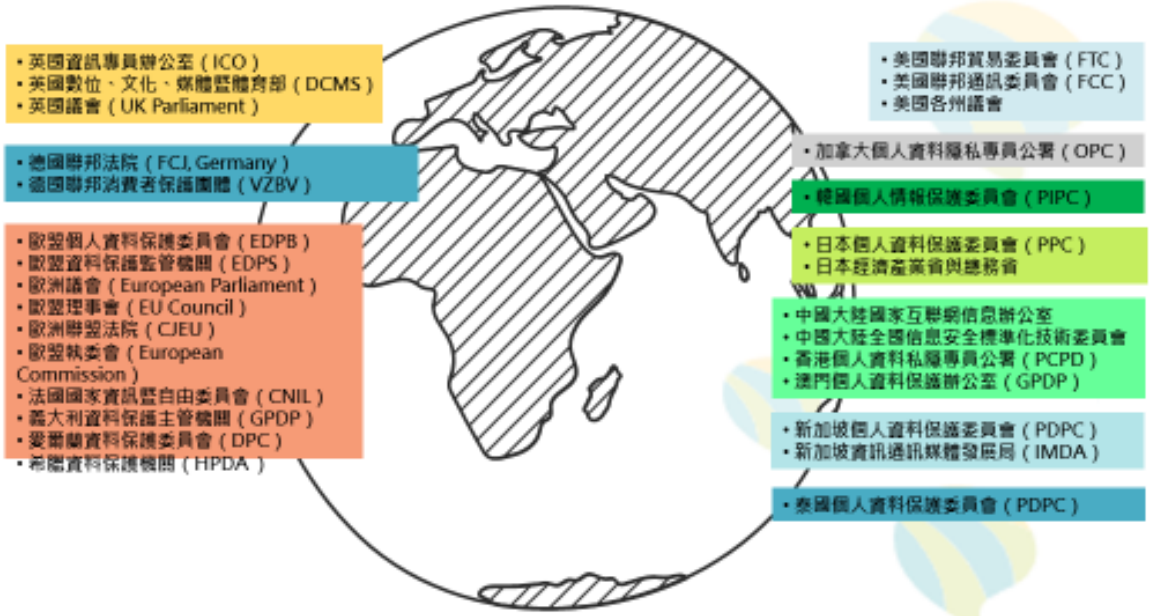
stli 科技法律研究所 SCIENCE & TECHNOLOGY LAW INSTITUTE

資訊工業策進會 Institute for Information Industry

大綱

- 國際個資法制觀測主管機關/單位
- 國際個資法制觀測議題綜覽
  - 1、國際法規動態或實作指南
  - 2、資通訊領域個資議題
  - 3、裁罰實務案例
  - 4、國際傳輸
  - 5、人工智慧或生物識別

國際個資法制觀測主管機關/單位



國際個資法制觀測議題綜覽

1、國際法規動態

1、國際法規動態 (1/7)

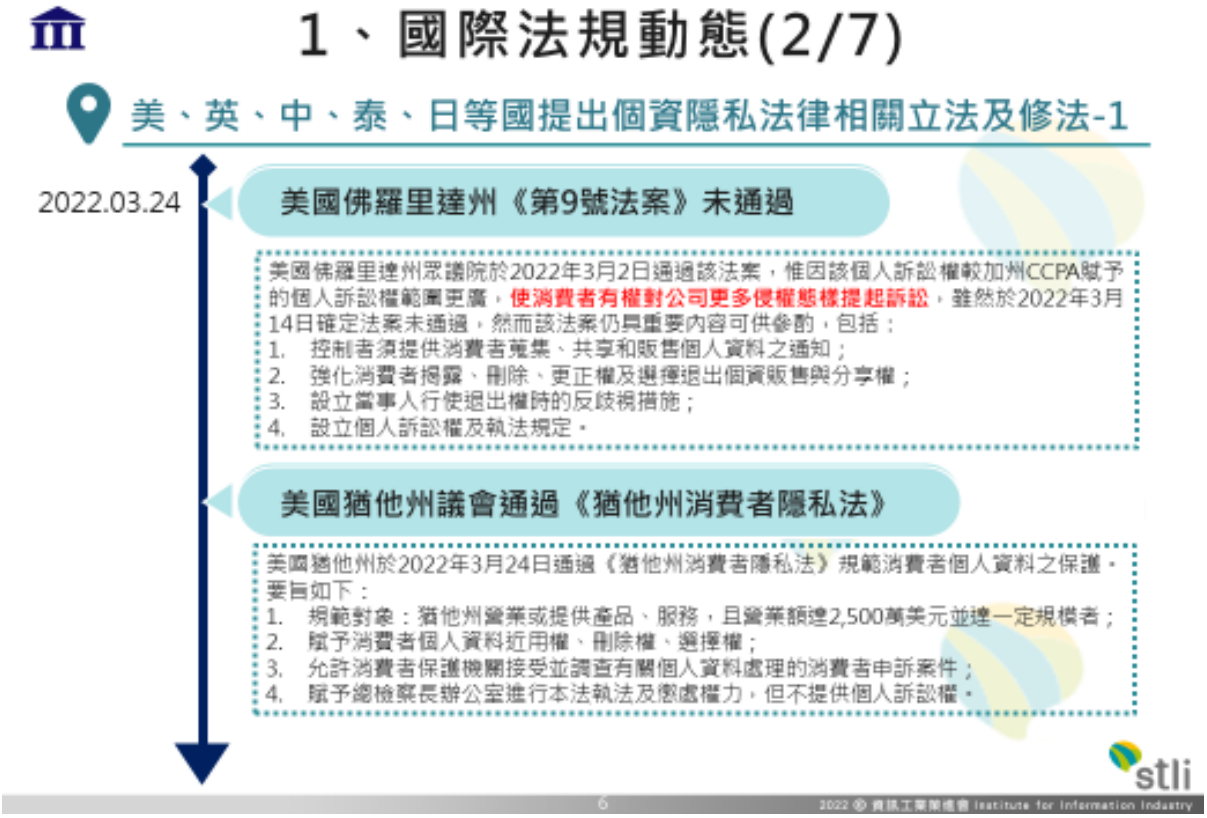
主題摘要

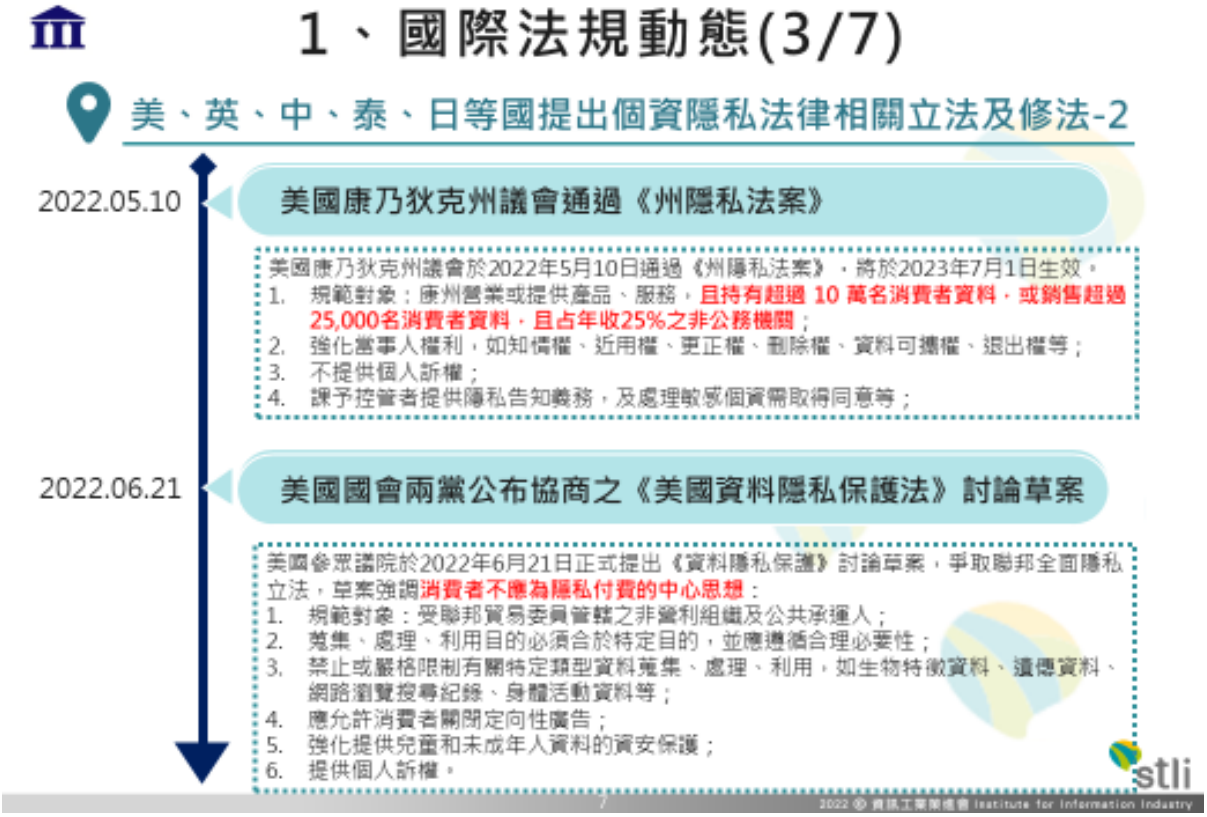
美、英、中、泰、日等國提出個資隱私法律相關立法及修法

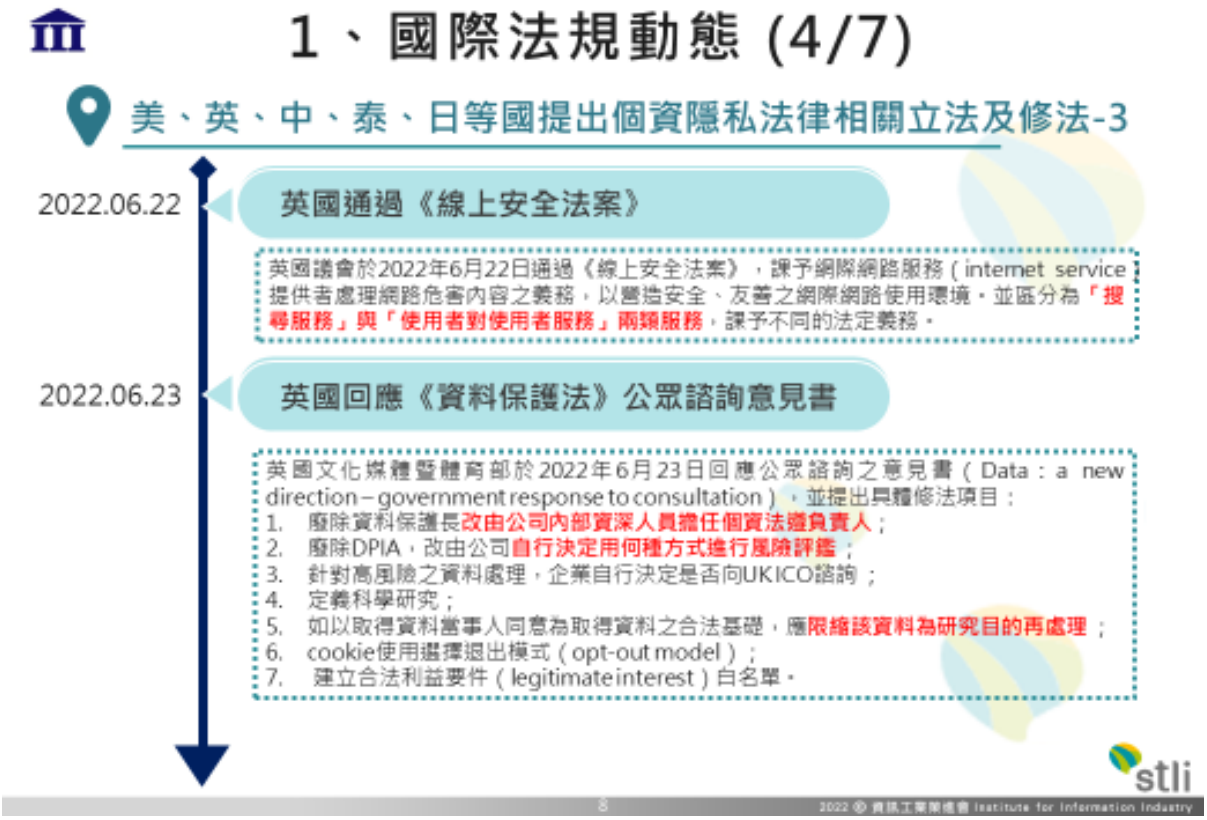
- 美國佛羅里達州《第9號法案》未通過
- 美國猶他州議會通過《猶他州消費者隱私法》
- 美國康乃狄克州議會通過《州隱私法案》
- 美國國會兩黨公布協商之《美國資料隱私保護法》討論草案
- 英國通過《線上安全法案》
- 英國回應《資料保護法》公眾諮詢意見書
- 中國大陸施行《網路安全審查辦法》
- 泰國全面實施《個人資料保護法》
- 日本通過修正《電信事業法》

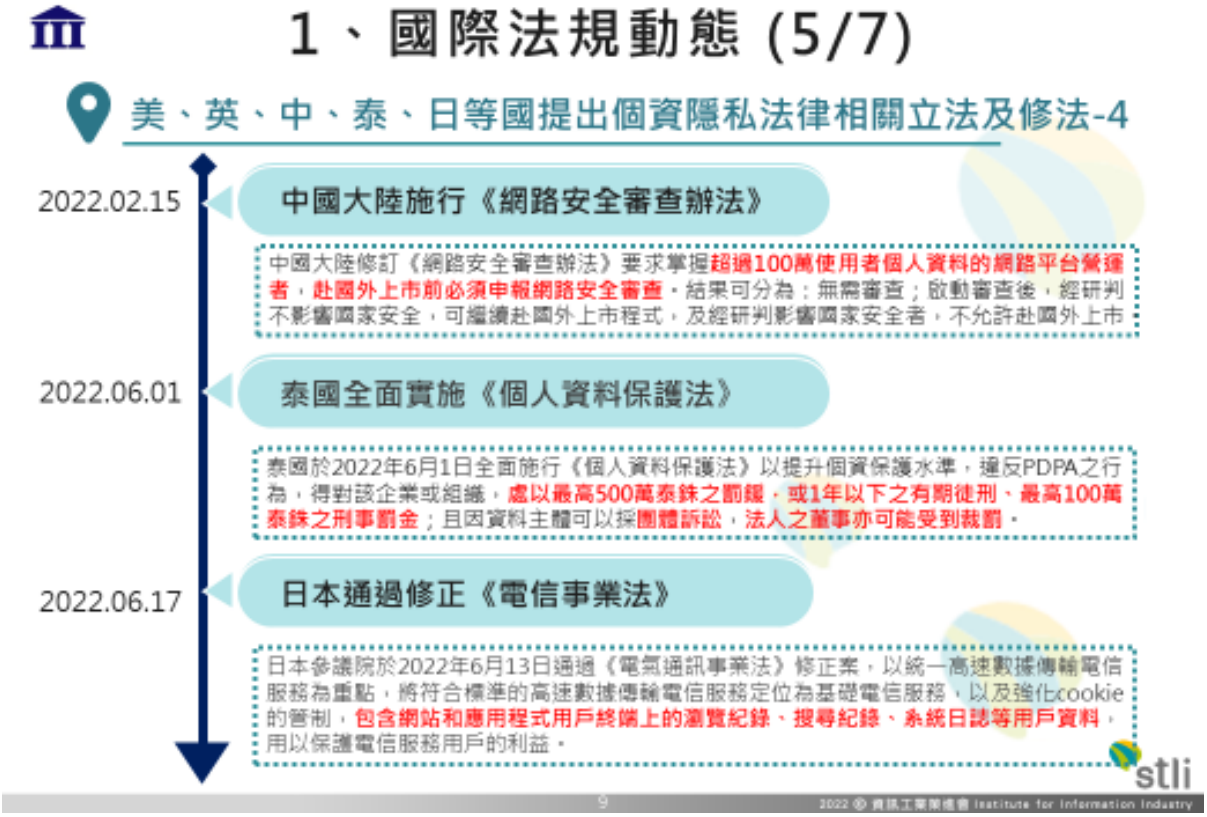
法、歐、美、新針對個資隱私法規發表意見或實作指南

- 法國發布《 GDPR資料保護長實用指南》
- 歐盟《資料治理法》發表共同意見
- 歐洲聯盟法院判決解釋「特殊類型之個人資料」
- 美國加強審查《兒童線上隱私保護法》違規行為
- 美國發布《 HIPAA隱私規則及和生殖健康資訊揭露指南》
- 新加坡發布《基本匿名化指南》

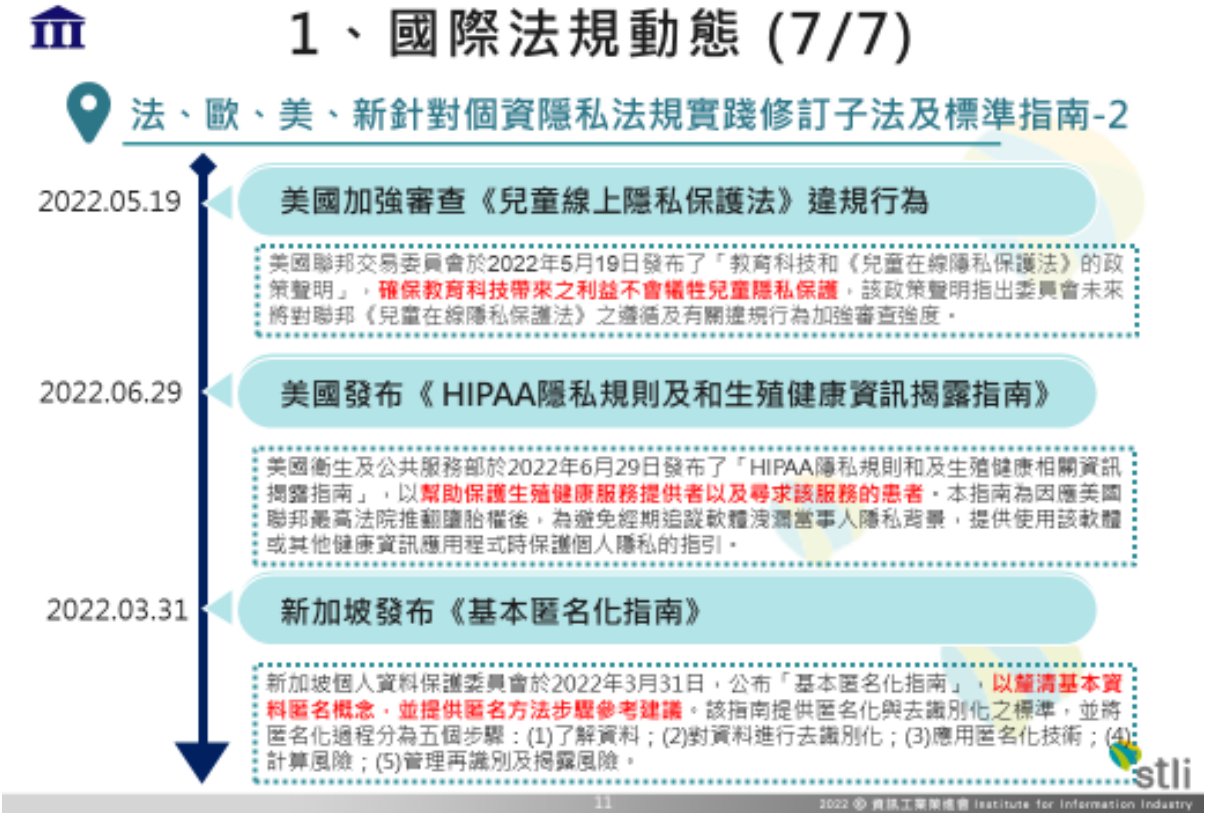

1、國際法規動態(2/7)
美、英、中、泰、日等國提出個資隱私法律相關立法及修法-1
2022.03.24
美國佛羅里達州《第9號法案》未通過
美國佛羅里達州眾議院於2022年3月2日通過該法案，惟因該個人訴訟權較加州CCPA賦予的個人訴訟權範圍更廣，使消費者有權對公司更多侵權態樣提起訴訟，雖然於2022年3月14日確定法案未通過，然而該法案仍具重要內容可供參酌，包括：
1. 控制者須提供消費者蒐集、共享和販售個人資料之通知；
2. 強化消費者揭露、刪除、更正權及選擇退出個資販售與分享權；
3. 設立當事人行使退出權時的反歧視措施；
4. 設立個人訴訟權及執法規定。
美國猶他州議會通過《猶他州消費者隱私法》
美國猶他州於2022年3月24日通過《猶他州消費者隱私法》規範消費者個人資料之保護，要旨如下：
1. 規範對象：猶他州營業或提供產品、服務，且營業額達2,500萬美元並達一定規模者；
2. 賦予消費者個人資料近用權、刪除權、選擇權；
3. 允許消費者保護機關接受並調查有關個人資料處理的消費者申訴案件；
4. 賦予總檢察長辦公室進行本法執法及懲處權力，但不提供個人訴訟權。
stli
6
2022 資訊工業策進會 Institute for Information Industry


1、國際法規動態(3/7)
美、英、中、泰、日等國提出個資隱私法律相關立法及修法-2
2022.05.10
美國康乃狄克州議會通過《州隱私法案》
美國康乃狄克州議會於2022年5月10日通過《州隱私法案》，將於2023年7月1日生效。
1. 規範對象：康州營業或提供產品、服務，且持有超過 10 萬名消費者資料，或銷售超過25,000名消費者資料，且占年收25%之非公務機關；
2. 強化當事人權利，如知情權、近用權、更正權、刪除權、資料可攜權、退出權等；
3. 不提供個人訴權；
4. 課予控管者提供隱私告知義務，及處理敏感個資需取得同意等；
2022.06.21
美國國會兩黨公布協商之《美國資料隱私保護法》討論草案
美國參眾議院於2022年6月21日正式提出《資料隱私保護》討論草案，爭取聯邦全面隱私立法，草案強調消費者不應為隱私付費的中心思想：
1. 規範對象：受聯邦貿易委員會轄之非營利組織及公共承運人；
2. 蒐集、處理、利用目的必須合於特定目的，並應遵循合理必要性；
3. 禁止或嚴格限制有關特定類型資料蒐集、處理、利用，如生物特徵資料、遺傳資料、網路瀏覽搜尋紀錄、身體活動資料等；
4. 應允許消費者關閉定向性廣告；
5. 強化提供兒童和未成年人資料的資安保護；
6. 提供個人訴權。
stli
7
2022 資訊工業策進會 Institute for Information Industry


1、國際法規動態 (4/7)
美、英、中、泰、日等國提出個資隱私法律相關立法及修法-3
2022.06.22
英國通過《線上安全法案》
英國議會於2022年6月22日通過《線上安全法案》，課予網際網路服務（internet service提供者處理網路危害內容之義務，以營造安全、友善之網際網路使用環境，並區分為「搜尋服務」與「使用者對使用者服務」兩類服務，課予不同的法定義務。
2022.06.23
英國回應《資料保護法》公眾諮詢意見書
英國文化媒體暨體育部於2022年6月23日回應公眾諮詢之意見書（Data：a new direction－government response to consultation），並提出具體修法項目：
1. 廢除資料保護長改由公司內部資深人員擔任個資法遵負責人；
2. 廢除DPIA，改由公司自行決定用何種方式進行風險評鑑；
3. 針對高風險之資料處理，企業自行決定是否向UKICO諮詢；
4. 定義科學研究；
5. 如以取得資料當事人同意為取得資料之合法基礎，應限縮該資料為研究目的再處理；
6. cookie使用選擇退出模式（opt-out model）；
7. 建立合法利益要件（legitimate interest）白名單。
stli
8
2022 資訊工業策進會 Institute for Information Industry


1、國際法規動態 (5/7)
美、英、中、泰、日等國提出個資隱私法律相關立法及修法-4
2022.02.15
中國大陸施行《網路安全審查辦法》
中國大陸修訂《網路安全審查辦法》要求掌握超過100萬使用者個人資料的網路平台營運者，赴國外上市前必須申報網路安全審查，結果可分為：無需審查；啟動審查後，經研判不影響國家安全，可繼續赴國外上市程式，及經研判影響國家安全者，不允許赴國外上市
2022.06.01
泰國全面實施《個人資料保護法》
泰國於2022年6月1日全面施行《個人資料保護法》以提升個資保護水準，違反PDPA之行為，得對該企業或組織，處以最高500萬泰銖之罰鍰，或1年以下之有期徒刑、最高100萬泰銖之刑事罰金；且因資料主體可以採團體訴訟，法人之董事亦可能受到裁罰。
2022.06.17
日本通過修正《電信事業法》
日本參議院於2022年6月13日通過《電氣通訊事業法》修正案，以統一高速數據傳輸電信服務為重點，將符合標準的高速數據傳輸電信服務定位為基礎電信服務，以及強化cookie的管制，包含網站和應用程式用戶終端上的瀏覽紀錄、搜尋紀錄、系統日誌等用戶資料，用以保護電信服務用戶的利益。
stli
9
2022 資訊工業策進會 Institute for Information Industry

1、國際法規動態 (6/7)
法、歐、美、新針對個資隱私法規實踐修訂子法及標準指南-1
2022.03.16
法國發布《GDPR資料保護長實用指南》
法國國家資訊自由委員會於2022年3月16日，公布了「GDPR資料保護長實用指南」，該指南是根據三年以來對資料保護長的實際經驗編纂。大致可分為：(1)資料保護長的角色(2)資料保護長的指派(3)資料保護長執行的任務(4)CNIL對資料保護長的支援等主題。
2022.05.04
歐盟EDPS及EDPB針對《資料治理法》發表共同意見
歐盟資料保護監管機關（EDPS）及歐盟資料保護委員會（EDPB）於2022年5月4日針對《資料治理法》，提倡連網裝置的資料共享，並強化相關資料可攜權。重點包括：
1. 當《資料治理法》與GDPR發生衝突時，應以GDPR之規範為優先；
2. 物聯網等設備應以不侵害資料主體隱私的方式設計，包括資料匿名化；
3. 資料利用者為資料主體以外之人，則須對資料的利用作相關的限制；
4. 強化個人資料可攜權之行使；
5. 應嚴格界定公務機關得近用資料的例外情形。
2022.08.01
歐洲聯盟法院判決解釋「特殊類型之個人資料」
歐洲聯盟法院於2022年 8月1日的判決，認為立陶宛政府的倫理委員會要求公職人員於指定的網站上公開涉及有關家庭成員之性取向等個資，為具有間接指向性的「特殊類型之個人資料」，就該資料進行蒐集，將構成GDPR第9條特殊類型之個人資料之處理。
stli
10
2022 資訊工業策進會 Institute for Information Industry


1、國際法規動態 (7/7)
法、歐、美、新針對個資隱私法規實踐修訂子法及標準指南-2
2022.05.19
美國加強審查《兒童線上隱私保護法》違規行為
美國聯邦交易委員會於2022年5月19日發布了「教育科技和《兒童在線隱私保護法》的政策聲明」，確保教育科技帶來之利益不會犧牲兒童隱私保護，該政策聲明指出委員會未來將對聯邦《兒童在線隱私保護法》之遵循及有關違規行為加強審查強度。
2022.06.29
美國發布《HIPAA隱私規則及和生殖健康資訊揭露指南》
美國衛生及公共服務部於2022年6月29日發布了「HIPAA隱私規則和及生殖健康相關資訊揭露指南」，以幫助保護生殖健康服務提供者以及尋求該服務的患者。本指南為因應美國聯邦最高法院推翻墮胎權後，為避免經期追蹤軟體洩漏當事人隱私背景，提供使用該軟體或其他健康資訊應用程式時保護個人隱私的指引。
2022.03.31
新加坡發布《基本匿名化指南》
新加坡個人資料保護委員會於2022年3月31日，公布「基本匿名化指南」，以釐清基本資料匿名概念，並提供匿名方法步驟參考建議。該指南提供匿名化與去識別化之標準，並將匿名化過程分為五個步驟：(1)了解資料；(2)對資料進行去識別化；(3)應用匿名化技術；(4)計算風險；(5)管理再識別及揭露風險。
stli
11
2022 資訊工業策進會 Institute for Information Industry

2、資通訊領域個資議題

2、資通訊領域個資議題(1/4)

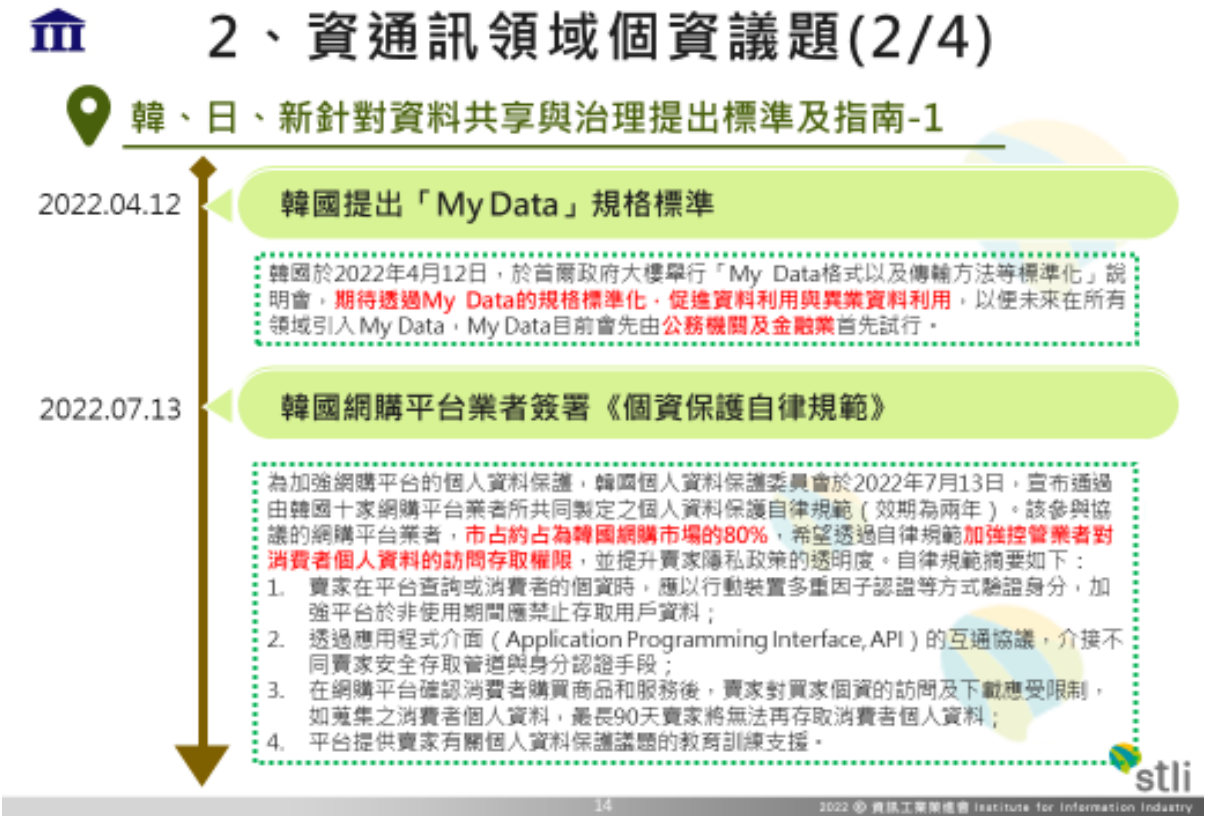
主題摘要

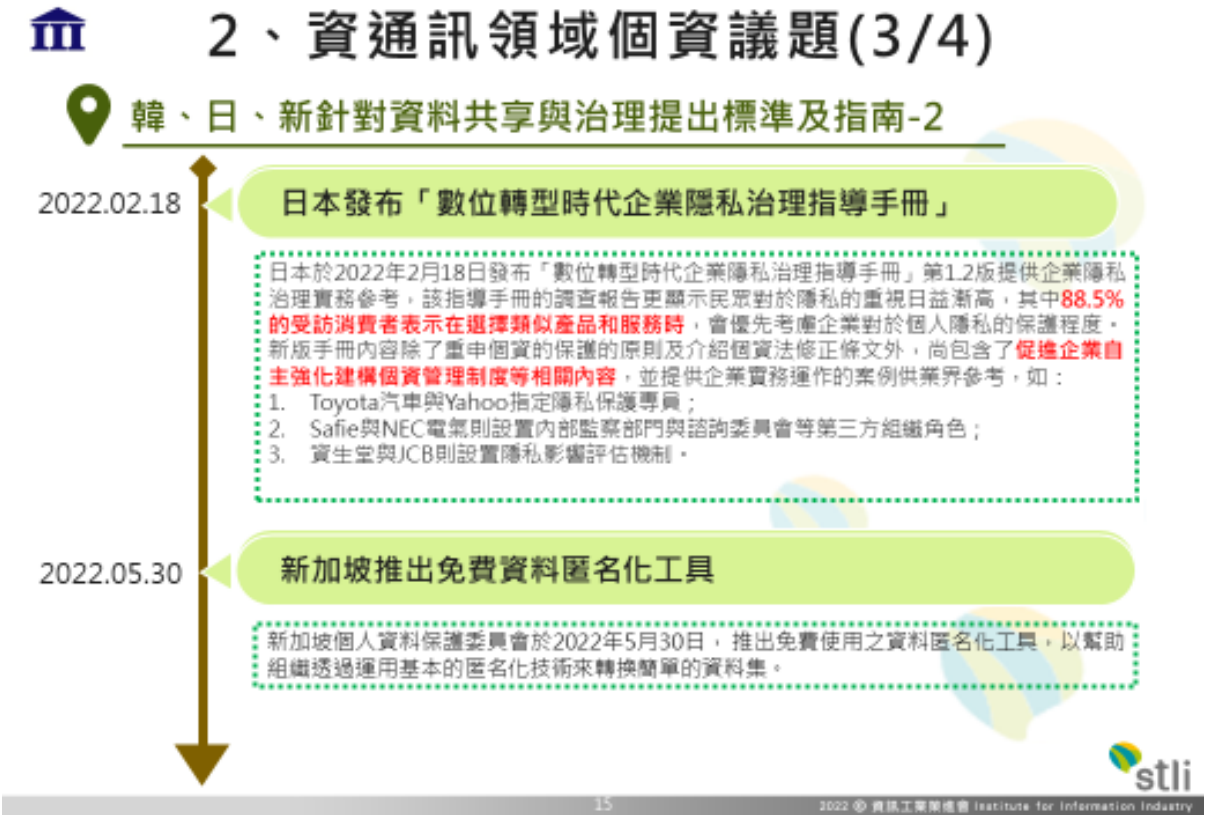
韓、日、新針對資料共享與治理提出標準及指南

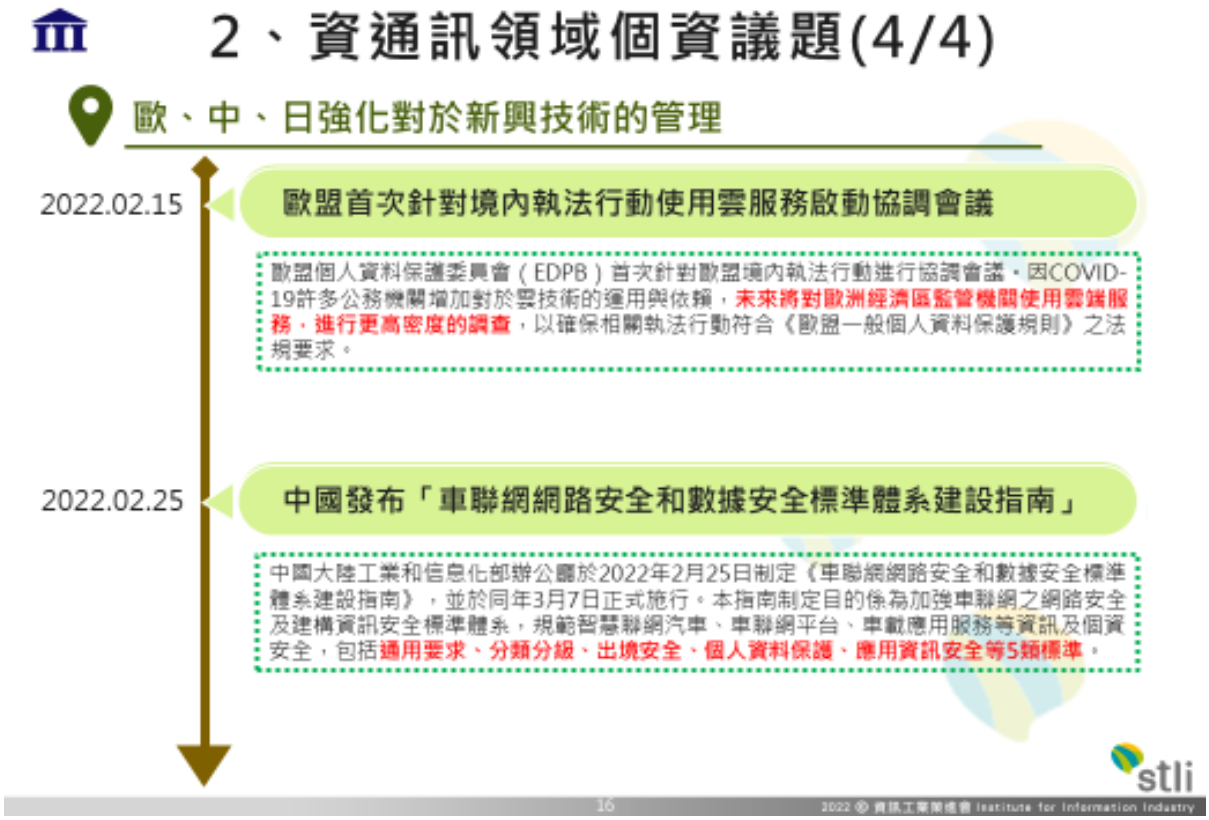
- 韓國提出「My Data」規格標準
- 韓國網購平台業者簽署《個資保護自律規範》
- 日本發布「數位轉型時代企業隱私治理指導手冊」
- 新加坡推出免費資料匿名化工具

歐、中、日強化對於新興技術的管理

- 歐盟首次針對境內執法行動使用雲服務啟動協調會議
- 中國發布「車聯網網路安全和數據安全標準體系建設指南」


2、資通訊領域個資議題(2/4)
韓、日、新針對資料共享與治理提出標準及指南-1
2022.04.12
韓國提出「My Data」規格標準
韓國於2022年4月12日，於首爾政府大樓舉行「My Data格式以及傳輸方法等標準化」說明會，期待透過My Data的規格標準化，促進資料利用與異業資料利用，以便未來在所有領域引入My Data，My Data目前會先由公務機關及金融業首先試行。
2022.07.13
韓國網購平台業者簽署《個資保護自律規範》
為加強網購平台的個人資料保護，韓國個人資料保護委員會於2022年7月13日，宣布通過由韓國十家網購平台業者所共同製定之個人資料保護自律規範（效期為兩年），該參與協議的網購平台業者，市占約占為韓國網購市場的80%，希望透過自律規範加強控管業者對消費者個人資料的訪問存取權限，並提升賣家隱私政策的透明度。自律規範摘要如下：
1. 賣家在平台查詢或消費者的個資時，應以行動裝置多重因子認證等方式驗證身分，加強平台於非使用期間應禁止存取用戶資料；
2. 透過應用程式介面（Application Programming Interface, API）的互通協議，介接不同賣家安全存取管道與身分認證手段；
3. 在網購平台確認消費者購買商品和服務後，賣家對買家個資的訪問及下載應受限制，如蒐集之消費者個人資料，最長90天賣家將無法再存取消費者個人資料；
4. 平台提供賣家有關個人資料保護議題的教育訓練支援。
stli
14
2022 資訊工業策進會 Institute for Information Industry


2、資通訊領域個資議題(3/4)
韓、日、新針對資料共享與治理提出標準及指南-2
2022.02.18
日本發布「數位轉型時代企業隱私治理指導手冊」
日本於2022年2月18日發布「數位轉型時代企業隱私治理指導手冊」第1.2版提供企業隱私治理實務參考，該指導手冊的調查報告更顯示民眾對於隱私的重視日益漸高，其中88.5%的受訪消費者表示在選擇類似產品和服務時，會優先考慮企業對於個人隱私的保護程度。新版手冊內容除了重申個資的保護的原則及介紹個資法修正條文外，尚包含了促進企業自主強化建構個資管理制度等相關內容，並提供企業實務運作的案例供業界參考，如：
1. Toyota汽車與Yahoo指定隱私保護專員；
2. Safie與NEC電氣則設置內部監察部門與諮詢委員會等第三方組織角色；
3. 資生堂與JCB則設置隱私影響評估機制。
2022.05.30
新加坡推出免費資料匿名化工具
新加坡個人資料保護委員會於2022年5月30日，推出免費使用之資料匿名化工具，以幫助組織透過運用基本的匿名化技術來轉換簡單的資料集。
stli
15
2022 資訊工業策進會 Institute for Information Industry


2、資通訊領域個資議題(4/4)
歐、中、日強化對於新興技術的管理
2022.02.15
歐盟首次針對境內執法行動使用雲服務啟動協調會議
歐盟個人資料保護委員會（EDPB）首次針對歐盟境內執法行動進行協調會議，因COVID-19許多公務機關增加對於雲技術的運用與依賴，未來將對歐洲經濟區監管機關使用雲端服務，進行更高密度的調查，以確保相關執法行動符合《歐盟一般個人資料保護規則》之法規要求。
2022.02.25
中國發布「車聯網網路安全和數據安全標準體系建設指南」
中國大陸工業和信息化部辦公廳於2022年2月25日制定《車聯網網路安全和數據安全標準體系建設指南》，並於同年3月7日正式施行。本指南制定目的係為加強車聯網之網路安全及建構資訊安全標準體系，規範智慧聯網汽車、車聯網平台、車載應用服務等資訊及個資安全，包括通用要求、分類分級、出境安全、個人資料保護、應用資訊安全等5類標準。
stli
16

3、裁罰實務案例
stli
17

3、裁罰實務案例(1/5)

主題摘要

歐、美企業遭裁罰主因資料處理法定依據不足

- 2021年度歐盟GDPR裁罰首要原因為資料處理未有足夠法依據
- GDPR裁罰金額及案件數量逐年成長
- Clearview AI先後遭義大利及希臘裁罰
- Google Analytics先後遭義大利、奧地利、法國公布違反GDPR規定
- Tiktok遭歐盟及美國挑戰其蒐集、處理、利用資料之合法性

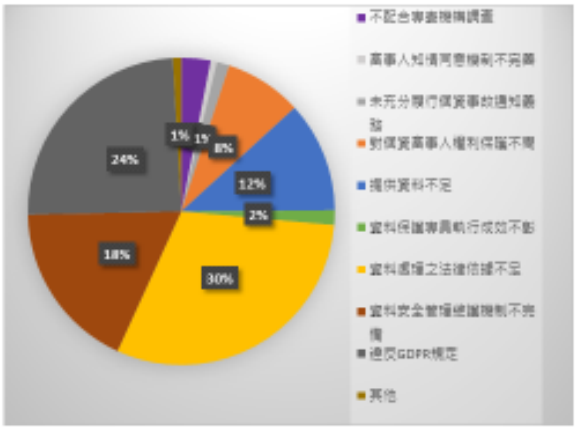
歐、韓國強化個資保護力度及執法成效

- 歐盟法院判決消費者保護團體具有訴權
- 歐盟發布「GDPR行政罰款計算指南」統一罰款標準
- 韓國要求OTT服務商改善消費者退出機制
- 韓國個人資料保護委員會公布2021年爭議案件統計情況

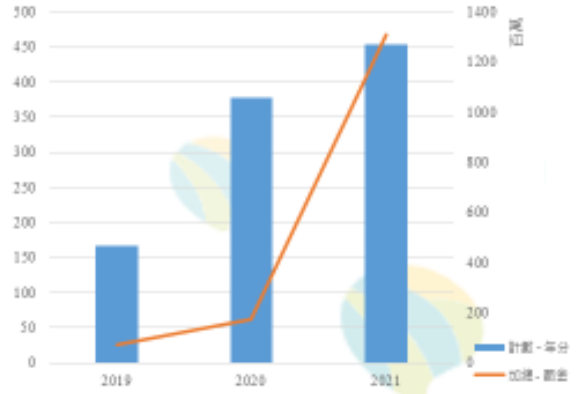
3、裁罰實務案例(2/5)

趨勢分析

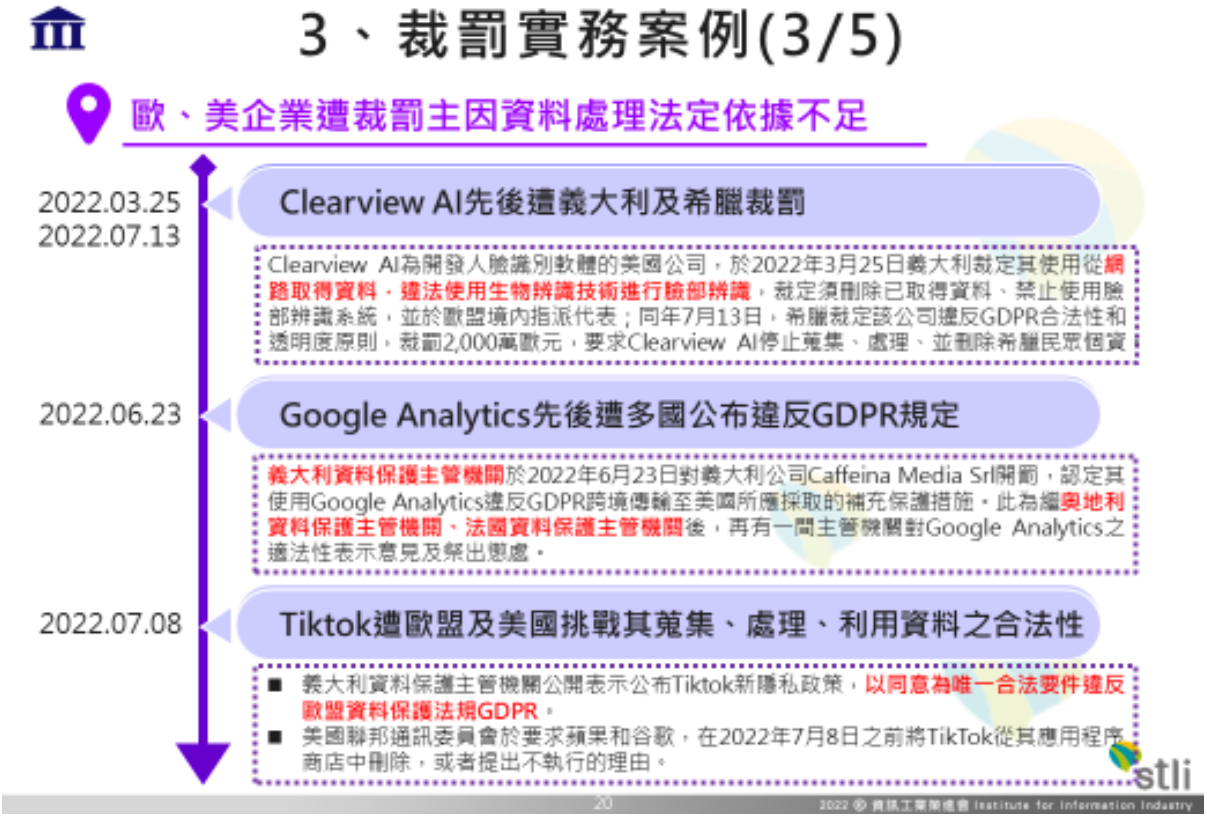
2021年GDPR案件裁罰類型

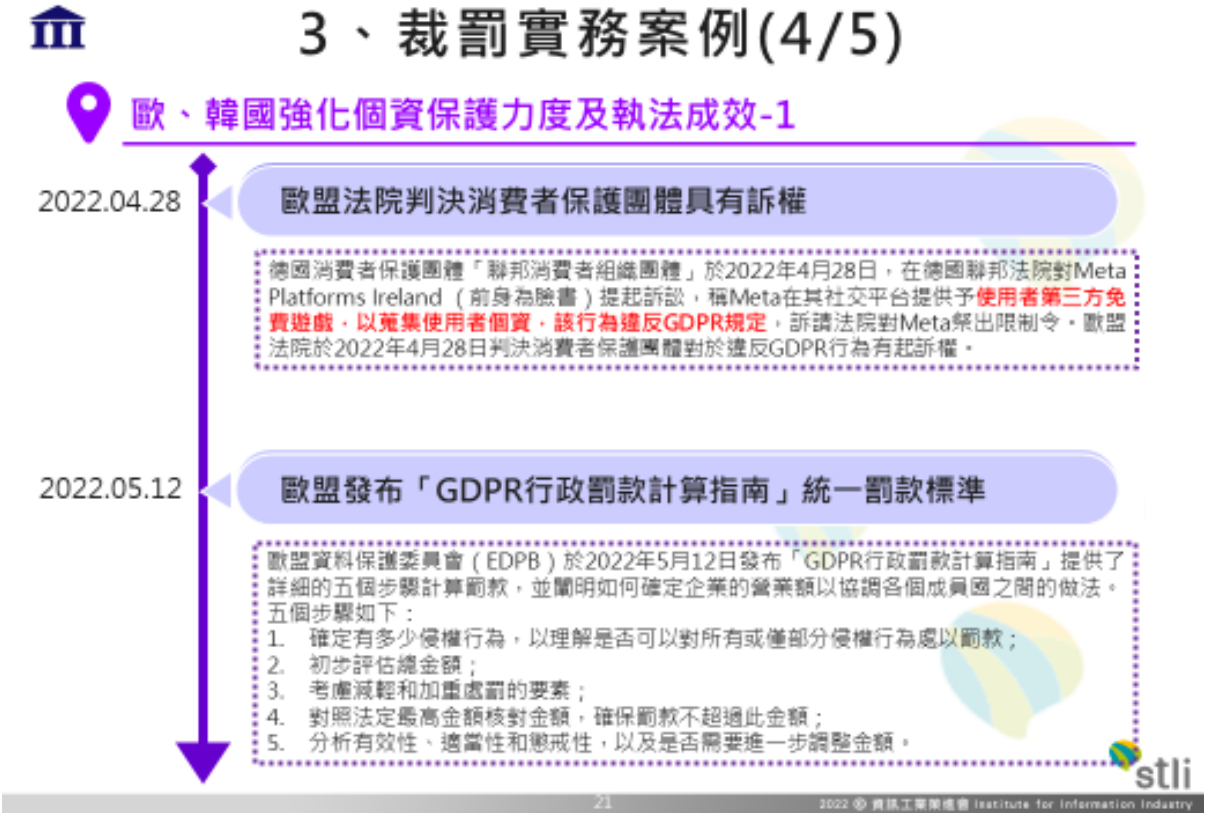


近三年GDPR裁罰案件數量及金額大幅增長



參考資料：GDPR Enforcement Tracker - list of GDPR fines


3、裁罰實務案例(3/5)
歐、美企業遭裁罰主因資料處理法定依據不足
2022.03.25
2022.07.13
Clearview AI先後遭義大利及希臘裁罰
Clearview AI為開發人臉識別軟體的美國公司，於2022年3月25日義大利裁定其使用從網路取得資料，違法使用生物辨識技術進行臉部辨識，裁定須刪除已取得資料、禁止使用臉部辨識系統，並於歐盟境內指派代表；同年7月13日，希臘裁定該公司違反GDPR合法性和透明度原則，裁罰2,000萬歐元，要求Clearview AI停止蒐集、處理、並刪除希臘民眾個資
2022.06.23
Google Analytics先後遭多國公布違反GDPR規定
義大利資料保護主管機關於2022年6月23日對義大利公司Caffeina Media Srl開罰，認定其使用Google Analytics違反GDPR跨境傳輸至美國所應採取的補充保護措施。此為繼奧地利資料保護主管機關、法國資料保護主管機關後，再有一間主管機關對Google Analytics之適法性表示意見及祭出懲處。
2022.07.08
Tiktok遭歐盟及美國挑戰其蒐集、處理、利用資料之合法性
■ 義大利資料保護主管機關公開表示公布Tiktok新隱私政策，以同意為唯一合法要件違反歐盟資料保護法規GDPR。
■ 美國聯邦通訊委員會於要求蘋果和谷歌，在2022年7月8日之前將TikTok從其應用程序商店中刪除，或者提出不執行的理由。
stli
20
2022 資訊工業策進會 Institute for Information Industry


3、裁罰實務案例(4/5)
歐、韓國強化個資保護力度及執法成效-1
2022.04.28
歐盟法院判決消費者保護團體具有訴權
德國消費者保護團體「聯邦消費者組織團體」於2022年4月28日，在德國聯邦法院對Meta Platforms Ireland（前身為臉書）提起訴訟，稱Meta在其社交平台提供予使用者第三方免費遊戲，以蒐集使用者個資，該行為違反GDPR規定，訴請法院對Meta祭出限制令。歐盟法院於2022年4月28日判決消費者保護團體對於違反GDPR行為有起訴權。
2022.05.12
歐盟發布「GDPR行政罰款計算指南」統一罰款標準
歐盟資料保護委員會（EDPB）於2022年5月12日發布「GDPR行政罰款計算指南」提供了詳細的五個步驟計算罰款，並闡明如何確定企業的營業額以協調各個成員國之間的做法。五個步驟如下：
1. 確定有多少侵權行為，以理解是否可以對所有或僅部分侵權行為處以罰款；
2. 初步評估總金額；
3. 考慮減輕和加重處罰的要素；
4. 對照法定最高金額核對金額，確保罰款不超過此金額；
5. 分析有效性、適當性和懲戒性，以及是否需要進一步調整金額。
stli
21
2022 資訊工業策進會 Institute for Information Industry

3、裁罰實務案例(5/5)

歐、韓國強化個資保護力度及執法成效-2

2022.02.14 **韓國要求OTT服務商改善消費者退出機制**

韓國公平貿易委員會於2022年2月14日發布新聞稿，要求谷歌(Google)、網飛（Netflix）等五家OTT（Over-the-top media services）服務商，改善其退訂機制。由於上述五間OTT服務商**訂閱容易但退訂困難，且未盡明確的告知義務，而有阻礙消費者取消訂閱之虞**而被KFTC處以1,950萬韓圓罰款。

2022.04.17 **韓國個人資料保護委員會公布2021年爭議案件統計情況**

韓國個人資料保護委員會於2022年4月17日公告2021年度個人資料糾紛調解案件，**88.7%的爭議案件發生在非公務機關**，僅有11.3%發生在公務機關。依行業別區分，違規數量最多的是**資通訊產業**，佔非公務部門紛爭總數35.4%，其次則為**金融與保險業**，以及**製造運輸及銷售業**，分別佔比18.4%及5.9%。

對照我國各部會所轄非公務機關個資外洩通報案件情形

統計日期：110.8.11~111.7.20.

	總計	內政部	教育部	文化部	金管會	交通部	衛福部	經濟部	通傳會	公平會	財政部	勞動部
總案	67	0	7	3	8	9	16	22	0	1	0	1
關係人端	50	0	4	2	7	9	7	21	0	0	0	0
內部疏失	15	0	3	0	1	0	6	1	0	1	0	1
不明	1	0	0	0	0	0	1	0	0	0	0	0
駭外洩	3	0	0	1	0	0	2	0	0	0	0	0

4、國際傳輸

4、國際傳輸(1/3)

主題摘要

日、歐、美強化資料國際傳輸於實務之運作

- 日本發布「國外個人資料保護制度調查報告」提升風險預見性
- 歐盟發布「行為守則作為傳輸工具指南」以利國際傳輸運作
- 美國與歐盟執委會達成新資料傳輸隱私框架

歐、韓透過驗證機制作為國際傳輸合法要件之一

- 韓國宣布受理CBPR認證申請
- 歐盟發布「驗證作為國際傳輸工具指南」說明驗證機制之運作

4、國際傳輸(2/3)

日、歐、美強化資料國際傳輸於實務之運作

2022.01.24 **日本發布「國外個人資料保護制度調查報告」提升風險預見性**

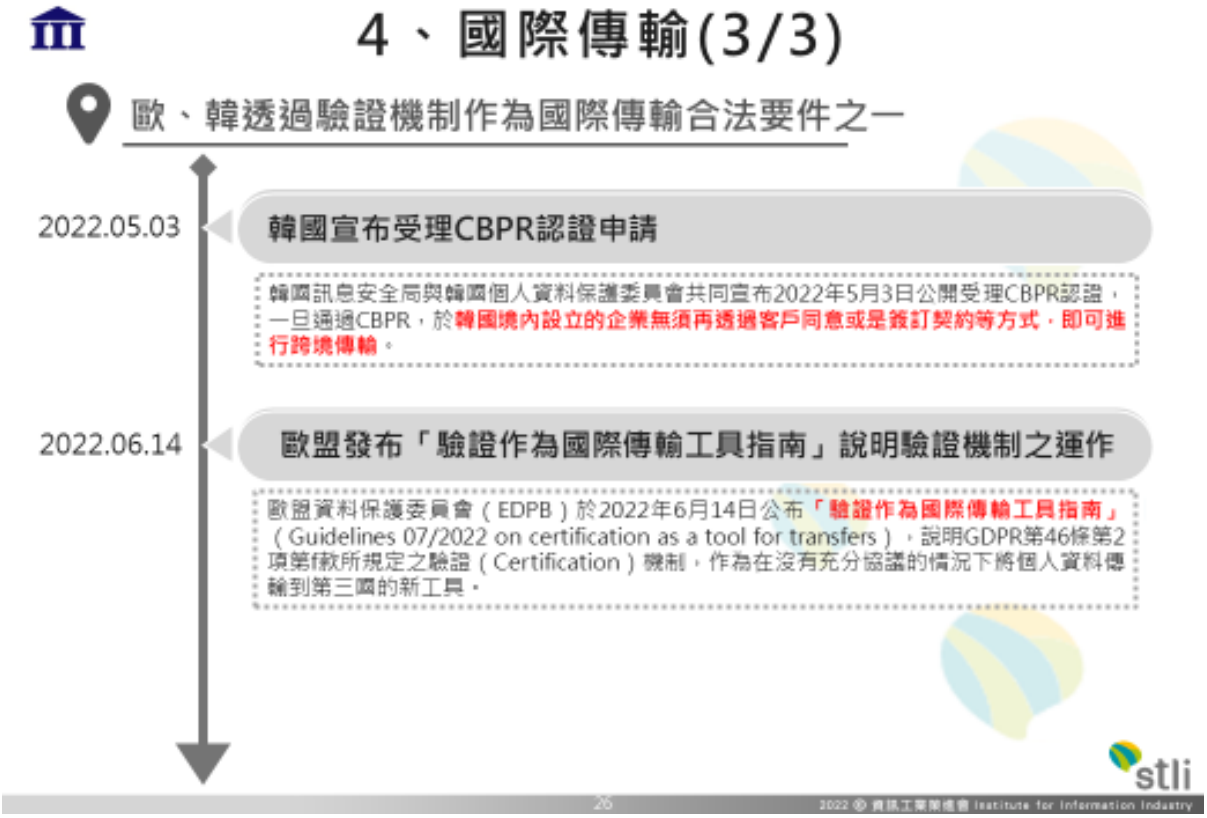
日本個人資料保護委員會於2022年1月24日根據2020年修訂的《個人資料保護法》，其中加強對外國第三者提供個人資料的規定，公布「國外個人資料保護制度調查報告」。要求事業**應向當事人充分提供資訊的目的**，旨在**提高當事人對國際傳輸伴隨風險的預測可能性**。

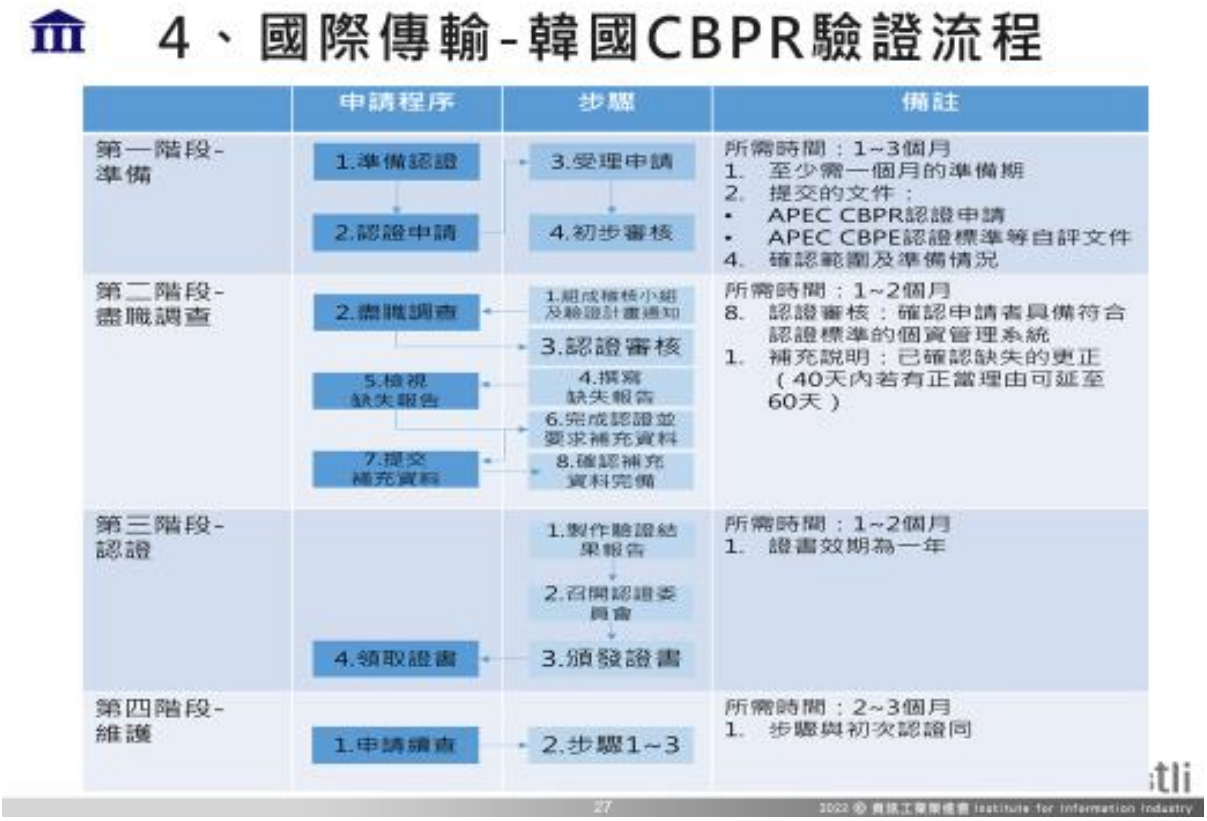
2022.02.22 **歐盟發布「行為守則作為傳輸工具指南」以利國際傳輸運作**

歐盟個人資料保護委員會（EDPB）針對國際傳輸議題涉及之「行為守則」（Codes of Conduct, CoC）於2022年2月22日發布「行為守則作為傳輸工具」指南及準則，**提供國際傳輸之行為守則清單**，以提供EDPB與歐盟境內所有個資主管機關明確參考依據，並透明化與一致化歐盟境內的CoC的評估標準及審查程序。

2022.03.25 **美國與歐盟執委會達成新資料傳輸隱私框架**

美國與歐盟執委會（European Commission）達成新資料傳輸隱私框架，新框架將確保**情報活動的蒐集，只限於促進合法國家安全目的之必要，且需符合比例性**；歐盟境內自然人得透過**層級化救濟機制**（multi-layer redress mechanism）尋求救濟，包括獨立的資料保護審查法院，由美國政府之外的成員組成，成員有權裁定賠償及所需救濟措施。


4、國際傳輸(3/3)
歐、韓透過驗證機制作為國際傳輸合法要件之一
2022.05.03
韓國宣布受理CBPR認證申請
韓國訊息安全局與韓國個人資料保護委員會共同宣布2022年5月3日公開受理CBPR認證，一旦通過CBPR，於韓國境內設立的企業無須再透過客戶同意或是簽訂契約等方式，即可進行跨境傳輸。
2022.06.14
歐盟發布「驗證作為國際傳輸工具指南」說明驗證機制之運作
歐盟資料保護委員會（EDPB）於2022年6月14日公布「驗證作為國際傳輸工具指南」（Guidelines 07/2022 on certification as a tool for transfers），說明GDPR第46條第2項第f款所規定之驗證（Certification）機制，作為在沒有充分協議的情況下將個人資料傳輸到第三國的新工具。
stli
26


4、國際傳輸-韓國CBPR驗證流程
申請程序
步驟
備註
第一階段-準備
1.準備認證
2.認證申請
3.受理申請
4.初步審核
所需時間：1~3個月
1. 至少需一個月的準備期
2. 提交的文件：
• APEC CBPR認證申請
• APEC CBPE認證標準等自評文件
4. 確認範圍及準備情況
第二階段-書職調查
2.書職調查
1.組成檢核小組及驗證計畫通知
3.認證審核
5.檢視缺失報告
4.撰寫缺失報告
6.完成認證並要求補充資料
7.提交補充資料
8.確認補充資料完備
所需時間：1~2個月
8. 認證審核：確認申請者具備符合認證標準的個資管理系統
1. 補充說明：已確認缺失的更正（40天內若有正當理由可延至60天）
第三階段-認證
1.製作驗證結果報告
2.召開認證委員會
3.頒發證書
4.領取證書
所需時間：1~2個月
1. 證書效期為一年
第四階段-維護
1.申請續查
2.步驟1~3
所需時間：2~3個月
1. 步驟與初次認證同
stli
27

4、國際傳輸-國際間CBPR執行狀況

CBPR 成員國	隱私執法機構 (Privacy Enforcement Authority, PEA)	當責機構 (Account Agent, AA)	參與認證公司 (Participants)
美國 2012	聯邦貿易委員會 Federal Trade Commission	TRUSTe Schellman & Co., LLC NCC Group HITRUST BBB National Programs	截至四月共計39家： ICT產業：23；民生消費：3 傳播娛樂：3；健康醫療：3 金融保險：3；廣告服務：1 資訊安全：1；法律/顧問：2
墨西哥 2013	國家資訊透明公開與個人資料保護局 Federal Institute for Access to Information and Data Protection of Mexico	無	-
日本 2014	日本個人情報保護委員會 Personal Information Protection Commission	JIPDEC	ICT產業共計3家： Intasect Communications、Paidy、Yahoo Japan
加拿大 2015	加拿大個人資料私隱專員公署 Office of the Privacy Commissioner of Canada	無	-
韓國 2017	個人資料保護委員會 Personal Information Protection Commission	KISA	-
澳洲 2018	澳洲私隱專員公署 Office of the Australian Information Commissioner	無	-
新加坡 2018	新加坡個人資料保護委員會 Personal Data Protection Commission	IMDA	共計6家： ICT產業：3；民生消費：1 金融保險：2
台灣 2018	由國發會整合經濟部、法務部、金管會等15個個資執法機關	資策會	-
菲律賓 2020	菲律賓官方機構國家隱私委員會 National Privacy Commission	無	-

5、人工智慧或生物識別

5、人工智慧或生物識別(1/5)

主題摘要

新、日、法針對AI運用發布標準或指南

- 新加坡首推「人工智慧驗證」以促進公司治理透明度
- 新加坡推出「隱私增強技術沙盒」以利建立技術規範標準
- 日本公布「監視器資料活用指南」第三版供企業參考
- 法國發布「人工智慧系統自我評估指南」協助企業自評風險

日、美、歐、新針對生物識別技術加以規範隱私保護

- 日本發布新版「人類生命科學與醫學研究倫理準則」以因應個資法修正
- 美國麻州發布政府「使用臉部識別技術最終報告」提供立法建議
- 歐盟發布「執法領域人臉辨識技術使用指引」提出禁止使用情境
- 新加坡公布「於安全性應用程式負責任的利用生物特徵識別資料指引」提供物業管理公司合理使用生物可辨識資料

5、人工智慧或生物識別(2/5)

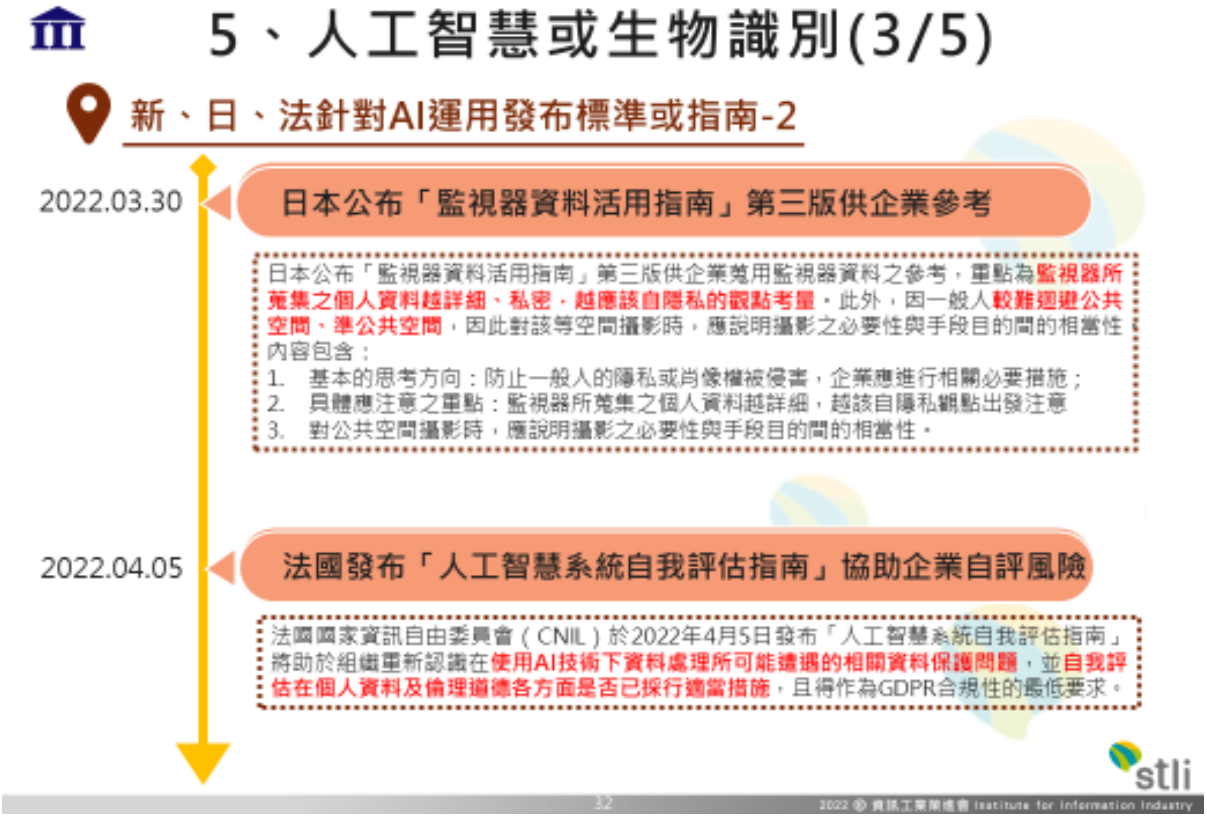
新、日、法針對AI運用發布標準或指南-1

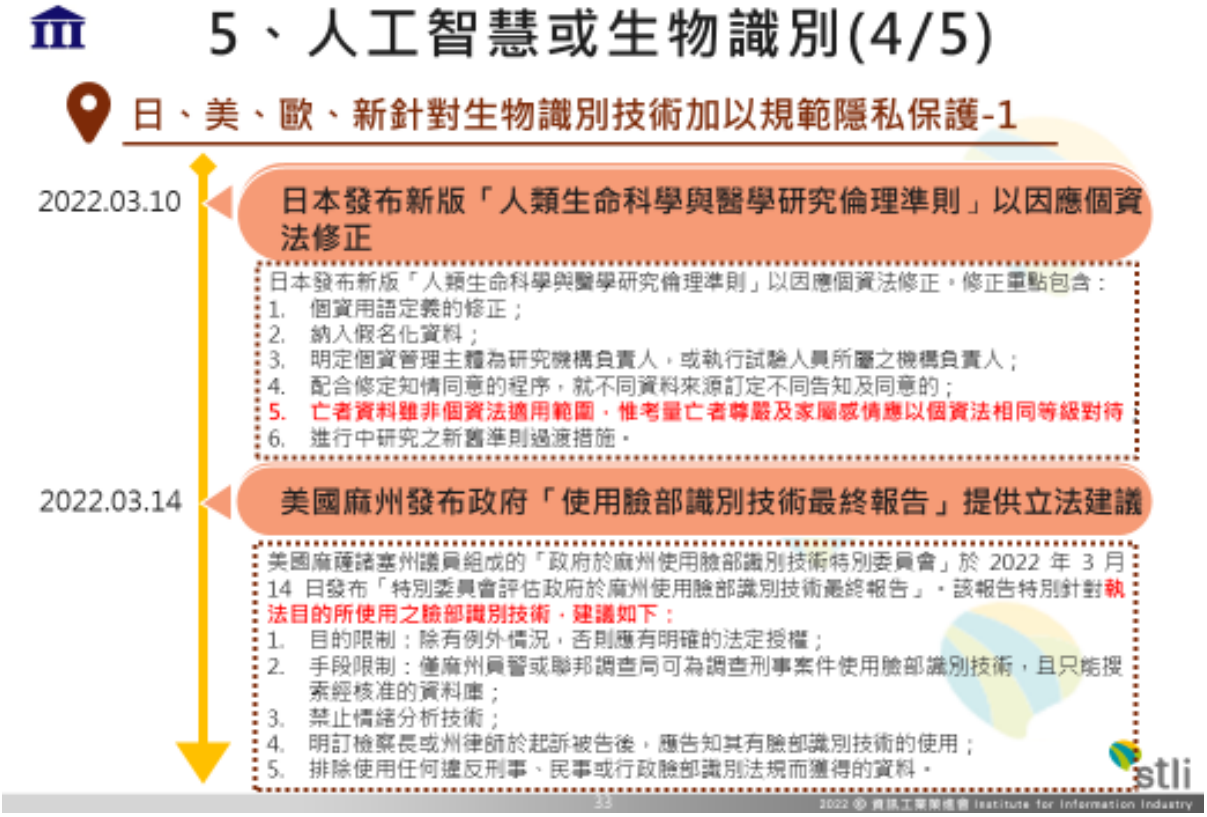
2022.05.17 **新加坡首推「人工智慧驗證」以促進公司治理透明度**

- 新加坡資訊通信媒體發展局與個人資料保護委員會於2022年5月25日，推出「人工智慧驗證」（AI Verify），以促進公司及其利益關係者間之透明度。該「人工智慧驗證」為**世界上第一組AI治理測試框架及工具包，適用於欲以客觀可驗證方式展示責任之AI公司亦為目前最小可行性產品（Minimum Viable Product）。**
- 並涵蓋以下領域：
  1. 透明度：關於使用人工智慧來實現既定的結果、了解 AI 模型如何做出決策、人工智慧預測的決策是否顯示出無意義之偏見；
  2. 人工智慧系統的安全性和彈性；
  3. 人工智慧系統之問責制與監督。

2022.07.20 **新加坡推出「隱私增強技術沙盒」以利建立技術規範標準**

- 新加坡資訊通訊媒體發展局和新加坡個人資料保護委員會於2022年7月20日，推出隱私增強技術沙盒（Privacy Enhancing Technologies Sandbox），**試行隱私增強技術（Privacy Enhancing Technologies, PET）項目**，以解決常見的企業業務挑戰。
- PDPC目標為與私部門參與者共同測試適合PET之使用情境，以及PET技術之限制，以利建立標準和最佳示範案例，以支持更大規模的運用。


5、人工智慧或生物識別(3/5)
新、日、法針對AI運用發布標準或指南-2
2022.03.30
日本公布「監視器資料活用指南」第三版供企業參考
日本公布「監視器資料活用指南」第三版供企業蒐用監視器資料之參考，重點為監視器所蒐集之個人資料越詳細、私密，越應該自隱私的觀點考量。此外，因一般人較難迴避公共空間、準公共空間，因此對該等空間攝影時，應說明攝影之必要性與手段目的間的相當性
內容包含：
1. 基本的思考方向：防止一般人的隱私或肖像權被侵害，企業應進行相關必要措施；
2. 具體應注意之重點：監視器所蒐集之個人資料越詳細，越該自隱私觀點出發注意
3. 對公共空間攝影時，應說明攝影之必要性與手段目的間的相當性。
2022.04.05
法國發布「人工智慧系統自我評估指南」協助企業自評風險
法國國家資訊自由委員會（CNIL）於2022年4月5日發布「人工智慧系統自我評估指南」將助於組織重新認識在使用AI技術下資料處理所可能遭遇的相關資料保護問題，並自我評估在個人資料及倫理道德各方面是否已採行適當措施，且得作為GDPR合規性的最低要求。
stli
32
2022 資訊工業策進會 Institute for Information Industry


5、人工智慧或生物識別(4/5)
日、美、歐、新針對生物識別技術加以規範隱私保護-1
2022.03.10
日本發布新版「人類生命科學與醫學研究倫理準則」以因應個資法修正
日本發布新版「人類生命科學與醫學研究倫理準則」以因應個資法修正。修正重點包含：
1. 個資用語定義的修正；
2. 納入假名化資料；
3. 明定個資管理主體為研究機構負責人，或執行試驗人員所屬之機構負責人；
4. 配合修定知情同意的程序，就不同資料來源訂定不同告知及同意的；
5. 亡者資料雖非個資法適用範圍，惟考量亡者尊嚴及家屬感情應以個資法相同等級對待
6. 進行中研究之新舊準則過渡措施。
2022.03.14
美國麻州發布政府「使用臉部識別技術最終報告」提供立法建議
美國麻薩諸塞州議員組成的「政府於麻州使用臉部識別技術特別委員會」於 2022 年 3 月 14 日發布「特別委員會評估政府於麻州使用臉部識別技術最終報告」。該報告特別針對執法目的所使用之臉部識別技術，建議如下：
1. 目的限制：除有例外情況，否則應有明確的法定授權；
2. 手段限制：僅麻州員警或聯邦調查局可為調查刑事案件使用臉部識別技術，且只能搜索經核准的資料庫；
3. 禁止情緒分析技術；
4. 明訂檢察長或州律師於起訴被告後，應告知其有臉部識別技術的使用；
5. 排除使用任何違反刑事、民事或行政臉部識別法規而獲得的資料。
stli
33
2022 資訊工業策進會 Institute for Information Industry

5、人工智慧或生物識別(5/5)

日、美、歐、新針對生物識別技術加以規範隱私保護-2

2022.05.16

歐盟發布「執法領域人臉辨識技術使用指引」呼籲禁止使用情境

歐盟個人資料保護委員會（EDPB）於2022年5月16日發布「執法領域人臉辨識技術使用指引」，並再次呼籲特定情況下應**禁止使用人臉辨識技術**，包括：

1. 於公共場所對個人進行遠端生物辨識；
2. 根據個人生物特徵而將個人依據歧視理由進行分類；
3. 以人臉識別或類似技術推斷自然人情緒；
4. 在執法環境中處理個人資料，且資料處理仰賴之資料庫以大規模、任意方式蒐集個資

2022.05.17

新加坡公布「於安全性應用程式負責任的利用生物特徵識別資料指引」提供物業管理公司合理使用生物可辨識資料

新加坡個人資料保護委員會於2022年5月17日公布「於安全性應用程式負責任的利用生物特徵識別資料指引」（Guide on the Responsible Use of Biometric Data in Security Applications），協助物業管理公司（Management Corporation Strata Title, MCST）、建築物及場所所有者或建物安全服務公司等管理機構，**合理的使用安全攝影機及生物特徵識別系統，以保護蒐集、利用或揭露的個人生物特徵識別資料**。

stli

34

2022 © 資訊工業策進會 Institute for Information Industry

1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13領導 e-Taiwan / m-Taiwan 14積極5G智慧科技創新應用 15支援文創與設計產業桌基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉與綠宜頻環境
19協助產業拓展高機並強化資安防護 20數位轉型化育者

THANK YOU

stli

2022 © 資訊工業策進會 Institute for Information Industry

附件四、諮詢會議之會議資料

「個人資料保護法相關議題」第 1 場產學專家學者諮詢會議—蒐集、處理、利用一般個人資料合法要件(不含「當事人同意」要件)

議程

壹、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討(不含「當事人同意」要件)、受託處理者義務、產業應用(含科學研究、假名化、匿名化)、當事人權利(可攜權、被遺忘權、權利限制規定)、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及瑞士「聯邦個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議，聚焦於蒐集、處理及利用一般個人資料之合法要件探討（不含同意），下一場會議將聚焦於蒐集、處理及利用特種個人資料之合法要件(不含同意)探討。

貳、議程

一、 主席致詞

二、 報告事項

「蒐集、處理、利用一般個人資料合法要件(不含「當事人同

意」探討(國發會)

三、 討論事項

綜觀各國個資保護規範，在我國個資法規定尚未將蒐集處理利用樣態整合為單一「處理(Processing)」行為前，一般個資之蒐集處理利用合法要件，若扣除同意及科學研究等要件，主要可歸納為：法律規定、契約、公共利益、保護個人（含資料當事人及其他人）權利、(控管者）正當利益、對當事權益有利或對其權利無侵害、取自公開資料或一般可得來源等 7 大類別。其中，依法律規定及契約兩項合法性要件各國較無顯著差異，僅就其餘要件整理討論內容如下列案由。

案由一、公共利益是否有進一步類型化必要，若須類型化，則何者應該納入相關要件？

說明：

以「公共利益」作為蒐集、處理利用之合法要件，於法理上並無不當。惟因其具備一定程度之不確定性，是否能以更清楚方式描述公共利益內含，以使人民對規定能有更充分認識，從而降低適用上之困擾，亦值得進一步考量。

綜觀各國規定，目前僅新加坡與我國個資法以較廣泛的「公共利益」或「國家利益」等形式規範此一合法要件。

多數國家（歐盟、德國、英國、美國、新加坡及瑞士）則對「公共利益」內含有更清楚之說明。其中，英國、新加坡及瑞士對非公務機關之公共利益以明文方式規範適用之項目，相較於我國以「公共利益」概括，似乎更為清楚(即便瑞士允許非公務機關以公共利益作為目的外利用合法要件，但仍要求應與當事人權益進行利益衡量)。

承上，擬請產學專家學者就我國現行「公共利益」合法要件，是否有進一步類型化必要；若須類型化，則何者應該納入討論等提供專業意見參考。

案由二、避免當事人及他人生命身體危險合法性要件，是否已能為我國現行其他蒐集合法要件所涵蓋？是否有必要仿效日、韓等國，將保護當事人或他人利益限縮於難以取得同意之

情形？

說明：

保護個人利益作為蒐集處理利用合法要件，可從以下三方面加以觀察：

（一）適用的權利類型

目前，我國允許於公務及非公務機關為免除當事人之生命、身體、自由或財產上之危險或防止他人權益之重大危害而在蒐集目的外利用個人資料。其他國家多限於生命、身體，但也有日本、韓國與我國一樣適用財產權利，德國則以法益的重大危害概括適用類型。整體而言我國規定與他國並無顯著不同。

（二）是否限於特定目的外利用

綜觀其他國家規定，例如: 新加坡或歐盟體系之國家，將保護當事人或其他人之生命、身體危害作為合法要件之一時，不限於利用階段，此為我國於資料蒐集時所無之規定。

（三）是否作為同意難以取得時之合法要件

此外，日本、韓國、新加坡、瑞士等國「保護當事人或他人利益」條文設計，特別提醒係於同意取得困難（或合理認為當事人不會反對）情形；相較起來，我國則於條文設計上未特別強調之。

小結：根據以上觀察，擬請產學專家學者就以下兩項議題提供建議，以供參考：

（一）參考歐盟體系國家將避免當事人及他人生命身體危險合法性要件之立法例，亦可能包含到相當我國蒐集行為階段，但我國目前並無類似規定。此種情形是否已能為我國現行其他蒐集合法要件（例如公務機關執行法定職務；非公務機關已對當事人無侵害為由蒐集）所涵蓋？又或者需要增訂？

（二）我國是否有必要仿效日、韓等國，將保護當事人或他人利益限縮於取得同意困難之情形？此種作法對我國產

業及公務機關運用時，是否造成困擾？

案由三、採用正當利益要件及對當事人之影響之利益衡量，是否較對當事人無侵害或有利作為利用要件，更能提供產業具彈性的利用空間？若以正當利益與利益衡量之作法，是否對當事人保護充足？

說明：

控管者之正當利益（legitimate interest）為許多國家承認之合法要件，但我國目前並未承認此一要件；相較之下我國承認「有利於當事人權益」、「對當事人權益無侵害」等要件，則較為少見。我國是否有必要調整相關規定，似有討論空間。

（一）「有利於當事人權益」、「對當事人權益無侵害」等要件

我國個資法規定，公務機關及非公務機關於蒐集時可以「對當事人權益無侵害」作為合法蒐集要件；在目的外利用時，可以「有利於當事人權益」作為合法要件。其中，公務機關之規定，係於「電腦處理個人資料保護法」立法時，參考當時有效之外國法（德國及日本）所制定。非公務機關，則係民國 104 年修法時，立法委員考量非公務機關立法需要提案增訂。由於我國規定要求對當事人「有利」或「無侵害」，為了避免可造成當事人權益微小侵害而引發爭端，目前實務上產業應用時，部分業者盡量避免援引此要件。

目前，僅瑞士、我國及美國統一州法律委員全國會議(ULC)於 2021 年公布之統一個資保護法範本(立法倡議並非真正法律）以有利於當事人或對當事人無侵害，作為合法要件。此種規範模式係著重於資料利用之結果。

（二）正當利益要件

正當利益部分，承認控管者正當利益國家可分為「不限制正當利益種類，但要求與當事人權益進行利益衡量」以及「限制正當利益種類，但無利益衡量要求」等兩大類。前者有歐盟體系國家、瑞士、韓國、新加坡等國採用；後者則有瑞士、美國統一個資保護法、新加坡及德國採用。此二種作法，前者係採取限縮控管者目的之範圍，並佐以對資料利用結果之衡量（當事人利益影響範圍）；後者則是立法時即已完

成目的及結果之衡量。

小結：就此，請產學專家學者就以下議題提供專業建議：相較於以資料應用之結果對當事人無侵害或有利作為利用要件；以控管者須具有正當利益，並與對資料當事人之影響進行利益衡量的作法，是否能提供產業更具彈性的利用空間？若以正當利益與利益衡量之作法，是否對當事人保護充足？

案由四、取自公開資料或一般可得來源相關要件對非公務機關適用上，是否有一定重要性？是否有必要限縮其範圍？

說明：

取自公開資料或一般可得來源之合法要件，僅我國等少數國家有類似要件，且過往產業應用上亦有爭議案件發生，爰有必要加以檢討。

目前，我國規定非公務機關於蒐集時，可以公開資料作為合法蒐集要件，或經過與當事人利益衡量狀況下，以一般可得來源作為合法蒐集要件。此二規定，分別為「電腦處理個人資料保護法」立法時，及民國 99 年修法時，參考當時有效之德國法制定。

我國目前實務上，曾發生業者蒐集商家基於法律或商業上需要所公開之資訊（如律師執業資訊），整理後販賣給其他業者做行銷使用；或利用大學申請入學榜單等公開資訊，整理為查榜系統，而意外拼湊當事人求學歷程，造成當事人困擾等事件。

除我國外，本次比較之國家中，僅瑞士及新加坡有類似設計（美國則是排除適用），是較為少見的合法要件。其中瑞士要求須考量當事人並未表示反對。

就此議題，擬請產學專家學者就以下議題提供建議：「取自公開資料或一般可得來源」此類規定，在我國目前實務運作上曾發生爭議，就目前實務運作上來說，這類規定對非公務機關適用上，是否有一定重要性？考量過去發生之爭議，若仿前述正當利益要件，以限縮控管者目的範圍（限於正當利益），並要求對當事人權益影響進行利益衡量的作法，是否

可取代「取自公開資料或一般可得來源」之要件？對於產業利用或當事人權益保障可能造成什麼影響？

蒐集、處理、利用之合法要件探討（一般個資）

國家發展委員會
110 年 10 月 6 日

大綱

一 討論範圍

二 議題分析

三 附件

一、 討論範圍 (1/2)

2

■ 討論範圍

一般個資（除當事人同意、學術研究外及自動決策處理外）之蒐集、處理、利用合法性要件

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
瑞士	聯邦個人資料保護法	2021	GDPR適足性認定（指令時代取得）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法**非實定法律**，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2020	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（進入最終程序）
新加坡	個人資料保護法	2020	CBPR成員

國家發展委員會

一、 討論範圍 (2/2)

3

■ 經整理各國蒐集、處理、利用合法要件，可分為以下7種類別：

	合法要件	說明
相似	法律規定	包含法定職務、法定義務，或其他法律授權蒐集處理利用
相似	契約	包含為制定、履行契約所必須之情形
各國規定差異較大	公共利益	基於對國家或不特定多數人之利益保護
各國規定差異較大	保護個人利益	保護資料當事人或特定他人之利益或權利
各國規定差異較大	有利於當事人或對當事人無侵害	對資料當事人之利益或權利有助益，或消極的對其無侵害
各國規定差異較大	（控管者）正當利益	基於資料控管者之利益、權利所為之個資蒐集處理利用
各國規定差異較大	公開或取自一般來源	公開資料：包含當事人自行公開、合法公開； 一般來源：一般人可知悉、接觸之來源管道

國家發展委員會

二、議題分析

我國個資法相關條文(1/2)

■ 蒐集、處理目的內

公務機關	非公務機關
第15條 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、執行法定職務必要範圍內。 二、經當事人同意。 三、對當事人權益無侵害。	第19條 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。 三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 八、對當事人權益無侵害。 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

6

我國個資法相關條文(2/2)

■ 目的外利用

公務機關	非公務機關
第16條 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。	第20條 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

7

(一) 公共利益 (1/5)

■ 我國現行規定

- 採取概括式「公共利益」的規範模式
- 公務機關：並非蒐集、處理合法要件，但得為維護國家安全、增進公共利益所必要，為目的外利用
- 非公務機關：得依此合法蒐集、處理，並得為目的外利用

	公務機關	非公務機關
蒐集、處理目的內	n/a	公共利益
目的外利用	公共利益 國家安全	公共利益

個人資料保護法第16條、19條、20條

(一) 公共利益 (2/5)

8

■ 國際立法例比較：蒐集、處理目的內

國別	廣義公共利益	國家利益	職務相關	其他
我國	○（限非公務）			
歐盟			○	
德國			○	
英國			○	支持或促進民主參與的活動
瑞士	○＋利益衡量（限非公務）			新聞／公眾人物的公開活動（非公務）
美國CCPA				
美國UPDPA			○（司法調查）	
日本				
韓國				
新加坡		○	○（執法）	如：藝術文學、新聞廣播、教育、醫療

要求利益衡量

多以類型化方式規定

國家發展委員會

(一) 公共利益 (3/5)

9

■ 國際立法例比較：目的外利用

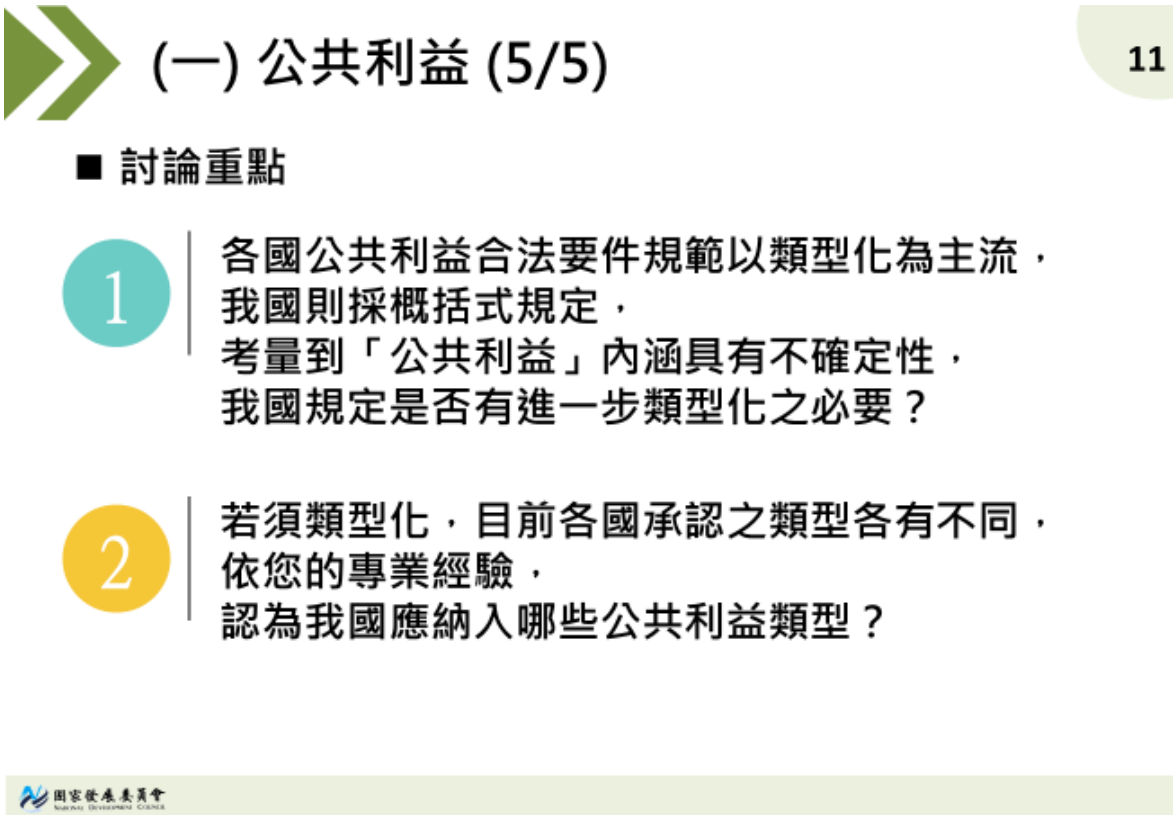
國別	廣義公共利益	國家高權	行政目的	司法相關	其他
我國	○	國安（公務）			
歐盟		得立法	得立法	得立法	
德國		國安、防衛、公安等	如：稅務海關、公眾利益、行政及考試監督	追訴犯罪、執行刑罰	
英國		得立法	得立法	得立法	
瑞士	○＋利益衡量（非公務）				如：新聞／公眾人物的公開活動（非公務）
美國CCPA					
美國UPDPA				司法調查	
日本					如：公衛、兒童發展且難以取得同意（非公務）
韓國		條約義務		刑事追溯與執行	
新加坡		國家利益	執法		如：藝術文學、新聞廣播、教育、醫療

要求利益衡量

多以類型化方式規定

國家發展委員會

(一)公共利益 (4/5)
10
■國際立法例比較結論
01
以類型化為主
各國規範普遍以類型化方式規範公共利益要件。
02
概括＋利益衡量
採取概括式要件之瑞士，另要求須與當事人利益進行利益衡量。
03
公共利益類型化後仍多有差異
各國類型化後的公共利益在目的外利用部份有所差異，但多數集中在國家高權、行政相關以及司法相關的類型。


(一) 公共利益 (5/5)
11
■ 討論重點
1
各國公共利益合法要件規範以類型化為主流，
我國則採概括式規定，
考量到「公共利益」內涵具有不確定性，
我國規定是否有進一步類型化之必要？
2
若須類型化，目前各國承認之類型各有不同，
依您的專業經驗，
認為我國應納入哪些公共利益類型？

(二) 保護個人利益 (1/4)

12

■ 我國現行規定

- 允許公務及非公務機關
  a) 基於免除當事人生命、身體、自由或財產上危險
  b) 基於防止他人權益重大危害
  允許為特定目的外利用

公務及非公務機關	當事人	其他人
蒐集、處理目的內	n/a	n/a
目的外利用	生命 身體 自由 財產	權益重大危害

個人資料保護法第16條、20條

(二) 保護個人利益 (2/4)

13

當事人

普遍承認　　部份國家承認

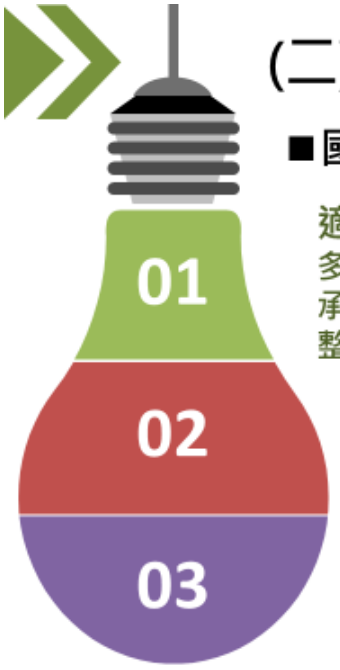
權利種類		生命	身體/健康	財產	自由	廣義法益/權利
無須考慮同意	目的內	歐盟、德國、英國	歐盟、德國、英國			
	目的外	我國	我國	我國	我國	
同意取得困難或應不會拒絕	目的內	新加坡、瑞士	新加坡、瑞士			
	目的外	日本、韓國、新加坡	日本、韓國、新加坡	日本、韓國		德國

其他人

權利種類		生命	身體/健康	財產	自由	廣義法益/權利
無須考慮同意	目的內	歐盟、德國、英國	歐盟、德國、英國			
	目的外					我國、德國（重大危害）
同意取得困難或應不會拒絕	目的內	新加坡、瑞士	新加坡、瑞士			
	目的外	日本、韓國、新加坡	日本、韓國、新加坡	日本、韓國		

作為蒐集要件之一

註：歐盟與英國得立法基於當事人或其他人權利保障而於特定目的外使用個資



(二) 保護個人利益 (3/4)

14

■國際立法例比較結論

適用類型無明顯差異
多數國家承認生命、健康作為合法要件，我國及日、韓承認財產權利；德國則以法益的重大危害概括適用類型；整體而言並無顯著差異。

部份國家將此作為蒐集要件
新加坡、歐盟體系國家亦可作為蒐集時之要件，與我國、日、韓規定較不相同。

部份國家要求以難以取得同意為限
日本、韓國、新加坡、瑞士等皆限於難以取得同意情形，我國並無相關規定。

(二) 保護個人利益 (4/4)

15

■ 討論重點

1. 歐盟體系及新加坡允許以保護個人利益作為蒐集時之合法要件，其是否能為我國現行其他蒐集時之合法要件涵蓋？
若不能，是否有增訂之必要？

2. 於目的外利用情形，
是否應如日、韓、新等規定，
將保護當事人或他人利益限於難以取得同意之情形？
此種作法對我國產業及公務機關運用，
是否造成困擾？

(三) 正當利益與對當事人無侵害 (1/4)

16

■ 我國現行規定

- 正當利益：未承認
- 對當事人無侵害：公務及非公務機關可以蒐集、處理
- 有利於當事人權益：公務及非公務機關得為特定目的外利用

	合法要件	立法理由
蒐集、處理目的內	對當事人權益無侵害	公務機關：電腦處理個資法立法時，參考當時有效德國、日本法 非公務機關：因**面試時確認背景**、確認是否應**利益迴避**等原因蒐集時，對當事人權益無侵害但仍須取得同意，徒增困擾。（104年個資法修訂）
目的外利用	有利於當事人	公務機關：電腦處理個資法立法時，參考當時有效德國、日本法 非公務機關：未特別說明（104年個資法修訂）

個人資料保護法第15條、16條、19條、20條

國家發展委員會

(三) 正當利益與對當事人無侵害 (2/4)

17

正當利益要件

規範模式	廣泛正當利益類型 + 利益衡量要求	類型化正當利益類型 + 無利益衡量要求
蒐集、處理目的內	歐盟、德國、英國、瑞士、韓國、新加坡	瑞士（商業競爭 + 不會揭露、信譽檢查） 美國UPDPA（管理、人事、行政、營運、假名化、去識別化、監督、定向廣告等） 新加坡（改進商業）
目的外利用	瑞士、新加坡	瑞士（商業競爭 + 不會揭露、信譽檢查） 美國UPDPA（管理、人事、行政、營運、假名化、去識別化、監督、定向廣告等） 德國（民事請求） 新加坡（改進商業）

多為內部管理措施或民事訴訟

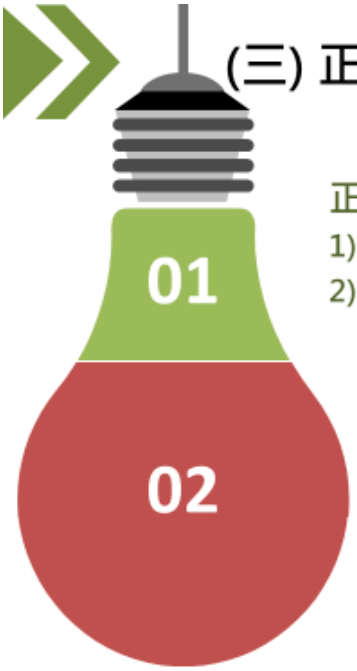
有利於當事人或對當事人無侵害

	我國	瑞士	美國UPDPA
有利於當事人	公務、非公務，目的外利用		○
對當事人無侵害	公務、非公務，蒐集、處理目的內	公務，須聯邦委員會許可	

國家發展委員會

(三) 正當利益與對當事人無侵害 (3/4)

18



正當利益要件規範模式有二

1)僅要求目的正當，但須衡量當事人權益

2)立法限縮目的類型，但不須利益衡量

正當利益與對當事人無侵害比較

	目的	判斷標準	採用國家	說明
A	無限制	對當事人有利或無侵害	瑞士、我國、美國 UPDPA	需確認「無侵害」甚至「有利」，**標準似乎較高**
B	廣泛正當利益	與當事人權益利益衡量	歐盟、德國、英國、韓國、新加坡	在正當利益目的下，換取判斷標準之放寬，利用彈性較大
C	類型化正當利益	未規範	瑞士、美國 UPDPA、德國、新加坡	將正當利益進一步類型化其目的範圍，即未特別規範判斷標準。

(三) 正當利益與對當事人無侵害 (4/4)

19

■ 討論重點

1. 我國「未限制正當利益，但要求對當事人無侵害或有利於當事人」之合法要件(A模式)，是否得以其他國家「正當利益+利益衡量」(B模式)或「類型化正當利益」(C模式)取代？若是，對當事人保護是否足夠？

2. 若採取「正當利益+利益衡量」為合法要件，能否提供產業更具彈性的利用空間？

(四) 取自公開資料或一般可得來源 (1/4)

20

■ 我國現行規定

- 允許非公務機關，以下列2項為蒐集、處理要件：

a) 當事人自行公開或其他已合法公開之個人資料

b) 個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。

	公務機關	非公務機關	立法理由
蒐集、處理目的內	n/a	公開資料	當時立法過程立委提案
		取自一般可得來源且與當事人利益進行利益衡量	99年個資法修正時參考當時有效之德國法
目的外利用	n/a	n/a	

個人資料保護法第19條

(四) 取自公開資料或一般可得來源 (2/4)

21

承認國家較少

	公開資料	一般可得來源
限於蒐集、處理目的內	我國（非公務機關）	我國（限非公務機關且須利益衡量）
不區分	瑞士（僅限當事人不反對） 新加坡 *美國CCPA、UPDPA（排除適用）*	

(四) 取自公開資料或一般可得來源 (3/4)

22

採用資料來源要件國家稀少
採用類似要件之國家，僅我國、瑞士及新加坡。
（美國排除公開資料適用個資法）

我國立法主要參考當時有效德國法

利用公開個資可能造成當事人困擾
我國過往曾有相關爭議案件；
瑞士特別要求須在當事人不反對的狀況下
才可使用公開個資。

(四) 取自公開資料或一般可得來源 (4/4)

23

■ 討論重點

1. 公開資料或一般可得來源之使用，
對非公務機關是否有重要性？

2. 限縮控管者目的範圍，
並要求與當事人權益影響進行利益衡量，
是否可取代此合法要件？
對於產業利用或當事人權益保障
可能造成什麼影響？

附件一 各國一般個資合法要件

24

我國相關規定

25

最近一次個資法修正：2015年
CBPR成員國、GDPR適足性認定諮商中

定義	識別性			排除
	直接	間接	對象	無
	○	○	自然人	

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（含法定職務）	○
契約		○（非公務）	
公共利益		○（非公務）	○（公務另含國家安全）
保護個人利益	當事人		生命身體自由財產危險
	其他人		權益
（控管者）正當利益			
公開或取自一般來源		○（非公務；一般來源須利益衡量）	
有利於當事人或對當事人無侵害		無侵害	有利當事人

國家發展委員會

歐盟相關規定（1/2）

26

最近一次個資法修正：2016年（2018年施行）

定義	識別性			排除
	直接	間接	對象	無
	○	○	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外
法律規定		○	○（會員國得立法之範圍*）
契約		○（履行、準備締約）	
公共利益		○（職務相關）	（須會員國立法*）
保護個人利益	當事人	○（生命、健康）	（須會員國立法*）
	其他人	○（生命、健康）	（須會員國立法*）
（控管者）正當利益		非公務：○（＋利益衡量）	
公開或取自一般來源			
有利於當事人或對當事人無侵害			

國家發展委員會

歐盟相關規定（2/2）

27

會員國可立法允許於蒐集目的範圍外處理、利用之項目：

- **國家高權與公共利益**
  - 國家安全
  - 國防
  - 公共安全
  - 公共利益（經濟、金融、財政、預算、稅賦、公衛、社會安全）
  - 行政機關監管
- **司法相關**
  - 刑事犯罪之預防、調查、偵查、追溯；刑罰執行
  - 特定職業道德規範之預防、偵查、追溯
  - 司法程序及獨立性保障
  - 民事請求執行
- **基本權保障**：當事人及他人權利自由之保障

國家發展委員會

德國相關規定（1/2）

28

最近一次個資法修正：2021年6月23日
歐盟成員國

定義	識別性			排除
	直接	間接	對象	無
	○	○	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外
法律規定		○	○（BDSG特別規定*）
契約		○（履行、準備締約）	
公共利益		○（職務相關）	公共利益、監管、刑事責任等*
保護個人利益	當事人	○（生命、健康）	法益+無理由認為當事人拒絕*
	其他人	○（生命、健康）	權利嚴重損害*
（控管者）正當利益		非公務：○（+利益衡量）	民事請求*
公開或取自一般來源			
有利於當事人或對當事人無侵害			

國家發展委員會

德國相關規定（2/2）

29

BDSG特別規定

公務機關	非公務機關
BDSG第23條第1項 **履行職務範圍內，且具有下列事由之一者：** ➢明顯地為**維護當事人法益**，且**無理由認為當事人會拒絕同意** ➢對於當事人的說明有事實根據認為**非正確性**，而須予以**審核** ➢基於必要之情形，為防止**公共利益**之重大損害，或**公共安全**、**防衛或國家安全**之危害；或為維護**公眾之重大利益**；或確保**稅務及海關**收益， ➢有**追訴犯罪或違反秩序之行為**之必要，以強制執行或執行《刑法典》（Strafgesetzbuch）第11條第1項第8款意義內之**刑罰或措施**；執行《少年法院法》（Jugendgerichtsgesetz）所定**感化教育或教養方法**；或為**執行罰鍰**之必要。 ➢為**防止對他人權利嚴重損害**之必要。 ➢為履行**監督及管控之職權**、**會計審查**或執行**對控制者之組織調查**；此亦適用於基於**教育及考試**之目的，由控制者處理個人資料之情形，但以當事人值得保護之**法益未有衝突**之範圍內為限。	**BDSG第24條第1項** **具有下列事由之一者：** ➢基於防止**國家或公共安全之危害，或追訴犯罪**之必要。 ➢為行使、主張或為對抗**民法上請求權**之必要。

國家發展委員會

英國相關規定

30

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

定義	識別性			排除
	直接	間接	對象	無
	○	○	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外
法律規定		○（法定義務）	○（得立法之範圍*）
契約		○（履行、準備締約）	
公共利益	司法及國會行政 個人或政府依法所獲職權 支持或促進民主參與的活動	○（公務）	（須立法*）
保護個人利益	當事人	○（生命、健康）	（須立法*）
	其他人	○（生命、健康）	（須立法*）
（控管者）正當利益		非公務：○（＋利益衡量）	
公開或取自一般來源			
有利於當事人或對當事人無侵害			

瑞士相關規定

31

最近一次個資法修正：2021年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

定義	識別性			排除
	直接	間接	對象	無
	○	○	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內　未區分蒐集目的內、外　圍外
法律規定		○（公務：依資料及樣態有不同要求）
契約		非公務：○
公共利益		非公務：（○＋利益衡量 / 新聞 / 公眾人物的公開活動）
保護個人利益	當事人	公務：生命身體＋同意困難 非公務：○（＋利益衡量）
	其他人	公務：生命身體＋同意困難 非公務：○（＋利益衡量）
（控管者）正當利益		非公務：不限＋利益衡量 / 商業競爭＋不會揭露 / 信譽檢查
公開或取自一般來源		公務：公開且不反對
有利於當事人或對當事人無侵害		公務：無侵害＋經聯邦委員會許可

美國相關規定（CCPA）

32

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

定義	識別性			排除
	直接	間接	對象	• 聯邦、州、地方政府之公開資料 • 去識別、聚合資料
	○	合理	自然人、家庭	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外
法律規定			
契約			
公共利益			
保護個人利益	當事人		
	其他人		
（控管者）正當利益			
公開或取自一般來源			
有利於當事人或對當事人無侵害			

CCPA 僅要求蒐集資料前有告知義務，
並對出售個人資料有選擇退出權
（16歲以下為選擇加入）

國家發展委員會

美國相關規定（UPDPA）

33

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案
CBPR成員國

定義	識別性			排除
	直接	間接	對象	• 公開訊息 • 去識別化資料 • 人體研究、搜索票、就業求職等
	○	合理	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	未區分蒐集目的內、外	範圍外
法律規定		○（法定義務）		
契約		○		
公共利益		○（犯罪預防等、個資監督）		
保護個人利益	當事人			
	其他人			
（控管者）正當利益		• 管理、人事、行政或營運等特定目的 • 將資料假名化或去識別化 • 內部監督或對代理人之外部監督 • 自己或向第三方揭露假名資料，提供定向廣告或表達性內容		
公開或取自一般來源		公開（定義排除）		
有利於當事人或對當事人無侵害		○		

國家發展委員會

日本相關規定

34

最近一次個資法修正：2021年
CBPR成員國、GDPR適足性（2019）

定義	識別性			排除
	直接	間接	對象	無
	○	易於	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外（非公務）
法律規定		日本個資法僅規定： 不得以虛偽或 其他不正當手段 取得個人資料	○
契約			
公共利益			公衛、兒童發展＋難取得當事人同意
保護個人利益	當事人		生命身體財產＋難取得當事人同意
	其他人		生命身體財產＋難取得當事人同意
（控管者）正當利益			
公開或取自一般來源			
有利於當事人或對當事人無侵害			

國家發展委員會

韓國相關規定

35

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定進入最終程序

定義	識別性			排除
	直接	間接	對象	無
	○	易於（時間費用技術等）	自然人	

蒐集、處理、利用之合法要件		蒐集目的範圍內	蒐集目的範圍外
法律規定		○（含法定職務、義務）	○（含法定職務、義務）
契約		○	
公共利益			○（條約義務、刑事追溯、裁判執行）
保護個人利益	當事人		生命身體財產＋難以取得同意
	其他人		生命身體財產＋難以取得同意
（控管者）正當利益		○	
公開或取自一般來源			
有利於當事人或對當事人無侵害			

國家發展委員會

新加坡相關規定

最近一次個資法修正：2020年
CBPR成員國

定義	識別性			排除
	直接	間接	對象	• 保存超過100年以上 • 死亡超過10年
	○	○	自然人（含死者）	

蒐集、處理、利用之合法要件		蒐集目的範圍 未區分蒐集目的內、外 範圍外
法律規定		
契約		○（買賣、租賃、併購、處置或融資之商業交易）
公共利益		○（國家利益、藝術文學、新聞廣播、教育、醫療、執法）
保護個人利益	當事人	生命、健康、安全＋未能即時取得同意
	其他人	生命、健康、安全＋未能即時取得同意
（控管者）正當利益		不限＋利益衡量／商業改進
公開或取自一般來源		○（公開）
有利於當事人或對當事人無侵害		

國家發展委員會

附件二
綜整各國一般個資合法要件

各國對個資定義比較

38

國別	直接識別	間接識別	識別對象	排除範圍
我國	○	○	自然人	
歐盟	○	○	自然人	
德國	○	○	自然人	
英國	○	○	自然人	
瑞士	○	○	自然人	
美國CCPA	○	合理	自然人、家庭	• 聯邦、州、地方政府之公開資料 • 去識別、聚合資料
美國UPDPA	○	合理	自然人	• 公開訊息 • 去識別化資料 • 人體研究、搜索票、就業求職等
日本	○	易於	自然人	
韓國	○	易於（時間費用技術等）	自然人	
新加坡	○	○	自然人（含死者）	• 保存超過100年以上 • 死亡超過10年

*識別性議題將另案討論

國家發展委員會

一般個資合法要件綜合比較（1/3）

39

國別	法律規定		契約		公共利益	
	蒐集目的內	蒐集目的外	蒐集目的內	蒐集目的外	蒐集目的內	蒐集目的外
我國	○	○	○（限非公務）		○（限非公務）	○
歐盟	○	○（限範圍）	○		○（職務相關）	○（須立法）
德國	○	○（BDSG）	○		○（職務相關）	○（限定情形）
英國	○	○（須立法）	○		○（4情況）	○（須立法）
瑞士*	○（公務：依資料及樣態有不同要求）		○（限非公務）		○＋利益衡量／新聞／公眾人物的公開活動（限非公務）	
美國CCPA*						
美國UPDPA*	○		○		○	
日本*		○				○（限定情形）
韓國	○	○	○			○（限定情形）
新加坡*			○（限定契約類型）		○（限定情形）	

*附註：
美國CCPA僅要求蒐集資料前有告知義務，並對出售個人資料有選擇退出權
日本個資法僅規定：不得以虛偽或其他不正當手段取得個人資料
瑞士、新加坡及美國UPDPA未明確區分蒐集目的內、外

國家發展委員會

一般個資合法要件綜合比較（2/3）

40

國別	保護個人利益（當事人）		保護個人利益（其他人）		（控管者）正當利益	
	蒐集目的內	蒐集目的外	蒐集目的內	蒐集目的外	蒐集目的內	蒐集目的外
我國		生命身體財產自由		權利重大危害		
歐盟	生命健康	得立法	生命健康	得立法	○＋利益衡量	
德國	生命健康	法益＋無理由認當事人會拒絕	生命健康	權利嚴重損害	○＋利益衡量	民事請求
英國	生命健康	得立法	生命健康	得立法	○＋利益衡量	
瑞士	公務：生命身體＋同意困難 非公務：○（＋利益衡量）		公務：生命身體＋同意困難 非公務：○（＋利益衡量）		非公務：不限＋利益衡量／商業競爭＋不會揭露／信譽檢查	
美國CCPA*						
美國UPDPA*					限定項目	
日本*		生命身體財產＋難取得同意		生命身體財產＋難取得同意		
韓國		生命身體財產＋難以取得同意		生命身體財產＋難以取得同意	○＋利益衡量	
新加坡*	生命健康安全＋未能即時取得同意		生命健康安全＋未能即時取得同意		○＋利益衡量 改進商業	

*附註：
美國CCPA僅要求蒐集資料前有告知義務，並對出售個人資料有選擇退出權；
日本個資法僅規定：不得以虛偽或其他不正當手段取得個人資料；瑞士、新加坡及美國UPDPA未明確區分蒐集目的內、外

國家發展委員會

一般個資合法要件綜合比較（3/3）

41

國別	公開或取自一般來源		有利於當事人或對當事人無侵害	
	蒐集目的內	蒐集目的外	蒐集目的內	蒐集目的外
我國	公開：非公務 一般來源：非公務＋利益衡量		無侵害	有利當事人
歐盟				
德國				
英國				
瑞士	公開：當事人不反對（公務）		無侵害：經聯邦委員會許可（公務）	
美國CCPA*	排除公開資料適用	排除公開資料適用		
美國UPDPA*	排除公開資料適用	排除公開資料適用	○	
日本*				
韓國				
新加坡*	公開○			

*附註：
美國CCPA僅要求蒐集資料前有告知義務，並對出售個人資料有選擇退出權；
日本個資法僅規定：不得以虛偽或其他不正當手段取得個人資料；瑞士、新加坡及美國UPDPA未明確區分蒐集目的內、外

國家發展委員會

「個人資料保護法相關議題」第 2 場產學專家學者諮詢會議—蒐集、處理、利用特種個人資料合法要件（不含「當事人同意」要件）

議程

參、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及瑞士「聯邦個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議，聚焦於蒐集、處理及利用特種個人資料之合法要件（不含同意）探討。

壹、　議程

一、 主席致詞

二、 報告事項

「蒐集、處理、利用特種個人資料合法要件（不含「當事人同意」）」探討（國發會）

三、 討論事項

綜觀各國個人資料保護規範，在我國個資法規定尚未將

蒐集、處理及利用樣態整合為單一「處理」(Processing)行為前,特種個人資料之蒐集處理利用合法要件,若扣除同意要件,主要可歸納為:法律規定、公共利益、保護個人(含資料當事人及其他人)權利、當事人自行公開、對當事人權益有利、學術研究及非營利組織等 7 大類別。其中,除學術研究將另案討論,僅就其餘要件整理討論內容如下列案由。

案由一、我國特種個人資料之定義與範圍,考量科技發展及人權保障,是否有進一步擴張範圍之必要?是否需仿效日本、韓國等國家,採行例示規定之立法方式?

說明:

我國於 99 年修正個資法第 6 條,參考 1995 年歐盟資料保護指令、德國聯邦個人資料保護法第 13 條及奧地利聯邦個人資料保護法等外國立法例,個資法所稱之特種個人資料僅限於病歷、醫療、基因、性生活、健康檢查及犯罪前科等六種類別,並於個資法施行細則第 4 條為進一步定義。

(一)特種個人資料之定義與範圍

綜觀各國法制,有關特種個人資料之定義及範圍各有不同,多數國家承認健康、遺傳基因、性生活、種族、宗教或哲學信仰、政治傾向、工會身分、生物特徵識別資料等屬於特種個人資料之範疇。此外,美國基於交易安全之目的,承認金融帳戶、簽帳金融卡或信用卡號碼、存取憑證等金融資料亦屬於特種個人資料。目前僅新加坡未有明文規定特種個人資料,惟其針對身分證明號碼等敏感性資料有發布相關諮詢指南。

有關基因資料之範圍,我國僅限於去氧核醣核酸分析(DNA),而歐美體系則肯認其範圍包含染色體分析、核醣核酸分析(RNA)資料。而有關醫療資料、健康檢查資料,我國考量該等資料作成之主體及目的,須以醫事人員或醫療行為之目的所作成為限,惟歐美體系有關健康資料之概念,已包含我國之醫療、病歷及健康檢查之定義,且不侷限於以醫事人員或是醫療行為所作成之資料。復有關犯罪前科,我國實務有認為限於公務機關保存之犯罪前科,不包括依公開審理程序或起訴書、判決公告等合法程序已揭露之資料,日本則承認當事人作爲犯罪嫌疑人或被告,進行逮捕、搜索、扣押、拘留、提起公

訴及其他刑事案件相關程序亦屬於特種個人資料之範圍。

隨著近來引發諸多討論之人臉識別應用、穿戴式裝置等新興科技，蒐集臉部、指掌紋、聲紋等敏感個人資料，基於人權保障之目的，如何較周延地保護個人資料當事人之權益，亦值得進一步考量。

（二）法規要件標準之立法方式

我國與歐美國家對於特種個人資料均採行列舉規定，惟列舉規定較難與時俱進，且修法歷程較為冗長將影響法安定性。而日本、韓國採行例示規定，例如日本承認「其他對於當事人產生不當差別待遇、偏見及其他不利益者」、韓國承認「其他明顯侵害當事人隱私之資料」，並透過行政規則補充說明例示規定。

小結：請產學專家學者就我國現行特種個人資料之定義與範圍提供專業意見，是否有進一步擴張之必要性？若須擴張，則何者應該納入討論？是否需採行例示規定之立法方式？

案由二、以公務機關執行法定職務或非公務機關履行法定義務必要範圍內作為蒐集、處理或利用特種個人資料之合法要件之情形，該法律或法規命令所需具備蒐集、處理利用個人資料之具體化程度為何？

說明：

我國為使公務機關或非公務機關蒐集、處理或利用特種個人資料得依法為之，且依相關規定提供適當安全維護措施，爰仿 1995 年歐盟資料保護指令第 8 條及德國聯邦個人資料保護法第 28 條等外國立法例，於 99 年個資法修訂第 6 條第 1 項但書第 2 款規定。當蒐集、處理或利用特種個人資料，係屬公務機關執行法定職務或非公務機關履行法定義務必要範圍內，如檢警機關偵辦犯罪，蒐集或利用涉嫌人之犯罪前科資料；醫生發現疑似法定傳染病，蒐集相關醫療資料通報主管機關等，得依本款作為合法要件。另考量基於公益性及必要性，為協助公務機關執行法定職務或非公務機關履行法定義務，他機關須提供個資供該公務或非公務機關利用，惟該利用行為非他機關之法定職務，爰於 104 年新增第 5 款為協助公務機關執行法定

職務或非公務機關履行法定義務必要範圍內之合法要件。

有關個資法第 6 條第 1 項但書第 2 款及第 5 款所稱法定職務，依個資法施行細則第 10 條包括「法律、法律授權之命令、自治條例、法律或自治條例授權之自治規則、法律或中央法規授權之委辦規則」;而有關第 2 款及第 5 款所稱法定義務，依個資法施行細則第 11 條包括「法律、法律具體明確授權之法規命令」。參考國外立法例，以歐盟 GDPR 為例，GDPR 第 6 條第 3 項第 b 款規定，若援引法定職務、履定法定義務作為運用個資之合法要件，該法律應包括規範控管者運用個資之合法性一般條款、個資類型、個資當事人、揭露對象及目的、目的限制、儲存期間等具體規定；而我國未就該法律或法規命令所需具備之具體程度為相關規定，與歐盟 GDPR 所定之要求有所不同。

小結：請產學專家學者就我國現行「公務機關執行法定職務或非公務機關履行法定義務必要範圍內」合法要件，該法律或法規命令所需具備蒐集、處理利用個人資料之具體化程度為何，提供建議。

案由三、取自當事人自行公開或其他已合法公開資料之合法要件，於適用上是否須考量相容性及公開之情境脈絡？是否有必要限縮其範圍？

說明：

我國個資法於 99 年修訂時，考量當事人已自行公開或其他合法公開之個人資料，隱私已無被侵害之虞，爰修訂個資法第 6 條第 1 項但書第 3 款之規定。依個資法施行細則第 13 條規定，當事人自行公開之個人資料係指當事人自行對不特定人或特定多數人揭露其個人資料;已合法公開之個人資料則包括依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

綜觀多數國家均有當事人自行公開之合法要件，惟歐盟體系對於當事人自行公開之合法要件，限於明顯由當事人自行公開之特種個人資料，排除其他已合法公開資料。如新聞媒體處理特種個人資料，須限於當事人明顯有意公開資料，且進階利用仍須符合原始利用目的之相容性及其公開之情境脈絡。

其他已合法公開資料之合法要件僅我國、日本等少數國家有類似要件，且過往我國實務上，曾發生非公務機關引用法院公開之判決資訊，而認基於新聞報導之公益目的而蒐集當事人犯罪前科之資料係屬合法；惟當事人屬於非公眾人物且非基於特定公共利益為蒐集、處理或利用時，則認定該行為係屬違法。故此一要件操作上存在當事人之身分及公共利益衡量之爭議，爰有必要加以檢討。

小結：就此議題，請產學專家學者就以下議題提供建議：「取自當事人自行公開或其他已合法公開資料」在我國目前實務運作上曾發生爭議，以及此規定對非公務機關適用上，是否具有相當之重要性？且考量過去發生之爭議，是否須將利用目的相容性及公開之情境脈絡等納入規定？倘做上開修正，對於產業利用或當事人權益保障可能造成什麼影響？

案由四、除當事人同意與法律明文規定，是否考量納入其他合法要件？

說明：

（一）「公共利益」要件

以「公共利益」作為蒐集、處理利用之合法要件，於法理上並無不當。惟因其具備一定程度之不確定性，是否能以更清楚方式描述公共利益內涵，以使人民對規定能有更充分認識，從而降低適用上之困擾，亦值得進一步考量。

綜觀各國規定，多數國家均有以公共利益作為合法要件。在公共利益之類型化，得區分為重大公共利益、國防安全、司法訴訟、公共衛生等類型。在重大公共利益之定義上，歐盟、德國、英國要求應與當事人權益進行利益衡量。日本針對公共利益此一合法要件，並要求須難以取得當事人同意為限。

（二）「保護個人利益」要件

保護個人利益係以避免當事人及他人生命、身體危險作為蒐集、處理或利用特種個人資料之合法要件。綜觀歐盟體系及日本均承認保護個人利益之合法要件，且此「個人利益」包含當事人及其他人之權利。惟適用之權利類型，歐盟體系以生命、身體之權利為限；日本則除了承認生命、身體之權利外，

尚包括財產權利之類型。

然各國對於保護個人利益之合法要件，均限於難以取得當事人同意之情形，歐盟體系對此採取嚴格標準，須當事人因身體因素無法給予同意或被法律定義為無能力給予同意之情形，始得為之。

小結：根據以上觀察，請產學專家學者就以下兩項議題提供建議，以供參考：

(一)我國若採納「公共利益」作為蒐集、處理或利用特種個人資料之合法要件，是否有進一步類型化必要；若須類型化，則應採納何者？

(二)保護個人利益是否能為我國現行其他蒐集合法要件所涵蓋？適用之權利類型應為何者？是否限於當事人或他人之生命、身體、財產？是否須限於難以取得同意之情形？

蒐集、處理、利用之合法要件探討（特種個資）

國家發展委員會
110 年 11 月 3 日

背景說明

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為保障當事人個資安全及隱私保護，並同時促進資料流通及資料經濟，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用	產業應用	國際傳輸	受託處理者義務	框架性討論	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3										

大綱

2

一 討論範圍

二 議題分析

三 附件

一、 討論範圍（1/2）

3

■ 討論範圍

特種個資（除當事人同意、學術研究外）之蒐集、處理、利用合法性要件

■比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
瑞士	聯邦個人資料保護法	2021	GDPR適足性認定（指令時代取得）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法**非實定法律**，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2020	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（進入最終程序）
新加坡	個人資料保護法	2020	CBPR成員

一、 討論範圍（2/2）

4

■ 經整理各國蒐集、處理、利用合法要件，可分為以下 7 種類別：

	合法要件	說明
相似	法律規定	包含法定職務、法定義務，或其他法律授權蒐集處理利用
相似	公共利益	基於對國家或不特定多數人之利益保護
相似	保護個人利益	保護資料當事人或特定他人之利益或權利
各國規定差異較大	當事人自行公開	明顯已自行公開之個人資料
各國規定差異較大	有利於當事人	對資料當事人之利益或權利有助益
各國規定差異較大	學術研究（涉產業應用，將另案專題討論）	基於資料控管者之利益、權利所為之個資蒐集處理利用
各國規定差異較大	非營利組織	基於政治、哲學、宗教或工會之目的，就其合法活動過程中所為之處理

5

二、議題分析

(一)特種個人資料定義與範圍 (1/7)

6

■ 我國個資法相關規定

個人資料保護法	個人資料保護法施行細則
第6條 1. 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。	第4條 1. 本法第二條第一款所稱病歷之個人資料，指醫療法第六十七條第二項所列之各款資料。 2. 本法第二條第一款所稱醫療之個人資料，指病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方、用藥、施術或處置所產生之個人資料。 3. 本法第二條第一款所稱基因之個人資料，指由人體一段去氧核醣核酸構成，為人體控制特定功能之遺傳單位訊息。 4. 本法第二條第一款所稱性生活之個人資料，指性取向或性慣行之個人資料。 5. 本法第二條第一款所稱健康檢查之個人資料，指非針對特定疾病進行診斷或治療之目的，而以醫療行為施以檢查所產生之資料。 6. 本法第二條第一款所稱犯罪前科之個人資料，指經緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄。

(一)特種個人資料定義與範圍（2/7）

7

我國採取列舉規定：限於病歷、醫療、基因、性生活、健康檢查及犯罪前科共6種

類型	個人資料保護法施行細則	實務見解
病歷	依醫療法第67條第2項： 一、醫師依醫師法執行業務所製作之病歷。 二、各項檢查、檢驗報告資料。 三、其他各類醫事人員執行業務所製作之紀錄。	
醫療	病歷及其他由醫師或其他之醫事人員，以治療、矯正、預防人體疾病、傷害、殘缺為目的，或其他醫學上之正當理由，所為之診察及治療；或基於以上之診察結果，所為處方用藥、施術或處置所產生之個人資料。	非公務機關拍攝當事人就診影片，但攝影之活動並非醫療行為，而係以教學為目的之示範活動，自非特種個資（高雄106訴1221民決）
基因	限於去氧核醣核酸（DNA）	

(一)特種個人資料定義與範圍（3/7）

8

類型	個人資料保護法施行細則	實務見解
性生活	性取向或性慣行之個人資料。	
健康檢查	非針對特定疾病進行診斷或治療之目的而以醫療行為施以檢查所產生之資料。	業者蒐集、處理、利用民眾自行操作器材所得之生理數據資訊，若未涉及醫事人員診察（診斷）、治療，或以醫療行為施以檢查，非屬特種個資（國發會107年11月21日發法字第1072002136號）
犯罪前科	緩起訴、職權不起訴或法院判決有罪確定、執行之紀錄	實務有認為限於公務機關保存之犯罪前科，不包括依公開審理程序或起訴書、判決公告等合法程序已揭露之資料（台中108簡781刑決、彰化108簡1764刑決）；經通緝有案尚未結案之資料亦非屬特種個資（法務部107年3月6日法律字第10603517050號函）

(一)特種個人資料定義與範圍（4/7）

9

■ 國際立法例比較 - 母法規定

要件 / 國別	明文規範	要件標準	類別 ※各國針對各項類別範圍仍有差異									
			健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會身分	其他
我國	O	列舉	O	O		O	O					
歐盟	O	列舉	O	O	O	O	O	O	O	O	O	
德國	O	列舉	O	O	O	O	O	O	O	O	O	
英國	O	列舉	O	O	O	O	O	O	O	O	O	
瑞士	O	列舉	O	O	O	O		O	O	O	O	社會扶助措施
美國CCPA	O	列舉	O	O	O		O	O	O		O	身分號碼、金融資料、地理位置等
美國UPDPA	O	列舉	O	O		O	O	O	O			身分號碼、金融資料、地理位置等
日本	O	例示	O			O		O	O			社會身分等
韓國	O	例示	O				O		O	O	O	思想
新加坡	X	諮詢指南	無規定特種個資，所有個資適用相同規定									身分證明資訊

(一)特種個人資料定義與範圍（5/7）

10

■國際立法例比較結論

01

我國立法主要參考1995年歐盟資料保護指令及當時有效德國法

02

各國對於各類特種個資定義及範圍仍有差異

- 基因資料：歐盟體系包含染色體分析、DNA、RNA
- 健康資料：歐盟體系定義為與自然人身體及心理相關資料，且非以醫事人員或醫療行為所作成為限。
- 犯罪前科資料：日本包含對犯罪嫌疑人或被告進行逮捕、搜索、扣押、拘留、提起公訴及其他刑事案件相關程序。
- 生物特徵識別資料：歐美體系包含與自然人身體、心理、行為特徵相關資料。

國家發展委員會

(一)特種個人資料定義與範圍（6/7）

11

■ 討論重點

1

我國特種個人資料之定義與範圍，考量科技發展及人權保障，是否有進一步擴張範圍之必要？

- 基因資料是否應包含染色體分析、核醣核酸分析（RNA）？
- 是否以「有關健康之資料」取代病歷、醫療、健康檢查等資料？
- 犯罪前科資料是否應包含刑事案件相關程序？
- 考量新興科技興起，生物特徵識別資料是否應納入特種個資？

2

倘擴張特種個資之範圍，對產業利用可能造成什麼影響？

國家發展委員會

(一)特種個人資料定義與範圍（7/7）

12

■ 討論重點

3 由於列舉規定較難與時俱進，是否需仿效日、韓等國採例示規定之立法方式？

國別	例示規定	類型
日本	承認其他對於當事人產生不當差別待遇、偏見及其他不利益者	依個人資料保護法施行令第2條規定： 1. 身心功能障礙 2. 健康診斷及檢查 3. 醫療行為 4. 刑事案件相關程序 5. 少年保護事件相關程序
韓國	承認其他對當事人明顯侵害隱私之資料	依個人資料保護法施行細則第18條規定： 1. 基因檢測等獲得的DNA資料 2. 犯罪前科相關資料 3. 生物特徵識別資料 4. 種族或族裔起源資料

國家發展委員會

(二)蒐集、處理或利用之合法要件

13

■ 我國個資法相關規定

個人資料保護法	個人資料保護法施行細則
第6條 1. 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限： 一、法律明文規定。 二、公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。 三、當事人自行公開或其他已合法公開之個人資料。 五、為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內，且事前或事後有適當安全維護措施。	第9條 本法第六條第一項但書第一款……所稱法律，指法律或法律具體明確授權之法規命令。 第10條 本法第六條第一項但書第二款及第五款……所稱法定職務，指於下列法規中所定公務機關之職務： 一、法律、法律授權之命令。 二、自治條例。 三、法律或自治條例授權之自治規則。 四、法律或中央法規授權之委辦規則。 第11條 本法第六條第一項但書第二款及第五款……所稱法定義務，指非公務機關依法律或法律具體明確授權之法規命令所定之義務。 第13條 1. 本法第六條第一項但書第三款……所稱當事人自行公開之個人資料，指當事人自行對不特定人或特定多數人揭露其個人資料。 2. 本法第六條第一項但書第三款……所稱已合法公開之個人資料，指依法律或法律具體明確授權之法規命令所公示、公告或以其他合法方式公開之個人資料。

國家發展委員會

1、法定職務及法定義務（1/3）

14

■ 我國現行規定

個資法第6條第1項但書第2款及第5款

公務或非公務機關得蒐集、處理或利用特種個資情形：

a) 執行法定職務或法定義務必要範圍內 (第2款)

b) 為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內 (第5款)

立法理由

- 公務機關或非公務機關蒐集、處理或利用特種個資得依法為之，且依相關法令規定提供適當安全維護措施，爰仿1995年歐盟資料保護指令第8條及德國聯邦個人資料保護法第28條等外國立法例，而為第2款之規定。（99年個資法修訂）
- 基於公益性及必要性，公務機關執行法定職務或非公務機關履行法定義務，須請求他機關提供個資供該公務或非公務機關利用，惟該利用行為非他機關之法定職務，無法依第2款規定提供，爰為第5款規定。（104年個資法修訂）

國家發展委員會

1、法定職務及法定義務（2/3）

15

■國際立法例比較結論

■ 歐盟GDPR為例

- GDPR第6條第3項第b款規定，若援引執行法定職務、履行法定義務作為運用個資之合法要件，該法律內容可能包括規範控管者運用個資之合法性一般條款、個資類型、個資當事人、揭露對象及目的、目的限制、儲存期間等具體規定。

■ 日本、韓國、我國未就該法律或法規命令所需具備之具體程度為相關規定。

國家發展委員會

1、法定職務及法定義務（3/3）

16

■ 討論重點

1 我國現行以「公務機關執行法定職務或非公務機關履行法定義務必要範圍內」及「為協助公務機關執行法定職務或非公務機關履行法定義務必要範圍內」作為蒐集、處理或利用特種個資之合法要件，該法律或法規命令所需具備蒐集、處理利用個人資料之具體化程度為何？

2、當事人自行或已合法公開資料（1/3）

17

■ 我國現行規定

個資法第6條第1項但書第3款

公務或非公務機關得蒐集、處理或利用特種個資情形：

a) 當事人自行公開
b) 其他已合法公開之個人資料

立法理由

- 當事人已自行公開或其他合法公開之個人資料，隱私已無被侵害之虞，爰為第3款之規定。（99年個資法修訂）

2、當事人自行或已合法公開資料（2/3）

18

■國際立法例比較結論

01

利用當事人自行公開資料之限制

歐盟體系限於明顯由當事人自行公開，且進階利用仍須符合其公開之脈絡/相容目的

02

我國利用已合法公開資料之實務見解

我國實務上認為非公務機關基於新聞報導之公益目的，得引用法院公開之判決資訊，蒐集當事人犯罪個資；惟倘當事人非公眾人物且非基於特定公益，則利用該特種個資屬違法（高院109上易458刑決、臺北109訴2188民決）

	我國	歐盟	德國	英國	瑞士	美國CCPA	美國UPDPA	日本	韓國	新加坡
當事人自行公開	○	○	○	○	○		○	○		
其他已合法公開	○			承認國家較少				○		

國家發展委員會

2、當事人自行或已合法公開資料（3/3）

19

■ 討論重點

1 實務上，當事人自行公開或其他已合法公開資料此一合法性要件是否應保留？若保留，是否將目的相容性(例如公開之情境脈絡、當事人之身分及公共利益衡量等因素)納入規定？

2 倘修正此一要件，對於產業利用或當事人權益保障可能造成什麼影響？

國家發展委員會

3、公共利益或保護個人利益（1/5）

20

■ 我國現行規定

- 公共利益：未承認
- 保護個人利益：未承認

	我國	歐盟	德國	英國	瑞士	美國CCPA	美國UPDPA	日本	韓國	新加坡
公共利益		○	○	○	○		○	○		
保護個人利益		○	○	○	○		○	○		

多數國家列為合法要件

國家發展委員會

3、公共利益或保護個人利益（2/5）

21

■ 國際立法例比較 - 公共利益

國別	重大公共利益	國家高權	司法相關	其他
我國				
歐盟	○+利益衡量		○	○醫療及社會福利、公共衛生
德國	○+利益衡量	○國防安全	○追訴犯罪、執行刑罰	○健康照護或藥品醫材安全
英國	○+利益衡量		○	○公共衛生
瑞士				○研究、規劃或統計
美國CCPA				
美國UPDPA			○司法調查	○公共衛生、公共政策或其他一般公共利益
日本				○公共衛生、兒童發展之必要且難以取得同意
韓國				
新加坡				

多以類型化方式規定

要求利益衡量

國家發展委員會

3、公共利益或保護個人利益（3/5）

22

■ 國際立法例比較 - 保護個人利益

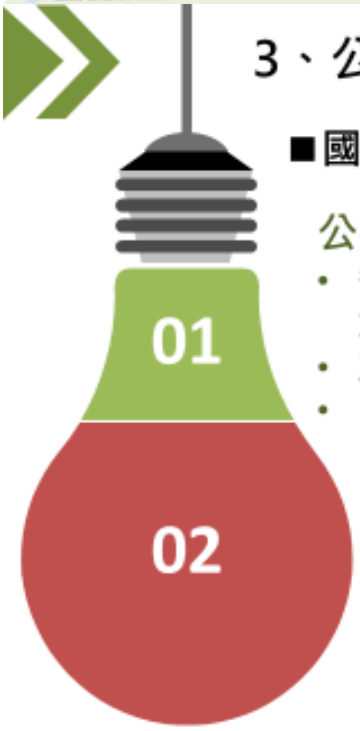
國別		生命	身體	財產	其他
我國	當事人				
	其他人				
歐盟	當事人	○	○		
	其他人	○	○		
德國	當事人	○	○		
	其他人	○	○		
英國	當事人	○	○		
	其他人	○	○		
瑞士	當事人	○	○		
	其他人	○	○		
美國CCPA	當事人				
	其他人				
美國UPDPA	當事人	○符合當事人期望			
	其他人				
日本	當事人	○	○	○	
	其他人	○	○	○	
韓國	當事人				
	其他人				
新加坡	當事人				
	其他人				

除美國UPDPA，其他國家對此要件均限於「難以取得當事人同意」之情形

國家發展委員會

3、公共利益或保護個人利益（4/5）

23



■國際立法例比較結論

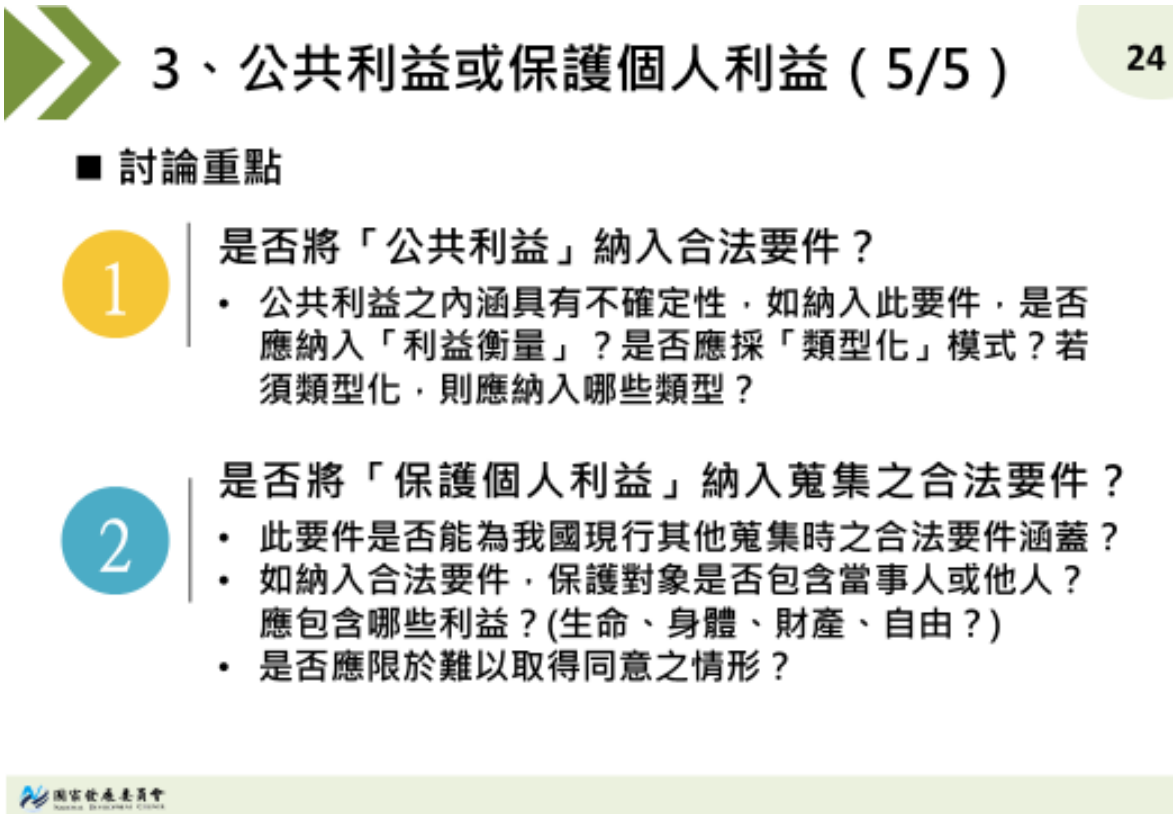
公共利益要件

- 各國普遍以類型化方式規範公共利益要件(如：重大公共利益、國防安全、追訴犯罪、司法調查等)。
- 重大公共利益須衡量當事人權益
- 日本限於難以取得當事人同意之情形

保護個人利益要件

- 多數國家承認保護範圍包含當事人及他人。
- 所稱利益以生命、身體(健康)為主，日本承認財產權利。
- 各國均限於難以取得同意。

國家發展委員會



三 附件
(一)各國特種個資合法要件

我國相關規定

26

最近一次個資法修正：2015年
CBPR成員國、GDPR適足性認定諮商中

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○	○		○	○					

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（含法定職務、法定義務）	
公共利益			
當事人自行公開		○ 包含其他已合法公開之個人資料	
保護個人利益	當事人		
	其他人		
有利於當事人			
學術研究		○ 限於醫療、衛生或犯罪預防目的為統計或學術研究必要且經去識別化	
非營利組織			

歐盟相關規定（1/2）

27

最近一次個資法修正：2016年（2018年施行）

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○	○	○	○	○	○	○	○	○	

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（勞動法、社會安全法、社會保護法）	若與原目的相容，則可使用。 *科學、歷史、統計例外情形原則上視為與原目的相容
公共利益		○	
當事人自行公開		○	
保護個人利益（生命、健康）	當事人	○（無法給同意：身體因素、無行為能力）	
	其他人	○（無法給同意：身體因素、無行為能力）	
有利於當事人			
學術研究		○（科學、歷史、統計 +適當保護措施）	
非營利組織		○（合法活動範圍內、與特定人員有關）	

歐盟相關規定（2/2）

28

特種個資	健康相關	遺傳基因	生物識別資料
列舉	定位或路徑如用於診斷有無確診新冠肺炎，則變成健康相關資料。	• 染色體分析 • 去氧核醣核酸分析 • 核醣核酸分析	• 臉部圖像 • 指掌紋

未明定以下是特種個資，但有特別規定蒐集、處理、利用之合法要件：

- **犯罪紀錄**
  - 唯有符合GDPR第6條第1項的合法處理要件，且受主管機關監管或基於歐盟成員國國內法規定，且採取適當安全措施時，得處理與犯罪紀錄相關的個人資料。
- **未成年人（孩童）**
  - 當孩童在使用資料社會服務（information society services）時，控制者唯有在孩童年齡超過16歲的情形，得以同意作為處理個人資料的合法要件。
  - 小於16歲，由法定代理人給予同意或孩童之同意經法定代理人認可。
  - 另歐盟成員國得自立國內法下修16歲的規定，但不得小於13歲。

＊歐盟成員國得對**遺傳基因、生物識別及健康相關**資料訂定相關法規，限制資料處理。

德國相關規定

29

最近一次個資法修正：2021年6月23日
歐盟成員國

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	O	O	O	O	O	O	O	O	O	

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內（*為公務機關才可適用類型）	目的範圍外利用（下列+左邊事由之一）	
			公務機關	非公務機關
法律規定		O（社會安全及社會保障權利+履行義務之必要）		
公共利益		O（限於公共健康、健康照護或藥品醫材安全、公共安全*、重大公共利益*、國防安全*）	O（公共利益、刑事責任、監管）	O（防止國家/公共危害/追訴犯罪）
當事人自行公開		O（限明顯自行公開）		
保護個人利益	當事人	O（無法給同意：身體因素、無行為能力）	O（明顯維護利益+無理由拒絕）	
	其他人	O（保護重大利益+處理必要性+利益衡量）	O（權利嚴重損害）	O（民事請求權）
有利於當事人				
學術研究		O（科學、歷史、統計+適當保護措施）		
非營利組織		O（合法活動範圍內、與特定人員有關）		

英國相關規定

30

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國，GDPR適足性認定（2021）

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○	○	○	○	○	○	○	○	○	

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（勞動法、社會安全法、社會保護法）	若與原目的相容，則可使用。 *科學、歷史、統計例外情形原則上視為與原目的相容
公共利益		○	
當事人自行公開		○	
保護個人利益（生命、健康）	當事人	○（無法給同意：身體因素、無行為能力）	
	其他人	○（無法給同意：身體因素、無行為能力）	
有利於當事人			
學術研究		○（科學、歷史、統計+適當保護措施）	
非營利組織		○（合法活動範圍內、與特定人員有關）	

瑞士相關規定（1/2）

31

最近一次個資法修正：2021年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○	○	○	○		○	○	○	○	○（社會扶助）

蒐集、處理、利用之合法要件	蒐集、處理目的範圍內		目的範圍外利用	
	公務機關	非公務機關	公務機關	非公務機關
法律規定	○（原則→法律；例外（法定任務之不可或缺行為）→法規命令）	○（例外：檢查當事人信用→不可使用特種個資）	○（原則→法律；例外（法定任務之不可或缺行為）→法規命令）	
公共利益	○（規劃、統計；需向第三人揭露時，須去識別）	○（規劃、統計；需向第三人揭露時，須去識別）	○（規劃、統計；需向第三人揭露時，須去識別）	
當事人自行公開	○（當事人無明確禁止）		○（當事人無明確禁止）	

瑞士相關規定（2/2）

32

最近一次個資法修正：2021年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	O	O	O	O		O	O	O	O	O（社會扶助）

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內		目的範圍外利用	
		公務機關	非公務機關	公務機關	非公務機關
保護個人利益	當事人	O（限生命、身體完整與安全+當事人無法及時同意）		O（限生命、身體完整與安全+當事人無法及時同意）	
	其他人	O（限生命、身體完整與安全+當事人無法及時同意）		O（限生命、身體完整與安全，且當事人無法及時同意）	
有利於當事人		O（對當事人不構成任何特別風險）		O（對當事人不構成任何特別風險）	
學術研究		O（需向第三人揭露時，須去識別）	O（需向第三人揭露時，須去識別）		

美國相關規定（CCPA）

33

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

定義	類型									※醫療、健康、臨床實驗資料適用特別法（CAL. CIV. CODE § 1798.145.）
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	O	O	O		O	O	O		O	O(身分號碼、金融資料、地理位置等)

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定			
公共利益			
當事人自行公開			
保護個人利益	當事人		
	其他人		
有利於當事人			
學術研究			
非營利組織			

CCPA 僅要求蒐集資料前有告知義務，
並賦予當事人事後限制利用與揭露、選擇退出等權利（16歲以下為選擇加入）

美國相關規定（UPDPA）

34

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○	○		○	○	○	○			○(身分號碼、金融資料、地理位置等)

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（法定義務）	
公共利益		○（法令遵循、犯罪預防等）	
當事人自行公開		○（符合當事人期望）	
保護個人利益	當事人	○（有利於當事人）	
	其他人		
有利於當事人		○	
學術研究		○（公共利益相關研究）	
非營利組織			

UPDPA似未嚴格區分是否為蒐集目的範圍內之處理、利用

日本相關規定

35

最近一次個資法修正：2021年
CBPR成員國、GDPR適足性（2019）

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
列舉	○			○		○	○			○(社會身分等)

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○（含法定職務、法定義務）	
公共利益		○ 為提升公眾衛生或推廣兒童健全發育有特別必要且難以取得當事人同意	
當事人自行公開		○	
保護個人利益	當事人	○ 包含生命、身體、財產，難以取得當事人同意且有必要時	
	其他人	○	
有利於當事人			
學術研究		○	
非營利組織			

韓國相關規定

36

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定進入最終程序

定義	類型									
	健康相關	遺傳基因	生物識別資料	犯罪紀錄	性生活	種族	宗教信仰	政治	工會	其他
例示	○				○		○	○	○	○(思想)

蒐集、處理、利用之合法要件		蒐集、處理目的範圍內	目的範圍外利用
法律規定		○	
公共利益			
當事人自行公開			
保護個人利益	當事人		
	其他人		
有利於當事人			
學術研究			
非營利組織			

新加坡相關規定

37

最近一次個資法修正：2020年
CBPR成員國

將影響個資安全維護措施之要求程度
進而影響是否加重減輕罰款額度之判斷

定義

無明文規定特種或敏感個資，但透過諮詢指南承認部分個資具有**敏感性**：

列舉

- 身分資訊（國民登記身分證及護照號碼）
- 金融財務資訊（交易及支付明細）
- 保險資訊（要保人或受益人姓名）
- 個人犯罪紀錄
- 醫療敏感資訊
- 未成年人個資

身分證明資訊

- 自2019年9月1日起，不得蒐集、利用、保存或揭露國民身分證或其他類似形式的身分證明（例如：出生證明、長期居留證或工作許可證、護照、駕照等）之號碼、複製本或實體卡片
- 蒐集、利用、揭露之合法要件
  - ☐ 符合二種情形之一，經通知目的並取得同意：
    - ✓ **法有明文**：其他法律明文（例如：入學或入職所必要）或PDPA例外規定（例如：視為同意或例外允許未經同意之蒐集、利用或揭露行為）
    - ✓ **高度確認真實性必要**：避免安全風險（例如：幼兒園訪客管制）、組織重大影響或損失（例如：詐騙行為）必須精準驗證或核對個人身分
  - ☐ 明確解釋蒐集、利用、揭露之必要性
  - ☐ 確實採取充足安全維護措施
  - ☐ 遵守PDPA責任義務

(二)綜整各國特種個資合法要件

特種個資合法要件綜合比較（1/2）

39

■ 國際立法例比較

國別	法律規定	公共利益	保護個人利益	當事人自行公開	有利於當事人	非營利組織	學術研究（另案討論）
我國	○（含法定義務、法定職務）			○（含其他已合法公開資料）			○（限特定目的）
歐盟	○（限於勞動法、社會安全法、社會保護法之法定義務）	○	○（當事人、他人，限無法給同意：身體因素、無行為能力）	○（限明顯自行公開）		○（合法活動範圍內、與特定人員有關）	○（科學、歷史、統計 +適當保護措施）
德國	○（社會安全及社會保障權利+履行義務之必要）	○（限於公共健康安全、國防安全）	○（當事人:限明顯身體或法律無法給予同意；他人：保護重大利益+處理必要性+利益衡量）	○（限明顯自行公開）		○（合法活動範圍內、與特定人員有關）	○（科學、歷史、統計 +適當保護措施）
英國	○（限於勞動法、社會安全法、社會保護法之法定義務）	○	○（當事人、他人，限無法給同意：身體因素、無行為能力）	○（限明顯自行公開）		○（合法活動範圍內、與特定人員有關）	○（科學、歷史、統計 +適當保護措施）
瑞士	○	○（研究、規劃或統計）	○（生命、身體完整與安全）	○（限明顯自行公開）			○（研究、規劃或統計）

特種個資合法要件綜合比較（2/2）

■ 國際立法例比較

國別	法律規定	公共利益	保護個人利益	當事人自行公開	有利於當事人	非營利組織	學術研究（另案討論）
美國CCPA	適用一般個資規定						
美國UPDPA	○（法定義務）	○（法令遵循、犯罪預防等）	○（符合當事人期望）	○（有利於當事人）	○		○（公共利益相關研究）
日本	○（法定職務、法定義務）	○（公眾衛生或兒童健全發育+難以取得當事人同意）	○（當事人他人，含生命、身體、財產+難以取得當事人同意且有必要時）	○			○
韓國	○						
新加坡	適用一般個資規定						

「個人資料保護法相關議題」第 3 場產學專家學者諮詢會議—產業應用

議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及菲律賓「隱私保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於產業應用有關科學研究之探討。

貳、議程

一、 主席致詞

二、 報告事項

產業應用探討（國發會）

三、 討論事項

我國有關因科學研究而蒐集、處理及利用個人資料之規定，規範於個資法第 6 條第 1 項第 4 款「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而

有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」、第 16 條第 5 款「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」、第 19 條第 1 項第 4 款「學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」以及第 20 條第 1 項第 5 款「公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」針對上述規定，蒐整司法判決及實務見解，進行比較法之分析，並提出下列三項案由。另有關去識別化及當事人權利限制置於其他場次討論。

案由一、有關學術研究條款之相關定義討論

說明：

一、各國概念用語之比較

綜觀各國法制，個資法有關研究之相關規定可分為「研究」、「科學研究」及「學術研究」之規範用語。規定「研究」（research）之國家，包含美國、新加坡及菲律賓；而歐盟、英國、德國及韓國則以「科學研究」（scientificresearch；wissenschaftliche Forschung；과학적연구）作為個資法規範規定；而我國及日本則係以「學術研究」（学術研究）作為條文用語。

二、我國現行用語之解釋

有關學術研究之具體內涵，參照司法院釋字第 380 號解釋及其協同意見書、法務部 104 年 7 月 2 日法律字第 10403508020 號函釋，所謂「學術研究」，係指針對有系統而較專門之學問中的特定主題，作深入且有系統的探討或研查，以發現事實，形成理論並付諸應用。惟上述說明均屬抽象之法律概念，尚難遽定其範圍及認定標準，仍宜依具體個案分別認定之。

小結：請產學專家學者就以下議題提供建議：

(一) 綜觀其他國家之法律概念，是否需調整我國個資法「學

術研究」之法律用語？是否需包含「產業研究」之概念？相關解釋對於產業之影響為何？

(二) 學術或科學研究既屬於不確定法律概念，且可能涉及學術研究機構之解釋，應留於主管機關規範，或個資法有清楚定義之必要？如要定義，應否以符合特定研究方法或倫理標準之研究為限？

案由二、因學術研究條款而蒐集、處理或利用個人資料合法要件之探討

說明：

一、要件適用之蒐集主體或提供對向範圍

(一)我國於特種個資部分(個資法第 6 條第 1 項第 4 款規定)

特定目的下之蒐集、處理或利用主體以及目的外利用提供對象皆限於公務機關或學術研究機構。

(二)我國於一般個資部分（個資法第 16 條第 5 款、第 19 條 1 項第 4 款及第 20 條第 1 項第 5 款規定）

非公務機關特定目的下蒐集、處理或利用主體限於學術研究機構公務及非公務機關特定目的外利用之提供對象，則以公務機關或學術研究機構為限。

經比較其他國家個資法之規定，有關科學研究之適用主體，歐盟、英國、德國、美國、韓國、新加坡等國家則不以公務機關或學術研究機構為限。

二、「學術研究機構」之定義

若上開條款之蒐集主體或提供對象有納入「學術研究機構」用語，則現行無任何立法定義，另大學法、學術研究機構設立辦法或法務部 98 年 11 月 16 日法律決字第 0980047501 號函釋等內容，並無統一定義。參考日本於 2021 年 5 月修正之個資法(令和 3 年改正個人情報保護法)規定，所謂「學術研究機關等」係指大學及其他以學術研究爲目的之機關或團體(私立大學、公益法人等機關或學會)，或所屬人員。是否值得我國作為立法上之參考。

三、要件適用是否限於特定原因或領域之研究行為

依我國個資法第 16 條第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款之規定，一般個資限於基於「公共利益」為目的而為統計或學術研究而有必要；第 6 條第 1 項第 4 款規定以「醫療、衛生或犯罪預防目的」，始得蒐集、處理或利用個人資料。但觀察歐盟、英國及德國之規定，主要回歸適用一般個資或特種個資之合法處理事由；另觀察美國、日本、韓國、新加坡等國家，基於研究目的或科學研究之目的，即得作為合法事由，而無須再限於某種特定原因或領域之研究行為，爰有探討我國個資法之必要。

四、要件適用是否搭配特殊保護措施

如未來我國個資法參考上述國家之規定，依個人資料之屬性，符合一般或特種個人資料之合法事由，或以研究目的或科學研究之目的等規範模式立法時，是否就「特種個人資料」再參考其他國家立法例，例如：禁止對當事人造成重大危害之處理、特殊利益衡量或經委員會審查等特殊規定，針對特種個人資料提供特殊適當之保護措施。

小結：請產學專家學者就以下議題提供建議：

(一) 比較各國規範及產業實務運用，我國適用主體限於公務機關或學術研究機構，是否有鬆綁之必要？

(二) 針對「學術研究機構」目前未有統一之法律規定，我國個資法是否有定義之必要？如需定義，是否參考日本新修正個資法有關學術研究機關等之規範？

(三) 我國因學術研究處理個資限於特定目的之規範，對於產業適用上是否產生阻礙？

(四) 綜觀先進國家對於特種個資所提供之特殊保護措施，是否有我國值得參考之處？

案由三、個資法有關學術研究而蒐集、處理或利用個人資料之其他特殊彈性規範

說明：

我國個資法第 9 條第 2 項第 4 款規定，公務機關或非公務機關依第 15 條或第 19 條規定蒐集非由當事人提供之一般個人資料，若基於公共利益為統計或學術研究之目的而有必要，且且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者，得於處理或利用前免為告知個人資料來源及第 8 條第 1 項第 1 款至第 5 款所列事項。有關特種個人資料之免告知義務，則係第 6 條第 2 項準用第 9 條第 2 項第 5 款之規定。

觀察歐盟國家針對科學研究之彈性規定，包含允許就科學研究之進階處理不視為與原始目的不相容、可延長一定儲存期間；或德國關於公開研究成果等規定，相關特殊規範是否可作為我國未來修法之借鏡。

小結：目前我國就學術研究之彈性規定，包含告知義務規定。就比較法之規定，個資法彈性之規定包含延長儲存期限、公開研究成果等特殊規定，有無值得我國參考之處？

產業應用
（科學研究）

國家發展委員會
110 年 12 月 6 日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	**產業應用（科學研究）**	產業應用	國際傳輸	受託處理者義務	框架性討論	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6									

大綱

2

一 討論範圍

二 議題分析

三 附件

一、討論範圍

3

■ 討論範圍

產業應用，以「科學研究」為主軸，有關假名化、匿名化及當事人權利限制置於其他場次討論，並以「個資法」為主要討論範疇。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
	健康保險可攜性及責任法（HIPAA）	2006	
日本	個人資料保護法	2020	CBPR成員、GDPR適足性（2019）*
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（進入最終程序）
新加坡	個人資料保護法	2020	CBPR成員
菲律賓	隱私保護法	2012	

*「學術研究」規定排除於GDPR適足性認定。

大綱

4

一 討論目的及範圍

二 議題分析

三 附件

二、議題分析 (1/2)

5

■ 我國個資法之相關規定

一般個人資料		特種個人資料
公務機關	非公務機關	
第16條第5款 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符。但有下列情形之一者，得為特定目的外之利用： 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。	**第19條第1項第4款** 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 **第20條第1項第5款** 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用： 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。	**第6條第1項第4款規定** 有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限： 四、公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。

二、議題分析 (2/2)

6

■ 我國個資法之相關規定

合法要件	一般個資		特種個資
	目的內	目的外	
適用主體	學術研究機構	公務機關或學術研究機構	
合法事由	基於**公共利益**為統計或學術研究而有必要		基於**醫療、衛生或犯罪預防之目的**，而為統計或學術研究有必要
保護措施	資料經提供者處理後/經蒐集者依其揭露方式**無從識別特定之當事人**		
彈性規定	間接蒐集得免為處理或利用前之**告知義務**		

(一)有關學術研究條款之相關定義討論(1/3)

7

我國個資法及施行細則針對「學術研究」並無明確性定義

國家	規範用語	定義說明	適用個資法？
我國	學術研究	N/A	O
歐盟	科學研究	包含科技發展及成果展示、基礎理論研究、應用研究及私人贊助研究等，但須依照各專業領域的研究方法執行，符合倫理標準等要求。	O
英國			O
德國			O
美國	研究	目的在發展及促進公共或科學知識之科學分析、系統研究與觀察，並應遵守所有相關適用的道德與隱私法律。	O
日本	學術研究	N/A	Δ 2022年4月特定情形適用個資法
韓國	科學研究	技術的開發與實證、基礎研究、應用研究及民間投資研究等使用科學方法的研究。	O
新加坡	研究	組織為進行研究或促進業務改進之研發活動，研發應用包括產品、服務、業務營運或市場銷售。	O
菲律賓	研究	為發展或促進可歸納的知識所進行之活動，或使用科學方法觀察、推理、分析及累積任何資訊的活動。	X 應遵循國家隱私委員會(NPC)意見

藍色：非法律明文規定

(一)有關學術研究條款之相關定義討論(2/3)

8

參考司法實務之解釋

國家	規範用語
我國	學術研究
歐盟	科學研究
英國	科學研究
德國	科學研究
美國	研究
日本	學術研究
韓國	科學研究
新加坡	研究
菲律賓	研究

- 所謂「學術研究」，係指針對有系統而較專門之學問中的特定主題，作深入且有系統的探討或研查，以發現事實，形成理論並付諸應用。因均屬抽象之法律概念，故尚難遽定其範圍及認定標準，仍宜依具體個案分別認定之。（法務部民國104年7月2日法律字第10403508020號）
- 憲法第十一條關於意見自由之保障，除於「言論自由」「著作自由」「出版自由」之外，復揭櫫「講學自由」乙項，揆其目的當在積極的鼓勵科學之研究（自然科學與社會科學），而以此使學者能夠獲得充分研究之自由，...所謂大學自治，係以學術研究之自由與其研究結果發表之自由（即講學自由）為中心，而此學術研究之自由與講學之自由，合而為一，即一般所稱之「學術自由」。（參考司法院釋字第380號協同意見書）

國家發展委員會

(一)有關學術研究條款之相關定義討論(3/3)

9

1 我國個資法以「學術研究」作為法律概念，是否需放寬？

- 綜觀歐盟、韓國(科學研究)，以及美國、新加坡(研究)之法律概念，是否需調整我國個資法「學術研究」之法律概念？是否需包含「產業研究」之概念？相關解釋可能對產業造成什麼影響？

2 學術或科學研究既屬於不確定法律概念，是否有清楚定義之必要？

- 學術或科學研究既屬於不確定法律概念，且可能涉及案由二該類條款適用之蒐集主體或提供對象之解釋，應留於主管機關規範，或個資法有清楚定義之必要？如要定義，應否以符合特定研究方法或倫理標準之研究為限？

國家發展委員會

(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(1/6)

10

*限於德國
**UPDPA規定
灰色：新法尚未施行
藍色：依NPC諮詢意見

國家		適用主體	合法事由（除當事人同意外）	管理措施	其他
我國		• 公務機關 • 學術研究機構	基於公共利益/醫療/衛生/犯罪預防目的+為統計或學術研究有必要	資料經提供者處理後/經蒐集者依其揭露方式無從識別特定之當事人	特種個資另有人體研究法、人體試驗及人體生物資料庫管理規定
歐盟		無限制	• 公共利益 • 執行職務所必要行使公權力所必要 • 追求正當利益所必要+利益衡量	對資料當事人之權利和自由提供適當保護措施，並應採取技術+組織上之措施+遵守最小化利用原則 *針對特種個資另有嚴格適當且具體之措施規定	
英國					• 禁止對當事人造成重大危害/痛苦之處理 • 醫學研究應經相關委員會核准
德國*					特種個資有特殊利益衡量
美國	UPDPA**	無限制	符合當事人期望/有利當事人+相容性作業資料判斷	落實合理資料安全措施+資料隱私與安全風險評估	• 醫療資料適用HIPAA；臨床實驗或其他生物醫學研究之個資應從其特別規定 • 不得對特定個人進行預測/決定**
	CCPA		基於研究之目的	落實明列之適當安全措施	
	HIPAA	健康計畫/健康照顧清算中心/健康資訊之健康照顧提供者	• 事前告知+選擇同意 • 經研究倫理/隱私委員會審查	管理安全+物理+技術上保護措施，應符合「電子保護健康資料之安全標準規則」	
日本		大學及其他以學術研究為目的之機構/團體/所屬人員	以學術研究為目的之活動	採取必要適當之安全管理措施，對從業人員或受委託人之適當監督	醫療個資另有「次世代醫療基盤法」加以規範
韓國		無限制	基於科學研究之目的	應進行假名化之處理	欲連結假名化資料，應取得指定之專門機關許可
新加坡		無限制	符合「視為同意」之情形	評估以消除或減輕不利影響+充分告知	不以單獨識別個人形式將無法合理實現目的
			基於促進業務改進之目的	須合理實現目的+一般人認為符合適當蒐集個資之情形	
			基於研究之目的	須合理實現目的+不切實際+公共利益+不影響個人+無法識別個人	
茅律置		無限制	基於科學/統計研究之目的	應落實明訂之管理措施	特種個資應符合專業倫理規則

(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(2/6)

11

*限於德國
**UPDPA規定
灰色：新法尚未施行
藍色：依NPC諮詢意見

國家		適用主體
我國		• 公務機關 • 學術研究機構
歐盟		無限制
英國		
德國*		
美國	UPDPA**	無限制
	CCPA	
	HIPAA	健康計畫/健康照顧清算中心/健康資訊之健康照顧提供者
日本		大學及其他以學術研究為目的之機構/團體/所屬人員
韓國		無限制
新加坡		無限制
茅律置		無限制

要件適用之蒐集主體或提供對象範圍		
我國	特種個資	特定目的下之蒐集、處理或利用主體以及目的外利用提供對象，皆限於公務機關或學術研究機構。
	一般個資	非公務機關特定目的下蒐集、處理或利用主體限於學術研究機構，公務及非公務機關特定目的外利用之提供對象，則以公務機關或學術研究機構為限。
國際立法例比較		有關科學研究之適用主體，歐盟、英國、德國、美國、韓國、新加坡等國家不以公務機關或學術研究機構為限。

1

我國個資法有關「公務機關或學術研究機構」之適用主體議題

- 比較各國規範及產業實務運用，我國適用主體限於公務機關或學術研究機構，是否有鬆綁之必要？

(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(3/6)

12

參考我國相關規定

- 大學為發揮教育、訓練、研究、服務之功能，得與政府機關、事業機關、民間團體、學術研究機構等辦理產學合作...。（大學法第38條）
- 本辦法所謂學術研究機構，係指國立研究院及私立大學研究所以外之學術研究機構。（學術研究機構設立辦法第2條）

2 我國個資法需否清楚界定「學術研究機構」定義？

1) 針對「學術研究機構」目前未有統一之法律規定，我國個資法是否有定義之必要？如需定義，是否參考日本新修正個資法有關學術研究機關等，即大學及其他以學術研究為目的之機關或團體，或所屬人員之規範？

國家發展委員會

(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(4/6)

13

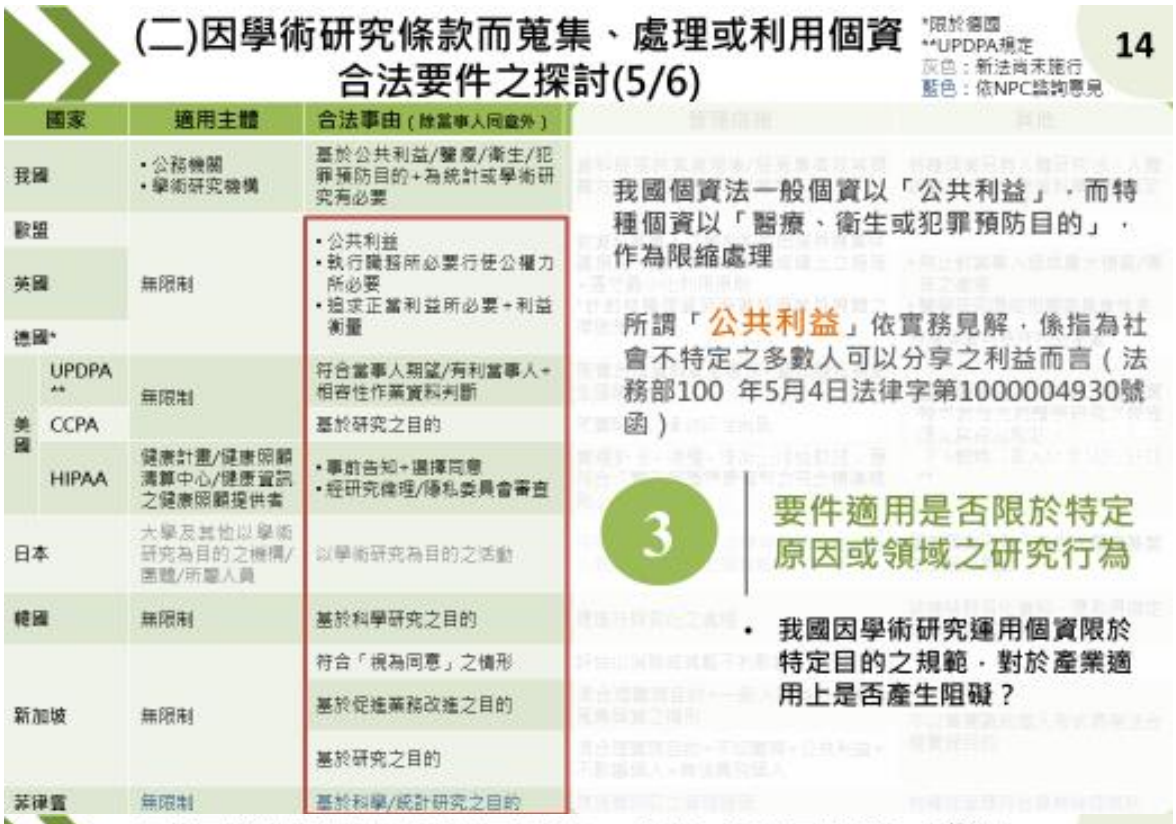
個資法學術研究要件，我國實務相關之爭議問題

- 之前「國家衛生研究院全民健康保險資料庫申請使用作業要點」包含非營利研究機構或個人。目前「各機關申請提供戶籍資料及親等關聯資料辦法」或「全民健康保險保險人資訊整合應用服務中心作業要點」，皆以公務機關或學術研究機構為限。
- 但實務上常有基於研究目的而以個人名義處理或利用個資，而違反個資法或判決訴訟之爭議（法務部103年4月9日法律字第10303503970號、臺北高等行政法院106年度訴字第283號判決）

2 我國個資法需否清楚界定「學術研究機構」定義？

2) 實務上對於「個人名義」之申請素有爭議，若未來參考日本新修正之個資法規定，是否應於個資法內明訂？或允許主管機關以行政規則方式擴張解釋？

國家發展委員會


(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(5/6)
*限於德國
**UPDPA規定
灰色：新法尚未施行
藍色：依NPC諮詢意見
14
國家
適用主體
合法事由（除當事人同意外）
我國
・公務機關
・學術研究機構
基於公共利益/醫療/衛生/犯罪預防目的+為統計或學術研究有必要
歐盟
英國
德國*
無限制
・公共利益
・執行職務所必要行使公權力所必要
・追求正當利益所必要+利益衡量
美國
UPDPA**
無限制
符合當事人期望/有利當事人+相容性作業資料判斷
CCPA
基於研究之目的
HIPAA
健康計畫/健康照顧清算中心/健康資訊之健康照顧提供者
・事前告知+選擇同意
・經研究倫理/隱私委員會審查
日本
大學及其他以學術研究為目的之機構/團體/所屬人員
以學術研究為目的之活動
韓國
無限制
基於科學研究之目的
新加坡
無限制
符合「視為同意」之情形
基於促進業務改進之目的
基於研究之目的
英屬
無限制
基於科學/統計研究之目的
我國個資法一般個資以「公共利益」，而特種個資以「醫療、衛生或犯罪預防目的」，作為限縮處理
所謂「公共利益」依實務見解，係指為社會不特定之多數人可以分享之利益而言（法務部100 年5月4日法律字第1000004930號函）
3
要件適用是否限於特定原因或領域之研究行為
・ 我國因學術研究運用個資限於特定目的之規範，對於產業適用上是否產生阻礙？

(二)因學術研究條款而蒐集、處理或利用個資合法要件之探討(6/6)
*限於德國
**UPDPA規定
灰色：新法尚未施行
藍色：依NPC諮詢意見
15
國家
其他
我國
歐盟
英國
德國*
美國
UPDPA**
CCPA
HIPAA
日本
韓國
新加坡
英屬
我國個資法一般個資以「公共利益」，其以「醫療、衛生或犯罪預防目的」，作為限縮特種個資之處理。
・ 2015年修法前，個資法第6條第1項第4款規定「公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且經一定程序所為蒐集、處理或利用之個人資料。」並刪除第2項授權辦法之規定。
・ 其將刪除程序控管之相關規範，修法理由指明基於資料之合理利用，鬆綁以促進學術研究發展，並由公務機關自行制訂行政規則。
特種個資另有人體研究法、人體試驗及人體生物資料庫管理規定
・禁止對當事人造成重大危害/痛苦之處理
・醫學研究應經相關委員會核准
特種個資有特殊利益衡量
・醫療資料適用HIPAA；臨床實驗或其他生物醫學研究之個資應從其特別規定
・不得對特定個人進行預測/決定**
醫療個資另有「次世代醫療基盤法」加以規範
欲連結假名化資料，應取得指定之專門機構許可
不以單獨識別個人形式將無法合理實現目的
特種個資應符合專業倫理規則
4
參考其他國家對於特種個資所提供之特殊保護措施，是否有我國值得參考之處？
・ 若未來合法事由參考其他國家之規範模式，則有關特種個資之保護，例如個資法明訂禁止(英)、特殊利益衡量(德)或委員會審查(英美)之規定，是否可供我國參考？

(三)個資法有關學術研究而蒐集、處理或利用個資之特殊彈性規範(1/2)

*限於德國
灰色：日本新修正之個資法尚未施行

16

國家	儲存時間延長	免除告知	公開研究成果	其他特殊規定
我國		間接蒐集免告知義務		
歐盟				
英國	• 可延長儲存期間 • 識別特定/可得特定之標記可以不用分開儲存*	提供資料之時間/精力，對科學研究造成影響，得免告知義務		
德國*			• 取得同意 • 歷史事件不可或缺	
美國				
日本			學術研究成果公佈/教授不得已時+不侵害個人權利或利益	
韓國				
新加坡		• 基於促進業務改進目的 • 基於研究目的	必須以無法識別個人之形式公布結果	遵守資料共享政策，得豁免PDPA規定
菲律賓	得延長儲存期間			

國家發展委員會

(三)個資法有關學術研究而蒐集、處理或利用個資之特殊彈性規範(2/2)

17

我國個資法針對「學術研究」之告知義務有彈性規範

一般個人資料	特種個人資料
第9條 一、公務機關或非公務機關依第15條或第19條規定蒐集非由當事人提供之個人資料，應於處理或利用前，向當事人告知個人資料來源及前條第1項第1款至第5款所列事項。 二、有下列情形之一者，得免為前項之告知： 4.基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。	第6條 一、有關病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，不得蒐集、處理或利用。但有下列情形之一者，不在此限：(略) 二、依前項規定蒐集、處理或利用個人資料，準用第8條、第9條規定…。

1

我國個資法就學術研究之規範，有無增訂特殊彈性之必要？

目前我國就學術研究之告知義務有彈性規範，就比較法之規定有無值得我國參考之處？

- 例如歐盟儲存限制的放寬規定
- 例如德國及日本得基於研究成果而公開個人資料
- 參考簡報附件有關新加坡資料共享制度，資料得於組織內部間流通

國家發展委員會

18

案由一：有關學術研究條款之相關定義討論

- 我國個資法以「學術研究」作為法律概念，是否需調整用語？是否需包含「產業研究」之概念？
- 學術或科學研究既屬於不確定法律概念，是否有清楚定義之必要？

案由二：因學術研究條款而蒐集、處理或利用個資合法要件之探討

- 比較各國規範及產業實務運用，我國適用主體限於公務機關或學術研究機構，是否有鬆綁之必要？
- 我國個資法需否清楚界定「學術研究機構」定義？
- 我國因學術研究運用個資限於特定目的之規範，對於產業適用上是否產生阻礙？
- 參考其他國家對於特種個資所提供之特殊保護措施，是否有我國值得參考之處？

案由三：個資法有關學術研究而蒐集、處理或利用個資之特殊彈性規範

- 目前我國就學術研究之告知義務有彈性規範，就比較法之規定有無值得我國參考之處？

國家發展委員會

19

大綱

一 討論目的及範圍

二 議題分析

三 附件

國家發展委員會

20

歐盟相關規定(1/2)

最近一次個資法修正：2016年（2018年施行）

	科學研究	建檔目的資料處理	歷史研究
定義	廣義詮釋—任何以發掘新知識為目標、以促進某領域發展為目標的活動，包含與人文相關的研究	永久儲存資料，用於歷史研究的前置作業＊與公共利益相關	單純歷史研究，包含地理研究
	例：科技發展及成果、基礎研究、應用研究、私人贊助研究、公衛研究、以營利為目的的研究		
合法要件	第89條第1項適合的保護措施（appropriate safeguards）		
適用主體	不限適用對象		

21

歐盟相關規定(2/2)

最近一次個資法修正：2016年（2018年施行）

GDPR對科學研究之彈性規定：

例外條款（exceptions）	特別規範條款（derogations）
與資料保護原則相關	**與當事人權利相關**
進階處理/二次利用資料： • 不視為與新舊目的不相容	**被告知權&告知義務：** 不可能提供資料或提供資料須付出不等比的時間精力，不用遵守告知義務
限制儲存原則： • 資料得儲存更長的時間 • 但非永久保留	**刪除權、近用權、更正權、限制處理權、拒絕權**（其他場次討論）
特種個資： • 為例外情形之一	

22

英國相關規定(1/2)

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國，GDPR適足性認定（2021）

- **科學研究之定義**
  - 廣義定義：包含科技、醫學、社會科學等研究。
  - 寬鬆解釋：包含科技發展及成果、基礎研究、應用研究及私人贊助。
- **適用要件**
  - 符合UK GDPR第6條或第9條之要件
- **保護措施、資料最小化**
  - 符合UK GDPR 89條第1項、DPA 2018 第19條之保護措施
  - 基於公共利益之建檔目的、科學或歷史研究目的或統計目的，應採取適當保護措施以保護資料主體之權利及自由及正當利益，包括公開資訊。
  - 保護措施應確保已備妥技術上及組織上之措施，特別是用以確保資料最少蒐集原則之落實。只要上開目的得以實現，措施得包括假名化。

23

英國相關規定(2/2)

- **目的外利用**
  - 原則：蒐集目的須特定、明確及合法，且不得為該等目的以外之進階處理，除非符合相容性判斷。
  - 例外：為達成公共利益之建檔目的、**科學或歷史研究目的或統計目的**所為之進階處理，不視為與原始目的不相容。
- **例外規定**
  - 原則：針對特定當事人的措施或決策之處理，不得依第89條第1項處理。
  - 例外：除處理目的為必要外，包含**經批准之醫學研究**目的。
- **限制**
  - 若處理可能對當事人造成重大損害或重大痛苦，則不符合GDPR第89條第1項之要求。

24

德國相關規定

最近一次個資法修正：2021年6月23日
歐盟成員國

合法要件		一般個資	特種個資
適用主體		不限制	
特定目的		科學或歷史研究目的，以及統計目的所必要	
合法要件		取得同意、公共利益執行職務所必要、行使公權力所必要、追求正當利益所必要*(擇一)	左邊事由外，資料控管者利益明顯大於當事人排除該處理之利益
保護措施		具備技術上或組織上之適當保護措施	預先規劃維護當事人利益的適當和具體措施，且應考慮到現有技術、實施成本和處理的類型、範圍、情況和目的，以及與自然人權利和自由處理相關的風險的不同發生概率和嚴重程度
彈性規定	目的	進階處理不視為與原始目的不相容，但其他法令規範則從其規定	
	儲存	在確保當事人權利及自由要求下，得以較長時間儲存	
	控管者義務	資料控管者無法提供或提供資訊之成本過鉅，則在符合GDPR所訂要件及保護措施，或要求之義務可能使該處理目標無法實現或嚴重損害其實現，得免除提供資訊之義務	
	公開	當事人同意，或為呈現時代「歷史事件」的研究成果所不可或缺時，得公開個人資料	

*追求正當利益所必要，須通過利益衡量

25

美國相關規定

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

	HIPAA	CCPA	UPDPA
研究定義	目的為發展或有助於知識普及之系統性調查，包含研究開發、測試與評估	目的係發展或促進公共或科學知識之科學分析、系統研究與觀察（包含基礎研究與應用研究）	係指利用個人資料來發現與公共衛生、公共政策或其他一般公共利益事項有關的事項
適用對象	1. 健康計畫 2. 健康照顧清算中心 3. 健康照顧提供者	不限	
合法要件	研究倫理審查委員會或類似之隱私委員會審查同意	針對企業研究限於蒐集個人資料背景相關之研究目的	允許基於產品或服務的研究與開發進行研究分析
管理措施	應符合HIPAA資安規則	應落實CCPA所列適當安全措施	1. 資料安全措施 2. 資料隱私與安全風險評估

26

日本相關規定(1/2)

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

現行個資法	令和3年修正個資法
學術研究一律排除適用個資法之規定。	1.適用對象：大學及其他以學術研究為目的之機關或團體，或所屬人員。 2.根據情形適用除外規定： （1）變更利用目的之限制 ①有學術研究目的處理之必要，且處理個資事業者為學術研究機關等 ②有學術研究目的處理之必要，而提供學術研究機關等 （2）取得敏感性個人資料之限制 ①有學術研究目的處理之必要，且處理個資事業者為學術研究機關等 ②從學術研究機關等取得，基於學術研究目的有取得之必要（僅限於共同進行學術研究時） （3）提供個人資料予第三者之限制 ①個人資料處理事業者為學術研究機關等時，為公佈學術研究成果或教授不得已時 ②處理個資事業者為學術研究機關等，基於學術研究目的有提供之必要時（僅限於共同進行學術研究時） ③第三者為學術研究機關等時，基於學術研究目的有運用之必要時 3.學術研究機關等之義務： （1）取得、利用及提供個資 利用目的之特定、禁止不當利用、適當取得、利用目的之通知、確保資料內容正確性 （2）安全管理措施、揭露與更正及停止利用請求對應、假名加工或匿名加工資料處理事業者義務、民間團體促進個資保護

27

日本相關規定(2/2)

醫療產業應用 -「次世代醫療基盤法」（優先於個資法之適用，個資法第76條第1項第3款研究利用之例外）

範圍 醫療資料包含一切與個人身心狀況相關資料；當事人不以現仍存活之自然人為限。

醫療資料處理事業

§30
1. 向主管機關申報
2. 選擇退出→依政令預先公告內容
3. 作成有關提供紀錄並保存之義務

事前告知
① 提供情事
② 提供醫療資料項目
③ 提供方法
④ 本人或其遺族得請求停止提供及其程序

提供醫療資料

認定匿名加工醫療資料作成事業

1. §8具備相關申請資格、符合法定要件並經主管機關認定
2. §17利用目的的限制：不得逾越達成認定事業目的必要範圍之處理
3. §18依主管機關所訂基準加工，至無法識別特定個人，並不得回復
4. §19無利用必要之資料刪除
5. §20安全管理措施、 §21從業人員之監督、 §24委託對象之監督
6. §23得委託認定醫療資料處理受託事業，處理醫療資料或進行匿名加工
7. §33作成確認紀錄並保存之
   ① 確認提供醫療資料事業之姓名、名稱、住所
   ② 該當被提供醫療資料取得之經過

提供匿名加工醫療資料

醫療機構、行政機關、健保機構等

§25其他認定匿名加工醫療資料作成事業

§15 未符合上述規定，主管機關得撤銷認定

§18 不得再取得其他資料與該當匿名加工醫療資料進行組合、比對，以回復特定個人識別性

28

韓國相關規定(1/2)

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定進入最終程序

韓國PIPA對於科學研究應用的修法重點

- 2020年新版PIPA為使相關產業能以活用資料作為韓國發展物聯網（IoT）、人工智慧（AI）、雲端（Cloud）等新興技術政策，放寬產業無須取得當事人同意的「假名資料」得被運用於科學研究中。
- 科學研究的定義：技術的開發與實證、基礎研究、應用研究及民間投資研究等使用科學方法的研究（第2條第8款參照）。
- 放寬無須取得當事人同意的假名資料應用領域（第28-2條參照）：

統計編制

科學研究

公益記錄保存

29

韓國相關規定(2/2)

科學研究資料適用之限制

假名資料限制範圍	內容	條文參照
假名資料的處理限制	• 應由保護委員會或相關中央行政機關首長指定之專門機關執行 • 若欲對外傳輸須取得專門機關負責人的批准方可為之 • 專門機關的指定或取消、輸出暨批准等必要事項，須依施行令定之	28-3
適當安全措施義務	• 應設置適當必要的安全措施，並將可還原辨識特定個人之額外情報分別保管及管理，以防止發生個資事故 • 要求個資管理者應填載並保存假名資料處理之目的及向第三方提供時的管理紀錄	28-4
禁止義務	• 任何人均不得以識別特定個人為目的而處理假名資料 • 個資處理者在處理假名資料過程中，產生識別特定個資時應即終止並將該資料銷毀	28-5

30

新加坡相關規定(1/2)

最近一次個資法修正：2020年
CBPR成員國

PDPA第13條：組織在未經個人同意或視為同意（deemed consent）之情況下，原則上禁止蒐集、處理或揭露個資，**除非符合PDPA第17條未經同意例外允許蒐集、處理或揭露之規定**，同意必須經PDPA第20條告知並依據特定目的表示同意，而個人若基於特定目的自願且合理提供個資則視為同意。

未經同意利用或揭露個資(PDPA Schedule 1 & Schedule 2)

基於促進業務改進目的	■目的擇一：(1)改善或加強商品或服務，或開發新商品或服務；(2)改善或發展新興商業模式；(3)瞭解客戶喜好；(4)客製化商品或服務所必要 ■要件：(1)**不以可單獨識別個人之形式**利用所蒐集個資，將**無法合理實現目的**；(2)**一般人認為符合適當蒐集個資之情形**
基於研究目的	■要件：(1)**不以可單獨識別個人之形式**利用或揭露個資，將**無法實現研究目的**；(2)尋求同意揭露是**不切實際**的；(3)有明顯之**公共利益**；(4)研究結果將**不會用於**做出任何影響個人之決定；(5)研究結果以**無法識別個人之形式公布**

視為同意利用或揭露個資(PDPA第15條及第15A條)

透過行為	PDPA第15條(1)： ■個人**自願**向組織提供個資或作出允許蒐集個資之行為（例如：提供信用卡號碼進行付款） ■目的明確、合理
依據契約需求	PDPA第15條(2)、(3)： ■為了**執行或完成交易/履行與個人之契約** ■組織A向組織B/組織C揭露個資是合理且必要的
透過充分告知	PDPA第15A條： ■**告知目的+個人未選擇退出**=視為同意 ■評估並確定個資+識別不利影響+實施合理措施+提供合理期間&方式拒絕同意

國家發展委員會

31

新加坡相關規定(2/2)

最近一次個資法修正：2020年
CBPR成員國

為因應國家政策與產業需求，PDPC依據PDPA第62條豁免權（exemption），允許個人或組織可在遵循PDPC所制定之指南，協助企業、組織遵守PDPA規範下**提供組織內部與組織間之個資共用**，進行組織內部及組織之間的**資料共享（Data Sharing）**

同一組織內或關係組織間共用	■出於個人已同意或被視為已同意之目的 ■組織應制定內部政策以防止個資濫用 ■未經同意共享個資必須確保符合PDPA相關例外規定
與資料仲介機構共用	■應與資料仲介機構簽訂書面契約 ■簡化業務委託決策：無需向個人徵求明確同意揭露個資 ■未經個人同意資料仲介機構不得將個資用於其他目的
與一個或多個組織共用	■應考慮共享的預期目的&可能帶來的潛在利益和風險 ■考慮因素：共享個資之類型、與預期目的相關性、是否需同意...

PDPC於2018年設立的沙盒計畫：**「資料共享安排」機制（Data Sharing Arrangements, DSA）**
組織只要遵循法律、達到一定資料技術應用品質與實施資安與個資保護措施下，向PDPC申請通過即可進行DSA之個人與商業資料共用，申請標準如下：

① 必須在指定時段內與指定的組織進行共享 ② 必須用於明確且具體的特定目的 ③ 不得產生任何不利影響；基於合法利益

組織應進行**資料保護影響評估**：評估資料共享預期風險及對個人之影響並實施必要措施減輕及解決風險

國家發展委員會

32

菲律賓相關規定

最近一次個資法修正：2012年（2019年提出修正案，目前尚未完成立法）

定義	• 例示：科學研究、統計研究 • 為發展或促進可歸納的知識（包含理論、原則、關係）所進行的活動 • 使用科學方法觀察、推理、分析和累積任何資訊的活動
適用對象	• 公務機關（構）、私人機構，並不限學術機關（構）
個資種類	• 一般個資、特種個資
適用要件	• 為追求公共利益（嚴格限縮解釋） • 符合特定法規（個案解釋） • 符合專業道德倫理規則（得以已獲得研究倫理委員會（Research Ethics Committee）批准作為證明方式） • 事先經「國家隱私委員會」（National Privacy Committee, NPC）審查
法律效果	• 排除《資料隱私法》的適用
進階處理／二次利用	• 目的：歷史、統計研究、科學研究 • 原始目的滿足或消失後，例外允許繼續利用，以及延長保存時間
管理措施	• NPC審查標準：僅限為了達成研究目的、功能或活動的範圍內，進行蒐集、處理、利用個資行為 • 特種個資：落實管理措施，以避免特種個資意外被破壞、修改和揭露

國家發展委員會

黑字：《資料隱私法》《資料隱私法施行細則》規定內容
藍字：菲律賓國家隱私委員會諮詢意見（具有拘束效力）

「個人資料保護法相關議題」第 4 場產學專家學者諮詢會議—產業應用

議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、匿名化、假名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及菲律賓「隱私保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於產業應用有關匿名化、假名化之探討。

貳、議程

一、 主席致詞

二、 報告事項

產業應用(匿名化、假名化)之探討（國發會）

三、 討論事項

「去識別化」並非我國個資法之法律用語，將個人資料去識別化之行為應定性為個資法第 2 條第 4 款之「處理」行為(法務部 107 年 9 月 4 日法律字第 10703512280 號書函意旨參

照)，至於去識別化後之結果是「匿名化」或「假名化」，亦非我國個資法之法律用語。我國個資法涉及個人資料去識別化行為之規定，於個資法第 6 條第 1 項第 4 款、第 9 條第 2 項第 4 款、第 16 條但書第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款均有「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。」之規定，作為學術研究之合法要件。由於去識別化結果依照資料加工程度所呈現之狀況，區分為「匿名化」、「假名化」。綜觀比較法，歐盟將匿名化、假名化視為資料處理之適當保護措施，鼓勵產業應用該措施，惟強調技術中立，故不以法律干預；美國、日本、韓國則針對匿名化、假名化訂有泛用性之規定。由於去識別化在大數據時代有其重要性，匿名化、假名化應採用何種標準作業流程，有效評估並控制重新識別之風險為本次議題核心。針對我國去識別化之效果、要件及判斷標準、加工方式、管理措施、義務要求等，蒐整司法判決及實務見解，進行比較法之分析，整理討論內容提出下列二項案由。

案由一、有關匿名化之相關規範探討

說明：

一、 匿名化之效果

我國針對匿名化之效果，依個資法第 9 條第 2 項第 4 款得免為向當事人告知個人資料來源及第 8 條所列事項。惟實務有認為「如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自無個資法之適用。」（法務部 103 年法律字第 10303513040 號函）；亦有認為「按個人資料保護法第 16 條第 5 款及第 20 條第 1 項第 5 款規定，係為促進資料合理利用，以統計或學術研究為目的時，應得准許特定目的外利用個人資料。」（法務部 104 年法律字第 10400065570 號函）

綜觀各國法制，多數國家認為個人資料匿名化後，已不具可識別性，故非屬個人資料，因此排除個資法之適用。惟歐盟強調資料匿名化仍應考量合理運用，包括所有客觀因素、識別所耗費之成本及時間、當時技術及科技發展。而日本允許依一定程序予以匿名加工後之資料，得不經當事人同意作目的外利

用或提供予第三人。

二、 匿名化之要件及判斷標準

依我國個資法第 6 條第 1 項第 4 款、第 16 條但書第 5 款、第 19 條第 1 項第 4 款以及第 20 條第 1 項第 5 款規定均有「資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人」。實務認為「如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者」（法務部 103 年法律字第 10303513040 號函），結合個資法施行細則第 3 條及第 17 條規定，我國去識別化係指「針對所保有的個人資料，運用代碼、匿名、隱藏部分資料或其他相類之技術，將個人可識別資訊予以去除，而達到無從直接識別特定之個人，並且也無法透過與其他資料對照、組合、連結等相類方式，進而識別出特定之個人。」，此種解釋較相近於匿名化之概念。復實務有認為「無從識別特定個人」係以「完全切斷資料內容與特定主體間之連結線索」程度為判準，若資料收受者掌握還原資料與主體間連結之能力，則不符合去識別化標準（最高行政法院 106 年判字第 54 號判決）。

綜觀各國法制，目前歐盟、英國、德國、美國及日本均有明訂「匿名化」之定義，新加坡、菲律賓則透過主管機關解釋。所謂「匿名化」係指「個人資料經加工處理須達到以合理手段均無法識別特定個人之程度，且無法復原者」，故主要可分為「處理」、「合理性」、「無法識別」、「無法復原」四個要件。

另所謂「無從識別特定個人」之判斷標準，日本有採「一般人基準說」，以一般人為基準，判斷其有無「其他資訊」作組合、比對之可能；或採「特別基準說」，認為「其他資訊」不應僅限於一般人容易獲得之資料，在具體事件上於判斷組合、比對之可能性時，雖僅為一定範疇之關係人可能知悉、保有之其他資訊，亦應納入考慮。英國及新加坡則採「有心侵入者測試」，當非具有專業電腦知識或技術之侵入者有動機嘗試時，是否可能成功地再識別。

三、 匿名化之加工方式

依我國個資法施行細則第 17 條例示去識別化之方式，得

以代碼、匿名、隱藏部分資料或其他方式，達到不再具有直接或間接識別個人之資料。參照我國實務所提及之加工方式尚包含刪除（最高行政法院 106 年度判字第 54 號判決）等。

綜觀各國法制，歐盟第 29 條資料保護工作小組曾指出，無論對資料控管者或接收者而言，若不刪除原始資料，無論資料經何種程度之處理，皆排除構成匿名資料之可能，且須達到盡一切現今合理可能之手段，均無法回復原狀之程度。惟歐盟強調技術中立，考量因各種資料屬性不一，不同資料有不同的應用領域與利用可能性，對個人隱私的侵害程度不盡相同，故此難以概念式地劃定加工方式之統一標準。日本則考量匿名化之加工方式涉及技術面問題，在法制設計上先由法律確立原則性加工方式及一般泛用性標準，再由個人資料保護委員會訂定法規命令揭示具體之加工方式。

四、 匿名化之管理措施

我國個資法未明文規範匿名化之管理措施，惟經濟部標準檢驗局已公布國家標準 CNS29100-2「資訊技術－安全技術－個人資訊去識別化過程管理系統」以及 CNS29191「資訊技術-安全技術-部分匿名及部分去連結鑒別之要求事項」，並委由財團法人台灣電子檢驗中心進行驗證，且研訂「個人資料去識別化過程驗證要求及控制措施」，作為去識別化具體要求及控制措施之參考。實務上認為驗證功能得協助證明機關並無違反個資法之主觀故意或過失，並已採行適當安全維護措施，且個資遭到違法蒐集或利用，並非因機關違反個資法所致（法務部 105 年 1 月「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告）。

綜觀各國法制，由於歐盟將匿名化視為風險管理技術，故未規定匿名化之管理措施。美國、日本則明定於個資法，英國、新加坡、菲律賓則透過主管機關解釋。觀察各國規定，管理措施主要可分為授權及監督責任、風險評估、制定處理規範及防止事故等類型。此外，日本另要求應建立申訴對應處理機制，以提供當事人救濟之管道。

五、 匿名化之義務要求

我國個資法未明文規範匿名化之義務要求，惟實務認為

「倘資料接收者嗣後運用特殊罕見之技術或方法進行重新識別而取得個人資料，仍須符合個人資料蒐集、處理或利用之要件」，如有違反則係違法之蒐集行為（法務部 105 年 1 月「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告）。

綜觀各國法制，由於經匿名化之資料仍可能會因情境變化而得以重新識別特定個人，針對匿名化之義務要求，多數國家均課予禁止重新識別之義務；美國限制匿名化資料須於特定目的利用；日本由於強調匿名化過程之透明性，故要求須公告其事業名稱、施作對象之個資類型、匿名化項目及利用目的，並向第三方明示所提供為匿名加工資料。

小結：請產學專家就以下議題提供建議：

(一) 針對「匿名化」應產生何種法律效果？比較立法例何種效果較值得我國參考？

(二) 由於匿名化為不確定法律概念，我國需否將「匿名化」明定於個資法？如需明定，應包含哪些要件及所採判斷標準為何？

(三) 由於「匿名化之加工方式」涉及業界之需求及專業技術，則我國需否明定於個資法？對於產業應用上是否產生阻礙？

(四) 參酌立法例，我國需否將「匿名化之管理措施」明定於個資法？綜觀其他國家要求之管理措施，是否有值得我國參考之處？對於產業應用可能造成影響為何？

(五) 由於匿名資料仍有重新識別之風險，我國需否將「匿名化之義務要求」明定於個資法？對於產業應用上是否產生阻礙？

案由二、有關假名化之相關規範探討

說明：

一、 假名化之效果

綜觀各國法制，由於個人資料假名化仍可能與其他資料

比對而得識別特定個人，屬於間接識別之個資，仍應有個資法之適用。故針對假名化之效果，有採利用目的放寬如美國、日本；有採免除個資事故通知義務如歐盟、英國、德國、日本、韓國；有採排除當事人權利行使如歐盟、美國、日本、韓國；或排除個資法適用如菲律賓；免除保存期限銷毀義務如韓國。

二、 假名化之要件及判斷標準

綜觀各國法制，目前歐盟、英國、德國、美國、日本、韓國均明訂「假名化」之定義，新加坡、菲律賓則透過主管機關解釋。所謂「假名化」係指「個人資料經加工後，非與其他資料比對無法識別特定個人」，由於不同匿名化要求去識別化達到無法復原之程度，故主要可分為「處理」、「無其他資料」、「無法識別」三個要件。

三、 假名化之加工方式

綜觀各國法制，歐盟強調技術中立性，故未規定假名化加工標準，惟歐盟第 29 條資料保護工作小組例示假名化得使用加密、雜湊函數、記號化之加工方式。而日本、韓國考量假名化之加工方式涉及技術面問題，故在法制設計上確立原則性加工方式及一般泛用性標準，規定應刪除或替換個人資料中之記述或符號，日本另要求應刪除或替換可能因非法使用所造成財產損失之記述。其他國家則係透過主管機關解釋，提供假名化加工方式之例示說明。

四、 假名化之管理措施

綜觀各國法制，歐盟、美國、日本、韓國均有明定於個資法，要求應對假名資料採行適當之安全管理措施。觀察各國規定，多數國家均要求假名化資料應與原始資料分別管理，應明確資料控管者權限及責任、建立管理制度及改善評估、防止無權近用等措施。另外韓國要求假名化應依規定填載目的，並保存相關文件管理紀錄。

五、 假名化之義務要求

綜觀各國法制，因假名化之資料仍有間接識別之風險，故針對假名化之義務要求，多數國家均課予禁止重新識別之義務；美國、韓國則限制假名化資料須於特定目的內利用；日本強調

假名資料係為供事業內部分析用途，故禁止目的外利用或提供予第三方，並禁止利用聯絡資訊，且仍課予須將利用目的公告之義務。

小結：請產學專家就以下議題提供建議：

(一) 由於產業應用假名化技術較匿名化可行，我國是否應承認「假名化」之制度？參酌比較法，何種法律效果較值得我國參考？

(二) 由於假名化為不確定法律概念，我國需否將「假名化」明定於個資法？如需明定，應包含哪些要件？

(三) 由於「假名化之加工方式」涉及業界之需求及專業技術，則我國需否明定於個資法？對於產業應用上是否產生阻礙？

(四) 參酌立法例，我國需否將「假名化之管理措施」明定於個資法？綜觀其他國家要求之管理措施，是否有值得我國參考之處？對於產業應用可能造成影響為何？

(五) 由於假名資料仍有間接識別之風險，我國需否將「假名化之義務要求」明定於個資法？如需明定，應包含哪些義務？對於產業應用上是否產生阻礙？

產業應用
（匿名化、假名化）

國家發展委員會
111年 1月 13日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	**產業應用（匿名化、假名化）**	國際傳輸	受託處理者義務	框架性討論	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13								

2

大綱

一 討論目的及範圍

二 議題分析

三 附件

3

一、討論目的及範圍(1/6)

■ 討論範圍

以「產業應用」為主軸，討論匿名化、假名化之規範要件，有關受託處理者義務及當事人權利限制置於其他場次討論，並以「個資法」為主要討論範疇。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
	健康保險可攜性及責任法（HIPAA）	2006	
日本	個人資料保護法	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員
菲律賓	隱私保護法	2012	

4

一、討論目的及範圍(2/6)

國別	規範名稱	匿名化	假名化
我國	個人資料保護法	去識別化	X
歐盟	一般資料保護規則	匿名化（anonymization）	假名化（pseudonymization）
德國	聯邦資料保護法		
英國	資料保護法		
美國	加州消費者保護法（CCPA）	去識別化（deidentified）※包含假名化（Pseudonymized）	
	統一個人資料保護法（UPDPA）	去識別化（deidentified）	假名化（Pseudonymized）
	健康保險可攜性及責任法（HIPAA）	去識別化（deidentified）	X
日本	個人資料保護法	匿名化（匿名加工）	假名化（仮名加工）
韓國	個人資料保護法	X	假名化（가명）
新加坡	個人資料保護法	匿名化（anonymization）※包含假名化（Pseudonymization）	
菲律賓	隱私保護法	匿名化（anonymization）	假名化（pseudonymization）

- ◆ **匿名化**為個人資料經加工後須達到以合理手段均無法識別特定個人之程度，且無法復原者（非屬個人資料）
- ◆ **假名化**為個人資料經加工後，非與其他資料比對無法識別特定個人（屬得間接識別之個人資料）

國家發展委員會

5

一、討論目的及範圍(3/6)

國別	規範名稱
我國	個人資料保護法
歐盟	一般資料保護規則
德國	聯邦資料保護法
英國	資料保護法
美國	加州消費者保護法（CCPA）
	統一個人資料保護法（UPDPA）
	健康保險可攜性及責任法（HIPAA）
日本	個人資料保護法
韓國	個人資料保護法
新加坡	個人資料保護法
菲律賓	隱私保護法

- 去識別化技術依資料加工程度，區分為**匿名化**及**假名化**
- 綜觀比較法之立法模式：
  - 歐盟、德國、英國將**去識別化**視為**資料處理之適當保護措施**，透過去識別化降低資料主體可能面臨之風險，鼓勵產業合理利用去識別化之資料，並且強調**技術中立**，故不以法律干預。
  - 美國、日本、韓國為供**產業應用**去識別化資料，針對去識別化訂有經常性可被使用之匿名化加工方式的相關規定(泛用性規定)，使產業得以遵循。
  - 新加坡將**假名化**例示為**匿名化**加工方式之一，故無假名化之相關規範；菲律賓則建議以ISO/IEC 29100標準處理。
- 由於去識別化在大數據時代有其重要性，匿名化或假名化應採用何種標準作業流程，有效評估並控制被再識別之風險為本次議題核心。

國家發展委員會

一、討論目的及範圍(4/6)

6

- 我國個資法針對匿名化、假名化，應參考何種立法模式？
- 匿名化或假名化之相關作業流程需否明定於個資法？
- 對於產業應用造成之影響為何？

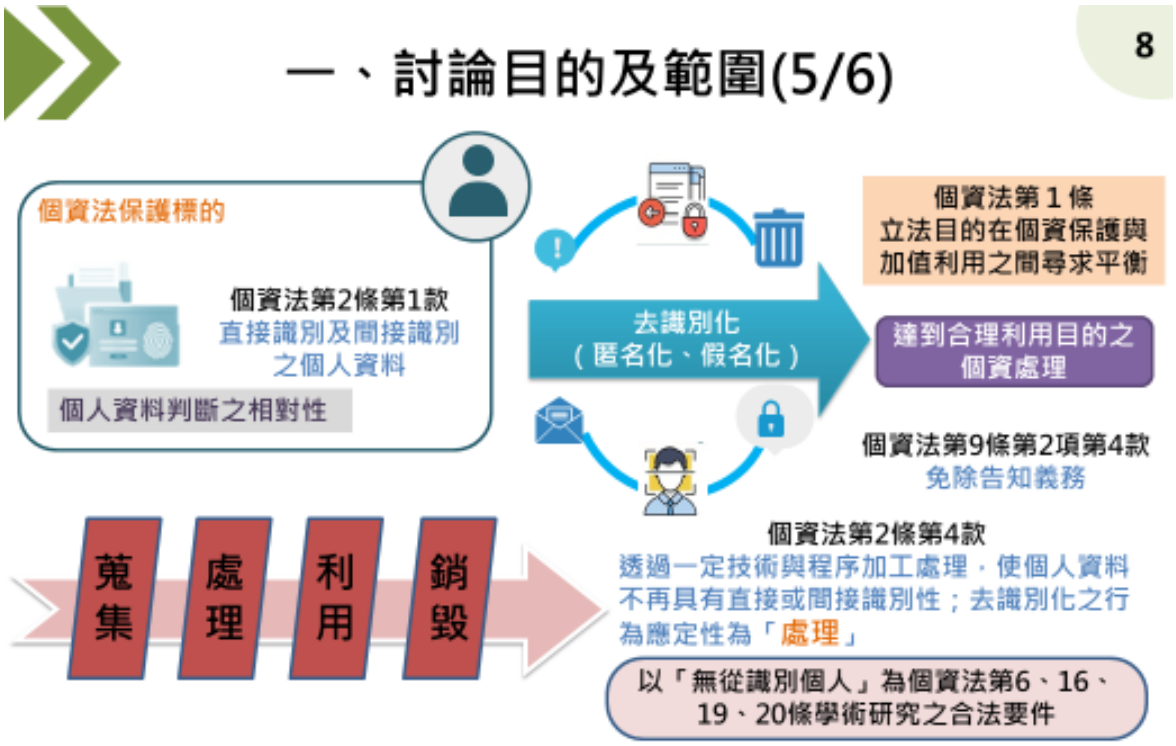
國家發展委員會

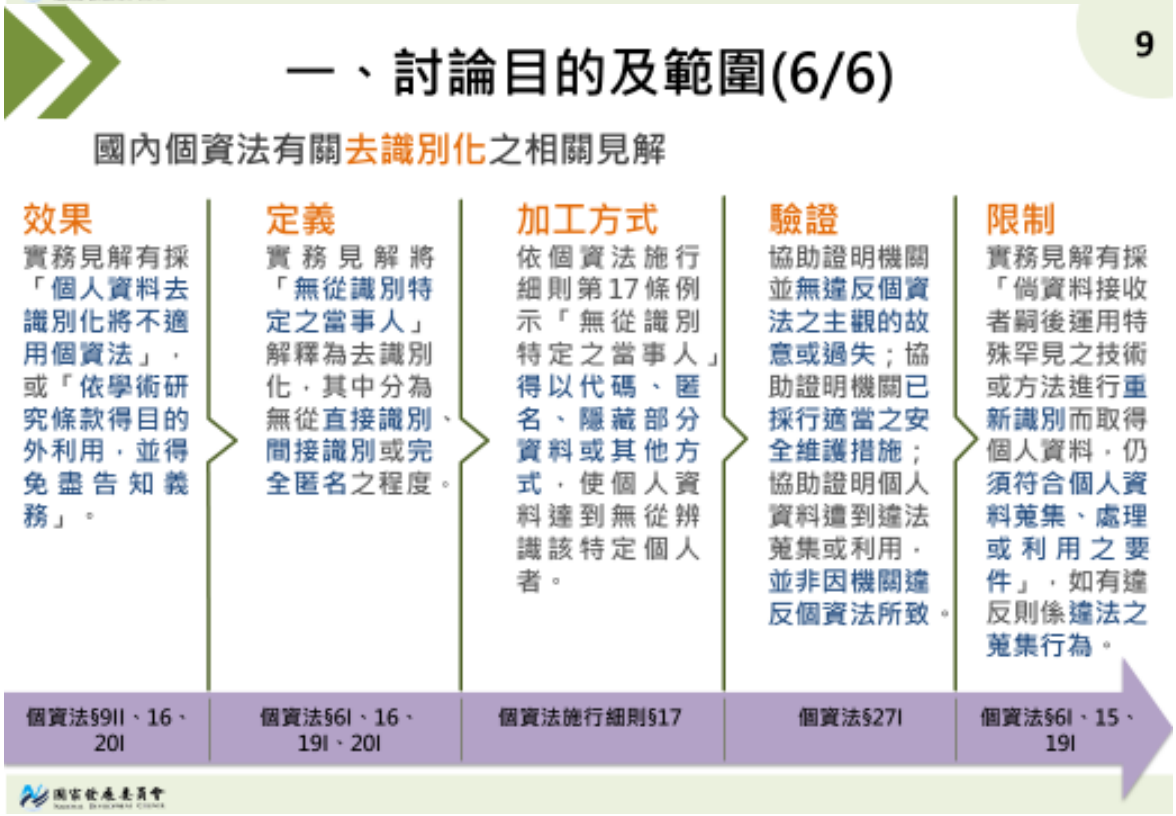
我國個資法相關規定

7

個人資料保護法	個人資料保護法施行細則
第6條第1項第4款（特種個資蒐集、處理、利用） 公務機關或學術研究機構基於醫療、衛生或犯罪預防之目的，為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 **第9條第2項第4款（間接蒐集免告知）** 基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。 **第16條但書第5款（公務機關利用）** 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 **第19條第1項第4款（非公務機關蒐集、處理）** 學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 **第20條第1項第5款（非公務機關利用）** 公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。	**第3條** 本法第二條第一款所稱得以間接方式識別，指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。 **第17條** 本法第六條第一項但書第四款、第九條第二項第四款、第十六條但書第五款、第十九條第一項第四款及第二十條第一項但書第五款所稱無從識別特定當事人，指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

國家發展委員會


8
一、討論目的及範圍(5/6)
個資法保護標的
個資法第2條第1款
直接識別及間接識別之個人資料
個人資料判斷之相對性
去識別化
（匿名化、假名化）
個資法第1條
立法目的在個資保護與加值利用之間尋求平衡
達到合理利用目的之個資處理
個資法第9條第2項第4款
免除告知義務
蒐集
處理
利用
銷毀
個資法第2條第4款
透過一定技術與程序加工處理，使個人資料不再具有直接或間接識別性；去識別化之行為應定性為「處理」
以「無從識別個人」為個資法第6、16、19、20條學術研究之合法要件


9
一、討論目的及範圍(6/6)
國內個資法有關去識別化之相關見解
效果
實務見解有採「個人資料去識別化將不適用個資法」，或「依學術研究條款得目的外利用，並得免盡告知義務」。
定義
實務見解將「無從識別特定之當事人」解釋為去識別化，其中分為無從直接識別、間接識別或完全匿名之程度。
加工方式
依個資法施行細則第17條例示「無從識別特定之當事人」得以代碼、匿名、隱藏部分資料或其他方式，使個人資料達到無從辨識該特定個人者。
驗證
協助證明機關並無違反個資法之主觀的故意或過失；協助證明機關已採行適當之安全維護措施；協助證明個人資料遭到違法蒐集或利用，並非因機關違反個資法所致。
限制
實務見解有採「倘資料接收者嗣後運用特殊罕見之技術或方法進行重新識別而取得個人資料，仍須符合個人資料蒐集、處理或利用之要件」，如有違反則係違法之蒐集行為。
個資法§9II、16、20I
個資法§6I、16、19I、20I
個資法施行細則§17
個資法§27I
個資法§6I、15、19I

10

大綱

一 討論目的及範圍

二 議題分析

三 附件

11

(一)有關匿名化之相關規範討論(1/13)

1) 匿名化之效果 - 我國現行規定

個資法第9條第2項第4款

- 效果：得免為向當事人告知個人資料來源及第8條所列事項

排除個資法適用	如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者，即非屬個人資料，自無個資法之適用。（法務部103年法律字第10303513040號函、法務部107年法律字第10703512280號函）

(一)有關匿名化之相關規範討論(2/13)

12

1) 匿名化之效果 - 比較立法例

匿名化加工後之資料仍有可能被回復識別，故各國對於匿名化資料是否應納入個資法規範及其配套措施作法不同。部分國家將匿名化資料排除個資法適用，部分國家則將匿名化作為得不受目的限制之條件，仍於個資法為適度規範。涉及法制規範架構之選擇，先提出討論。

排除個資法適用	歐盟（合理運用）、英國、德國、美國*UPDPA*&*CCPA*、韓國、新加坡、菲律賓
其他	美國*HIPAA*（目的外利用） 日本（目的外利用、提供予第三人）

1

我國個資法需否清楚界定「匿名化」之效果？

個人資料匿名化後，其效果在多數國家採排除個資法適用，日本採目的外利用、提供予第三人，何種效果較值得我國參考？

(一)有關匿名化之相關規範討論(3/13)

13

2) 匿名化之要件 - 我國現行規定

個資法第6、16、19、20條

- 資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定之當事人。

- 如公務機關或非公務機關保有之個人資料，運用各種技術予以去識別化，而依其呈現方式已無從直接或間接識別該特定個人者（法務部103年法律字第10303513040號函）

- 結合施行細則第3條及第17條，我國去識別化為「針對所保有的個人資料，運用代碼、匿名、隱藏部分資料或其他相類之技術，將個人可識別資訊予以去除，而達到無從直接識別特定之個人，並且也無法透過與其他資料對照、組合、連結等相類方式，進而識別出特定之個人。」

(一)有關匿名化之相關規範討論(4/13)

14

2) 匿名化之要件 - 「無從識別特定個人」之判斷標準

日本
有採「一般人基準說」；或採「特別基準說」

英國、新加坡
採「有心侵入者測試」（the motivated intruder test）

我國係以「完全切斷資料內容與特定主體間之連結線索」程度為判準，如資料收受者掌握還原資料與主體間連結之能力，則未達去識別化標準（最高行政法院106年判字第54號判決）

(一)有關匿名化之相關規範討論(5/13)

15

2) 匿名化之要件 - 比較立法例

「匿名化」係指「個人資料經加工處理須達以合理手段均無法識別特定個人之程度，且無法復原者」，故主要分為「處理」、「合理性」、「無法識別」、「無法復原」四個要件。

國家		名稱	處理	合理性	無法識別	無法復原	其他
我國		去識別化	O		O		或依揭露方式
歐盟							
德國		匿名化	O	O	O	O	
英國							
美國	UPDPA	去識別化	O	O	O		
	CCPA	去識別化	O	O	O		
	HIPAA	去識別化	O	O	O		
日本		匿名化	O		O	O	
韓國		匿名化	O	O	O		無法比對其他資料
新加坡		匿名化	O		O		
菲律賓		匿名化	O		O	O（永久性）	

2 **我國個資法需否清楚界定「匿名化」之要件？**

歐盟體系及美國、日本、韓國均明定「匿名化」之定義，其他國家則透過主管機關解釋。「匿名化」既屬於不確定法律概念，我國需否明定於個資法？如需明定，其要件及判斷標準為何？

(一)有關匿名化之相關規範討論(6/13)

16

3) 匿名化之加工方式 - 我國現行規定

個資法施行細則第17條

- 無從識別當事人：個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者。

	最高行政法院106年度判字第54號判決
涉及個資	姓名、出生年月、身分證統一編號
加工方式	刪除
影響因素	由資料提供者或是資料接受者執行刪除作業

- 實務解釋僅處理去識別化之呈現方式須達已無從直接或間接識別該特定個人之程度，並未就加工方式進一步探討。
（參法務部103年法律字第10303513040號函）
- 施行細則亦僅例示可能用來處理資料識別性之方法，及明示處理後或揭露時須達到無從識別特定個人之程度。

(一)有關匿名化之相關規範討論(7/13)

17

3) 匿名化之加工方式 - 比較立法例

歐盟

WP29採嚴格標準：必須刪除原始（可識別）資料

美國*HIPAA*

- 專家核決：依專業經驗判斷僅有極小識別風險
- 安全港條款：刪除18項識別因子均無「實際具體知識」得識別

日本個資法

刪除(替換)個人資料中可識別之記述或符號，並考量構成資料庫之相當措施

(一)有關匿名化之相關規範討論(8/13)

18

3) 匿名化之加工方式

歐盟體系

- 強調**技術中立**，由於各種資料屬性不一，不同資料有不同的應用領域與利用可能性，對個人隱私的侵害程度不盡相同，故難以概念式地劃定加工方式之統一標準。

美日體系

- 訂有**泛用性**之匿名化加工方式，供資料控管者遵循

3

我國個資法需否明定「匿名化加工方式」？

綜觀各國法制，美國、日本有明定匿名加工方式之泛用性標準，由於加工方式涉及業界之需求及專業技術，則我國需否將匿名化加工方式明定於個資法？對於產業應用上是否產生阻礙？

(一)有關匿名化之相關規範討論(9/13)

19

4) 匿名化之管理措施 - 我國現行規定

- 我國個資法及施行細則針對「匿名化」管理措施並無明確規範
- 經濟部標準檢驗局制訂國家標準**CNS29100-2「資訊技術 - 安全技術 - 個人資訊去識別化過程管理系統」**以及**CNS29191「資訊技術-安全技術-部分匿名及部分去連結鑒別之要求事項」**，並委由財團法人台灣商品檢測驗證中心進行驗證，且研訂**「個人資料去識別化過程驗證要求及控制措施」**，作為去識別化具體要求及控制措施之參考。
- 我國實務認為驗證功能有：
  1. 協助證明機關並**無違反個資法之主觀故意或過失**；
  2. 協助證明機關**已採行適當之安全維護措施**；
  3. 協助證明個人資料遭到違法蒐集或利用，**並非因機關違反個資法所致**。（法務部105年1月「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告）

(一)有關匿名化之相關規範討論(10/13)

20

4) 匿名化之管理措施 - 比較立法例

國家		授權及監督責任	風險評估	制定處理規範	防止事故	其他
歐盟			O			
英國		O	O	O	O	員工培訓
德國			O			
美國	UPDPA	考量因素包括個人資料類型、敏感性程度、對外提供資料之方式、引發他人重新識別之意圖等因素，並根據風險評估之結果計算設定風險檻值，進而判斷匿名化之技術類型或程度。		N/A		
美國	CCPA				O	確保資料未與消費者或家庭相關連
美國	HIPPA			N/A		
日本		O		O	O	申訴對應處理機制及其他適當必要措施
韓國				N/A		
新加坡			O			
菲律賓						ISO/IEC 29100標準

4

我國個資法需否明定「匿名化管理措施」？

比較各國法僅有美國*CCPA*、日本有明定，而歐盟、英國透過主管機關規範。則我國需否將管理措施明定於個資法？如需明定，應包含哪些類型？對於產業應用可能造成何影響？

國家發展委員會

(一)有關匿名化之相關規範討論(11/13)

21

5) 匿名化之義務要求 - 我國現行規定

- 我國個資法及施行細則針對「匿名化」義務要求並無明確規範
- 我國實務見解有採「倘資料接收者嗣後運用特殊罕見之技術或方法進行**重新識別**而取得個人資料，仍**須符合個人資料蒐集、處理或利用之要件**」，如有違反則係**違法之蒐集行為**。（法務部105年1月「公務機關利用去識別化資料之合理風險控制及法律責任」之研析報告）

國家發展委員會

(一)有關匿名化之相關規範討論(12/13)

22

5) 匿名化之義務要求 - 比較立法例

國家		禁止重新識別	限於特定目的	其他
美國	歐盟	O		
	德國			
	英國			
	UPDPA	O		
	CCPA	O	O（研究）	公開承諾、契約要求符合去識別化規定
	HIPAA			N/A
日本		O		公告匿名加工資料所包含之個資類別及提供方式；向第三方明示其所提供為匿名加工資料
韓國				N/A
新加坡		O		
菲律賓				N/A

承認國家較多

國家發展委員會

(一)有關匿名化之相關規範討論(13/13)

23

5) 匿名化之義務要求

- 經匿名化之資料仍可能會因情境變化而得以重新識別特定個人；歐盟及英國個資主管機關均指出，在現今數位時代下，縱將個資進行匿名化，透過技術之應用、彙整、串連與相互比對，原為識別個人身分無關之片段或零碎資料(非個資)，仍有機會重新識別出特定之個資主體，使特定個人身分遭到重新識別之風險大幅提升。
- 美國有研究顯示，透過分析比對性別、出生年月與郵遞區號此三類資料，即能識別出大約87%之美國人口。若於處理、利用匿名化資料的過程中，而重新識別出特定個人，此時再加以適用個資法規範，其保護實益仍相當有限。

5 我國個資法需否明定「匿名化義務要求」？

綜觀各國比較法，多數國家均課予禁止重新識別之義務；美國限於特定目的利用；日本要求須進行公告及向第三方明示。則我國需否將義務要求明定於個資法？如明定應包含哪些類型？對於產業應用上是否產生阻礙？

國家發展委員會

(二)有關假名化之相關規範討論(1/8)

24

1) 假名化之效果 - 比較立法例

利用目的放寬	美國*CCPA*（基於研究目的利用）、日本（排除變更利用目的限制）
免個資事故通知	歐盟、英國、德國、日本、韓國
排除當事人權利行使	歐盟、美國*UPDPA*（複製權、更正權）、日本、韓國
其他	菲律賓（不適用個資法）、韓國（免保存期限銷毀）

1

我國個資法需否清楚界定「假名化」之效果？

綜觀比較法，個人資料假名化後，其效果有採利用目的放寬、免個資事故通知、排除當事人權利行使及其他。我國如承認假名化制度，則何種效果較值得我國參考？

(二)有關假名化之相關規範討論(2/8)

25

2) 假名化之要件 - 比較立法例

「假名化」係指「個人資料經加工後，非與其他資料比對無法識別特定個人」，故主要分為「處理」、「無其他資料」、「無法識別」三個要件。

國家	名稱	處理	無其他資料	無法識別	其他
歐盟	假名化	O	O	O	
英國					
德國					
美國 UPDPA	假名化	O		O	不包含直接識別符
美國 CCPA	假名化	O		O	
美國 HIPAA			N/A		
日本	假名化	O	O	O	
韓國	假名化	O	O	O	
新加坡			N/A		
菲律賓	假名化	O			暫時性

2

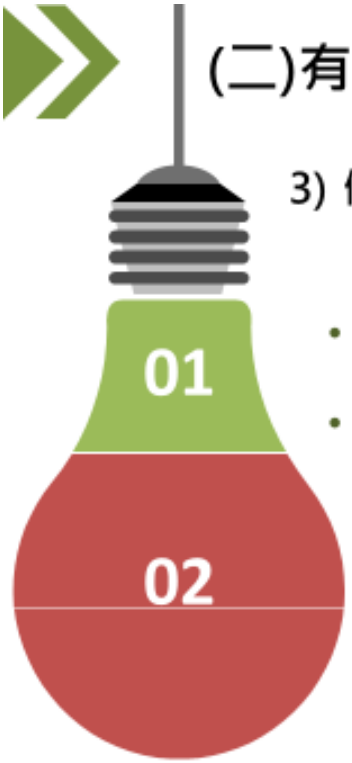
我國個資法需否清楚界定「假名化」之要件？

歐盟、英國、德國、美國、日本、韓國均明定「假名化」之定義，指非與其他資料比對無法識別特定個人，此概念是否應明定於我國個資法？如需明定，其應包含哪些要件？

(二)有關假名化之相關規範討論(3/8)

26

3) 假名化之加工方式 - 比較立法例



- 歐盟 - WP29例示加工方式有加密、雜湊函數、記號化
- 菲律賓 - NPC說明電子金鑰加密傳輸

- 日本個資法 - 刪除(替換)個人資料中可識別之記述或符號，及可能因非法使用所造成財產損失之記述
- 韓國個資法 - 刪除(替換)個人資料之全部、部分等方法

(二)有關假名化之相關規範討論(4/8)

27

3) 假名化之加工方式

歐盟體系

- 強調技術中立性，透過主管機關解釋，提供假名化加工方式之例示說明。

日韓體系

- 訂有泛用性之假名化加工方式，並透過法規命令方式或個資主管機關進一步解釋。

3

我國個資法需否明定「假名化加工方式」？

綜觀各國法制，日本、韓國有明定假名化加工方式，由於加工方式涉及業界之需求及專業技術，則我國需否將假名化加工方式明定於個資法？對於產業應用上是否產生阻礙？

(二)有關假名化之相關規範討論(5/8)

28

4) 假名化之管理措施 - 比較立法例

國家		資料分別管理	授權及監督責任	建立管理制度	防止事故	其他
歐盟		O		O		原始資料須加密
英國						
德國						
美國	UPDPA			N/A		
	CCPA	O				確保無法識別
	HIPAA			N/A		
日本			O	O	O	
韓國		O			O	保存相關文件管理紀錄
新加坡		承認國家較多		N/A		
菲律賓				N/A		

(二)有關假名化之相關規範討論(6/8)

29

4) 假名化之管理措施

- 歐盟體系、英國
  - 透過主管機關規範。

- 美國*CCPA*、日本、韓國
  - 明文規範假名資料之管理措施。
  - 資料分別管理（美、韓）；授權及監督責任（日）；建立管理制度（日）；防止事故（日、韓）

4

我國個資法需否明定「假名化管理措施」？

綜觀立法例，我國需否將管理措施明定於個資法？如需明定，應包含哪些類型？對於產業應用可能造成何影響？

(二)有關假名化之相關規範討論(7/8)

30

5) 假名化之義務要求 - 比較立法例

國家		禁止重新識別	限於特定目的	其他
歐盟			N/A（仍適用個資一般規範）	
英國		O		
德國			N/A（仍適用個資一般規範）	
美國	UPDPA	O		
	CCPA	O	O（研究）	
	HIPAA			
日本		O		禁止目的外利用或提供第三方、公告義務、禁止利用聯絡資訊
韓國		承認國家較多	O（科學研究）	
新加坡				N/A
菲律賓				N/A

(二)有關假名化之相關規範討論(8/8)

31

5) 假名化之義務要求

- 歐盟體系
  - 強調假名資料仍屬個人資料，仍適用個資之一般規定
- 英國、美國*CCPA & UPDPA*、日本、韓國
  - 明文規範假名資料之義務要求
  - 禁止重新識別之義務（英、美、日）；限特定利用目的（美、韓）；限內部利用並要求公告義務（日）。

5 我國個資法需否明定「假名化義務要求」？

由於假名化仍存有識別風險，我國需否將義務要求明定於個資法？如需明定，應包含哪些義務？對於產業應用上是否產生阻礙？

32

議題討論

案由一：有關匿名化之相關規範探討

1) 針對「匿名化」應產生何種法律效果？比較法哪種效果較值得我國參考？
2) 針對「匿名化」需否明定於個資法？如需明定，應包含哪些要件及所採判斷標準為何？
3) 針對「匿名化之加工方式」需否明定於個資法？對於產業應用上是否產生阻礙？
4) 針對「匿名化之管理措施」需否明定於個資法？如需明定，應包含哪些類型？對於產業應用可能造成影響為何？
5) 針對「匿名化之義務要求」需否明定於個資法？如需明定，應包含哪些類型？對於產業應用上是否產生阻礙？

案由二：有關假名化之相關規範探討

1) 針對「假名化」應產生何種法律效果？比較法哪種效果較值得我國參考？
2) 針對「假名化」需否明定於個資法？如需明定，應包含哪些要件？
3) 針對「假名化之加工方式」需否明定於個資法？對於產業應用上是否產生阻礙？
4) 針對「假名化之管理措施」需否明定於個資法？如需明定，應包含哪些類型？對於產業應用可能造成影響為何？
5) 針對「假名化之義務要求」需否明定於個資法？如需明定，應包含哪些義務？對於產業應用上是否產生阻礙？

國家發展委員會

33

大綱

一 討論目的及範圍

二 議題分析

三 附件(一)各國相關規定

國家發展委員會

34

歐盟相關規定（1/2）

最近一次個資法修正：2016年（2018年施行）

	假名化	匿名化
定義	如不使用其他資料，表面上無法識別個人。 *其他資料：分開保管+技術上或組織上的措施防止資料可識別或可得識別出自然人	無法直接識別或間接識別個人的資料
排除適用	X	O
方式	• 加密（Encryption） • 雜湊函數（Hash Functions） • 記號化（Tokenization）	• 雜訊加入（Noise Addition） • 排列變更（Permutation） • 資料聚集與K匿名（Aggregation/K-Anonymity）

35

歐盟相關規定（2/2）

最近一次個資法修正：2016年（2018年施行）

假名化管理規定

歐盟網路安全局（ENISA）公布被假名化的機密（pseudonymisation secrets）之最佳實務典範：

- 分開於不同的檔案夾
- 於不安全的媒體中刪除
- 以管理制度或章程管理存取權限，且存取紀錄應以log紀錄
- 加密及加密金鑰管理

假名化之效果

- 為風險管理的技術
- 技術及組織上的安全措施→協助達到資料最小化及設計包含隱私之義務
- 個資事故→已採取假名化技術，使外洩的個人資料無法被一般人所讀取，則不須通知資料主體
- 匿名化技術應用於巨量資料，或機密資料以保護商業機密

英國

36

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

	假名化	匿名化
定義	該處理個認資料之方式，可使個資在無額外資訊的輔助下，無法連結到特定當事人。 *額外資訊：分開存放、採取技術性和組織性措施等措施，確保個資不會被使用於識別或可識別特定自然人。	將資料中可識別資料主體之資料去除，並採取技術性措施，使該資料主體無法再被直接或間接識別。
資料性質	屬於個資範圍，受UK GPDR、DPA 2018規範	非屬個資，不受UK GDPR規範
管理規定	「匿名化：資料管理風險守則」、「匿名化決策架構」、「匿名化、假名化和隱私增強技術指南」 →建議進行隱私影響評估、員工訓練、設立SIRO等	
效果	• 作為風險管理技術，技術性及組織性之安全措施 ，可促進達成資料最小化及設計隱私之義務。 • 假名化個資之個資事故，不須通知資料主體 • 同一控管者可將假名化資料進行一般分析	
禁止事項	• 不得由資料再利用者進行假名化 • 不得再識別	

德國相關規定

37

最近一次個資法修正：2021年6月23日
歐盟成員國

	BDSG	內容
假名化定義	第46條第5款	無額外資料的情形時，不能夠將資料識別至特定個人。此外，針對該額外資料必須分開保管，並採取技術及組織上的措施，以避免個人資料被歸屬於一個已識別或足資識別的自然人。
去識別化之管理規定	第22條第2項	**基於第22條第1項處理特種個人資料**時，應預先規範維護數據主體利益的**適當及具體措施**（angemessene und spezifische Maßnahmen），該措施必須考慮到現有技術、實施成本和處理的類型、範圍、情況和目的，以及與自然人權利和自由處理相關的風險的不同發生概率和嚴重程度，包含採行技術及組織上之措施、假名化、加密個人資料，或為維護處理之安全性，就技術性及組織性措施之有效性，建立經常性之查核、評估及評等之程序。
	第48條第2項	**基於履行職務**之必要而運用**特種個人資料**時，應提供**適當保障**（geeigneteGarantien），該保障包括符合資料安全或資料保護控之特殊要求、假名化或加密個人資料。
	第27條第3項	除符合上開本法第22條第2項所列措施外，若係**基於科學或歷史研究**，或研究目的而運用**特種個人資料**者，**應將該資料予以匿名化**。但如果匿名化的結果會與當事人正當利益衝突時，則不在此限。
其他規定	第64條第1項	資料控管者及受託處理者應遵守聯邦資訊安全局相關手冊之建議及指導內容，加入至適當及具體措施之內，使其措施與面臨的風險具有相當性
	第64條第2項	假名化或加密之措施應能夠確保：（1）與處理個人資料有關連的系統及服務，具備機密性、完整性、可用性及彈性要求（2）在發生物理或技術事故時，個人資料的可用性及近用性能夠被快速地回復。
	第71條第1項	決定個人資料處理方式或進行處理時，應取適當的預防措施，並就資料保護影響評估被認為是適當的、有效落實資料保護原則。

38

美國相關規定(1/2)

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

	HIPAA	CCPA	UPDPA
匿名化定義	無法識別出特定個人，且無合理依據相信其可用於識別特定個人之健康資料	不能合理用於推斷有關特定消費者的資料或以其他方式連結至特定消費者的資料	係指已刪除所有直接識別符之個人資料
管理規定	1. 專家核決 2. 安全港條款	1. 採行合理安全措施 2. 承諾不會重新識別 3. 契約要求第三方	合理確保未經允許或者不具備特殊存取權限之人無法透過相關資料識別特定資料主體
效果	受規範機關（構）可以將去識別之健康資訊進行其他目的使用	不適用CCPA	不適用UPDPA
禁止事項	無	禁止重新識別	禁止重新識別

國家發展委員會

39

美國相關規定(2/2)

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

	HIPAA	CCPA	UPDPA
假名化定義	HIPAA僅就匿名化為規範	在不使用額外資料的情形下，以不再連結特定消費者的方式處理個人資料	不包含直接識別符的個人資料，無法合理與資料主體之身分相關連，或無法被維護以允許與資料主體進行個人化的溝通或處理
管理規定		額外資料單獨保存並確保採取資料無法識別或可識別消費者的技術上與組織上措施	無
效果		企業得依據假名化資料為研究	特定情形排除當事人權利行使
禁止事項		禁止重新識別	禁止重新識別

國家發展委員會

40

日本相關規定(1/4)

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

藍色：個人資料保護法施行規則

	假名化
定義	加工後非與其他資料比對**無法識別**特定個人的資料
限制	1. 非依法令不得目的外利用；2. 須公告其利用目的，且不得僅向本人通知；3. 非依法令不得提供予第三方；4. 禁止用於識別特定個人；5.禁止利用聯絡資訊
加工標準	應刪除(替換)個人資料中之姓名、出生年月日及其他得以識別特定個人之記述、個人資料中包含個人識別符號者。 1. 刪除(替換)個人資料中可以識別特定個人之全部或部分記述 2. 刪除(替換)所有個人識別符號 3. 刪除(替換)可能因非法使用所造成財產損失之記述
安全管理措施	資料處理者於「作成假名加工資料時」或「取得假名加工資料及刪除之資料時」，為了防止資料洩漏必須採取安全管理措施。 1. 應明確規範刪除之資料等(包括刪除之資料與加工方法之資料)處理者的權限及責任 2. 應制定有關刪除之資料等處理的規範，並依照該規範進行適當處理，評估處理情形並根據結果採取必要的改善措施 3. 為防止非法權限者近用刪除之資料，應採取必要且適當的措施。
彈性規定	不適用以下規定：1. 變更利用目的之限制；2. 資料外洩報告義務；3. 保有個人資料事項之公告義務、揭露義務、訂正義務、停止利用或刪除等義務

創設假名加工資料係為供事業內部分析用途，諸如市場統計、消費者動向調查等大數據分析

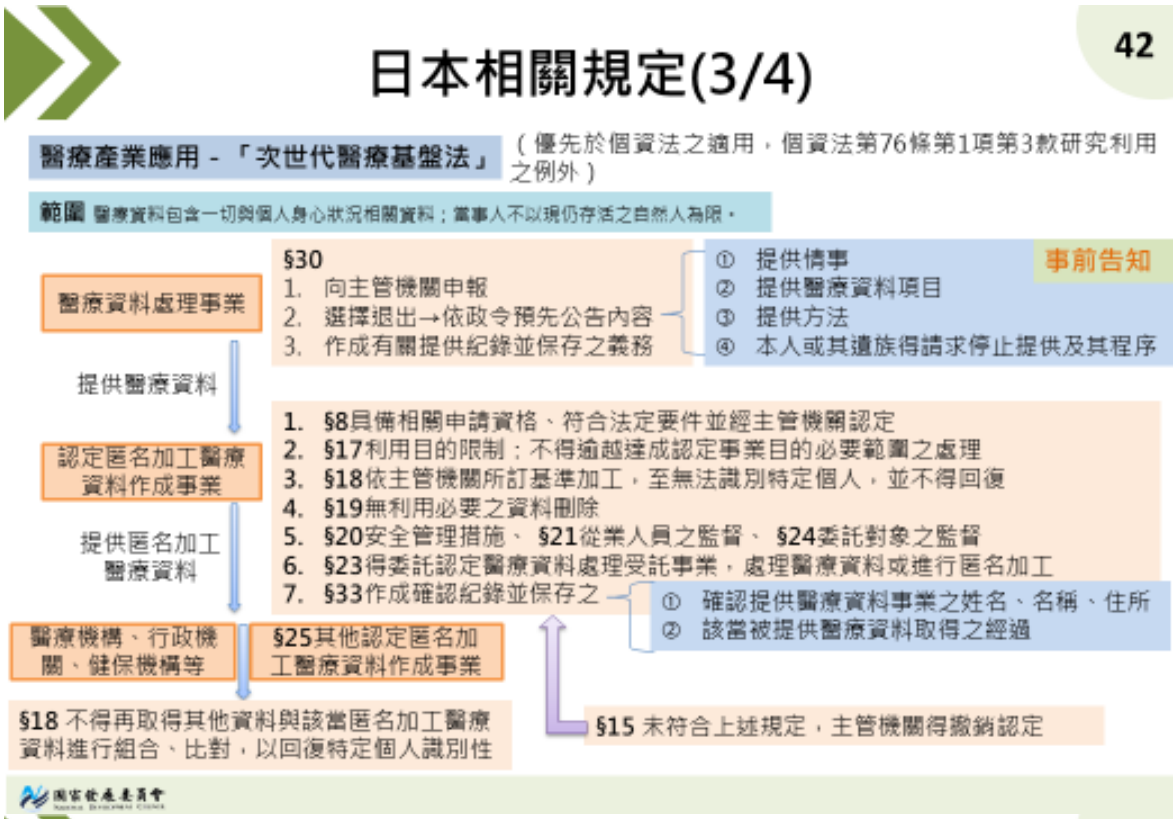
41

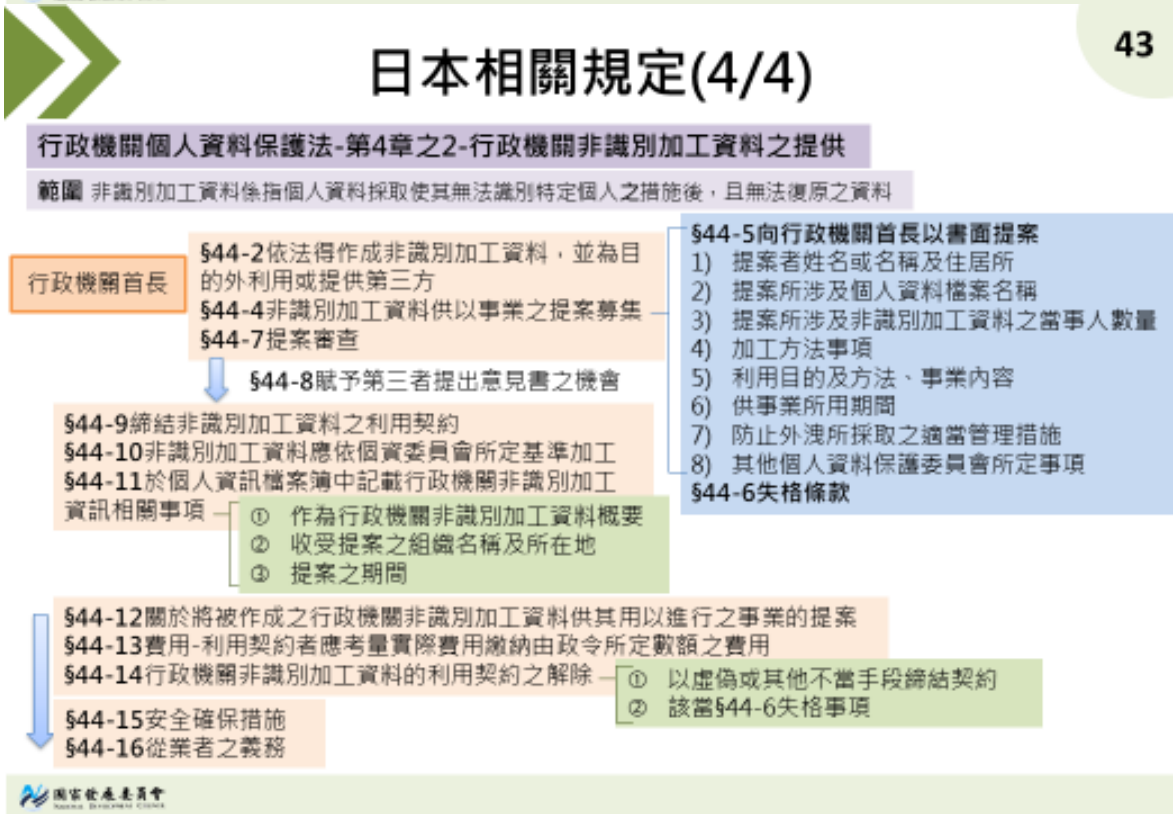
日本相關規定(2/4)

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

藍色：個人資料保護法施行規則

	匿名化
定義	經加工後**無法識別**特定個人且**無法復原**成原始個人資料的資料
限制	1. 識別行為之禁止；2. 於匿名加工後及時利用網路或其他適當方式，公佈匿名加工資料中所包含之個人資料類別；3. 提供予第三人應事先公布匿名加工資料中所包含個人資料類別及其提供之方式，並對該第三人明示所提供為匿名加工資料(明示得利用電子郵件或書面交付等其他適切方式為之)
加工標準	應刪除(替換)個人資料中之姓名、出生年月日及其他得以識別特定個人之記述、個人資料中包含個人識別符號者。 1. 刪除(替換)個人資料中可以識別特定個人的全部或部分記述 2. 刪除(替換)所有個人識別符號 3. 刪除(替換)用於連接個人資料與相應資料採取措施而取得的符號 4. 刪除(替換)特異記述等 5. 考慮其他個人資料資料庫等性質的適當措施
安全管理措施	匿名加工資料處理事業者自身應致力採取對匿名加工資料之安全管理上必要且適當之措施、有關匿名加工資料之申訴處理及其他為確保匿名加工資料之適當處理上所必要之措施，且公告該當措施之內容。 1. 應明確規範刪除之資料等(包括刪除之資料與加工方法之資料)處理者的權限及責任 2. 應制定有關刪除之資料等處理的規範，並依照該規範進行適當處理，評估處理情形並根據結果採取必要的改善措施 3. 為防止非法權限者近用刪除之資料，應採取必要且適當的措施。
彈性規定	允許得未經本人同意，提供予第三人或進行目的外利用


42
日本相關規定(3/4)
醫療產業應用 -「次世代醫療基盤法」（優先於個資法之適用，個資法第76條第1項第3款研究利用之例外）
範圍 醫療資料包含一切與個人身心狀況相關資料；當事人不以現仍存活之自然人為限。
醫療資料處理事業
§30
1. 向主管機關申報
2. 選擇退出→依政令預先公告內容
3. 作成有關提供紀錄並保存之義務
① 提供情事
② 提供醫療資料項目
③ 提供方法
④ 本人或其遺族得請求停止提供及其程序
事前告知
提供醫療資料
認定匿名加工醫療資料作成事業
1. §8具備相關申請資格、符合法定要件並經主管機關認定
2. §17利用目的限制：不得逾越達成認定事業目的必要範圍之處理
3. §18依主管機關所訂基準加工，至無法識別特定個人，並不得回復
4. §19無利用必要之資料刪除
5. §20安全管理措施、 §21從業人員之監督、 §24委託對象之監督
6. §23得委託認定醫療資料處理受託事業，處理醫療資料或進行匿名加工
7. §33作成確認紀錄並保存之
① 確認提供醫療資料事業之姓名、名稱、住所
② 該當被提供醫療資料取得之經過
提供匿名加工醫療資料
醫療機構、行政機關、健保機構等
§25其他認定匿名加工醫療資料作成事業
§18 不得再取得其他資料與該當匿名加工醫療資料進行組合、比對，以回復特定個人識別性
§15 未符合上述規定，主管機關得撤銷認定

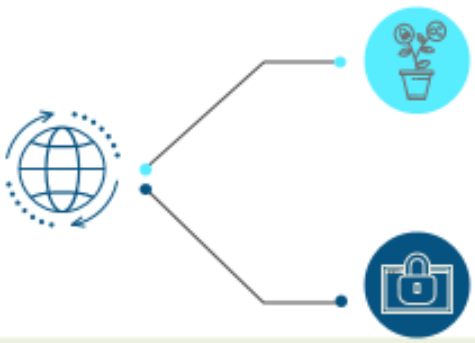

43
日本相關規定(4/4)
行政機關個人資料保護法-第4章之2-行政機關非識別加工資料之提供
範圍 非識別加工資料係指個人資料採取使其無法識別特定個人之措施後，且無法復原之資料
行政機關首長
§44-2依法得作成非識別加工資料，並為目的外利用或提供第三方
§44-4非識別加工資料供以事業之提案募集
§44-7提案審查
§44-5向行政機關首長以書面提案
1) 提案者姓名或名稱及住居所
2) 提案所涉及個人資料檔案名稱
3) 提案所涉及非識別加工資料之當事人數量
4) 加工方法事項
5) 利用目的及方法、事業內容
6) 供事業所用期間
7) 防止外洩所採取之適當管理措施
8) 其他個人資料保護委員會所定事項
§44-6失格條款
§44-8賦予第三者提出意見書之機會
§44-9締結非識別加工資料之利用契約
§44-10非識別加工資料應依個資委員會所定基準加工
§44-11於個人資訊檔案簿中記載行政機關非識別加工資訊相關事項
① 作為行政機關非識別加工資料概要
② 收受提案之組織名稱及所在地
③ 提案之期間
§44-12關於將被作成之行政機關非識別加工資料供其用以進行之事業的提案
§44-13費用-利用契約者應考量實際費用繳納由政令所定數額之費用
§44-14行政機關非識別加工資料的利用契約之解除
① 以虛偽或其他不當手段締結契約
② 該當§44-6失格事項
§44-15安全確保措施
§44-16從業者之義務

44

韓國相關規定(1/2)

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定（2021）

- PIPA修正前，個人資料的定義為「雖無法特定個人，但可以透過結合其他資料輕易辨識出特定個人的資料」作為基準，但範圍無法明確界定，而妨礙資料在產業應用上的分析與運用。
- PIPA修正後，乃以歐盟GDPR的假名資料（pseudonymous data）作為參考依據，仍為PIPA保護的範圍而有保護之必要。
- 假名化資料與匿名化資料區別：



假名資料

1. 屬PIPA定義之個人資料
2. 依法進行假名處理
3. 不使用、結合其他供還原識別之額外資訊，即不能夠再辨識特定個人

匿名資料

以合理之時間、費用、技術予以評估，透過其他資料也無法識別特定個人

45

韓國相關規定(2/2)

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定（2021）

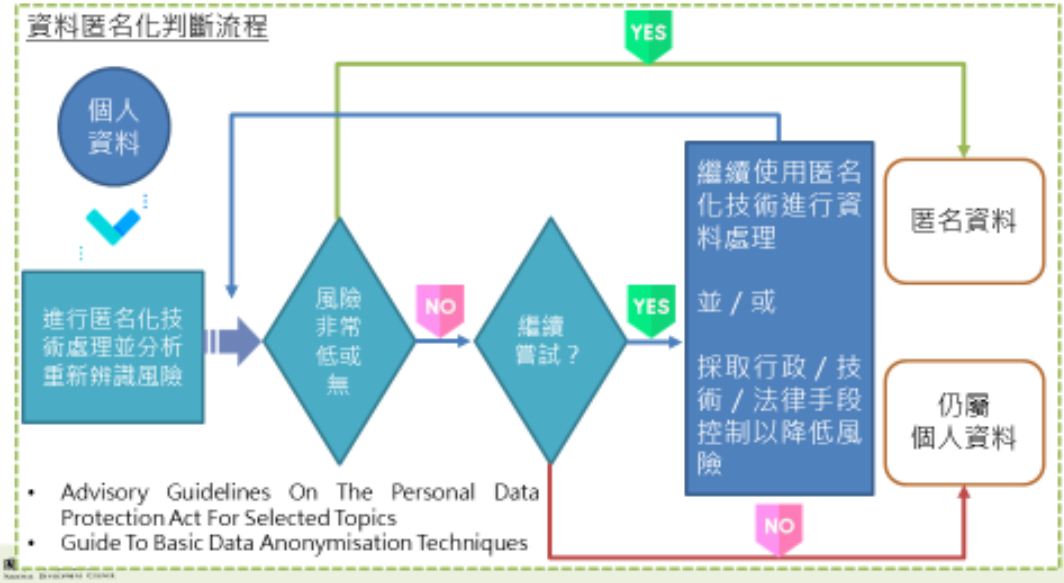
假名資料運用的限制範圍

假名資料限制範圍	內容	條文參照
假名資料的處理限制	• 應由保護委員會或相關中央行政機關首長指定之專門機關執行 • 若欲對外傳輸須取得專門機關負責人的批准方可為之 • 專門機關的指定或取消、輸出暨批准等必要事項，須依施行令定之	28-3
適當安全措施義務	• 應設置適當必要的安全措施，並將可還原辨識特定個人之額外情報分別保管及管理，以防止該個資事故的發生 • 要求個資管理者應填載並保存假名資料處理之目的及向第三方提供時的文管紀錄	28-4
禁止義務	• 任何人均不得以識別特定個人為目的而處理假名資料 • 個資處理者在處理假名資料過程中，產生識別特定個資時應即終止並將該資料銷毀	28-5
不適用假名資料	• 假名資料應經過假名化的處理相較於一般個資更為安全，因此限縮「第 20 條、第 21 條、第 27 條、第 34 條第 1 項、第 35 條至第 37 條、第 39 條之3、第 39 條之 4、第 39 條之 6 至第 39 條之 8 等規定於假名資料不適用」	28-7

46

新加坡相關規定(1/2)

匿名化：透過技術移除資料中可識別標識符，將原始資料轉化為「匿名資料」的過程
匿名資料：已通過匿名化技術且針對特定個人重新識別之風險進行評估的資料



47

新加坡相關規定(2/2)

資料匿名化參考因素

資料性質與類型
- 判斷需要刪除多少識別資訊使其不再可用於識別特定個人
- 樣本資料集內具有特殊資料也可能無法使用匿名化方式

對特定個人潛在影響
- 應考慮重新識別個人身分對特定個人有無任何潛在負面影響
- 若屬於具有高度敏感性質個人資料（例如愛滋病毒感染紀錄）應謹慎考慮是否合適

評估&管理匿名資料重新識別之風險

影響重新識別風險之因素
- 資料利用性質及揭露程度
- 一般大眾認知及個人專業知識
- 揭露數個資料集之情形
- 資料接收者重新識別的能力及動機
- 環境變化

評估重新識別風險之測試
- 「有心侵入者測試」（motivated intruder test）
- 判斷是否可透過動機、能力、資料存取資源（例如網際網路等）從匿名資料重新識別特定個人

重新識別風險之管理
- 應採取適當匿名化技術以確保資料是否確實匿名化
- 考量採取其他適當控制措施降低重新識別風險
- 可透過協議或政策、技術措施或物理措施實施控制措施

違反效果（第9B編有關影響個人資料與匿名資訊之犯罪行為）

(a)個人採取任何行動重新識別，或導致可重新識別受影響之人（亦即與該組織或公共機構所擁有或控制之匿名資料相關者）；(b)重新識別未經該組織或公共機構授權；(c)明知或無視該重新識別未經授權→處以二年以下有期徒刑，或科或併科五千元以下新幣罰款

菲律賓《資料隱私法》

48

最近一次個資法修正：2012年（2017年、2019年分別提出修正案，但未完成立法程序）

定義	• 《資料隱私法》和《資料隱私法施行細則》並未規定 • 匿名化：將個人資料永久地轉換為非個人資料的方法 • 假名化：將個人資料暫時地轉換為非個人資料的方法
判斷標準	• 依個案分析、個案判斷 • 匿名化：可參考ISO / IEC 29100標準，以及去識別化資料接收方是否仍有機會接觸原始資料 • 假名化：例示：電子金鑰加密傳輸
管理規定（組織、程序面）	• 匿名化作業程序：可依照ISO / IEC 29100標準化作業流程辦理，ISO / IEC 29100認證可作為舉證方式之一 • 匿名化資料共享、委託第三人處理經匿名化後的資料：宜訂定資料共享協議（Data Sharing Agreement），以便確認權利義務關係
法律效果	• 匿名化後的資料：排除《資料隱私法》和《資料隱私法施行細則》的適用 • 假名化後的資料：仍受《資料隱私法》和《資料隱私法施行細則》拘束

黑字：《資料隱私法》《資料隱私法施行細則》規定內容
藍字：菲律賓國家隱私委員會諮詢意見（具備拘束效力）

國家發展委員會

大綱

49

一 討論目的及範圍

二 議題分析

三 附件(二)綜整立法例比較

國家發展委員會

綜整立法例比較(1/8)

50

「匿名化」定義及效果

國家		明文規範	定義說明	效果
我國		▲	資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人	不適用個資法
歐盟		O (前言)	採取一切可能合理手段均無法直接識別或間接識別特定個人之資料	不適用個資法（合理運用）
德國				
英國		(ICO)	應使資料以與已識別或可識別的個人無關，或以無法識別個人身分的方式呈現（匿名化、假名化和隱私增強技術指南草案）	
美國	UPDPA	O	已刪除所有直接識別符之個人資料，並可合理確保未經允許或無特殊存取權限之人無法透過相關資料識別特定資料主體	不適用個資法
	CCPA	O	不能合理用於推斷有關特定消費者的資料或以其他方式連結至特定消費者的資料	不適用個資法
	HIPAA	O	無法識別出特定個人，且無合理依據相信其可用於識別特定個人之健康資料	目的外利用
日本		O	個人資料經加工後為無法識別特定個人之資料，且無法復原者	目的外利用、提供第三方
韓國		O	以合理之時間、費用、技術予以評估，當透過其他資料也無法識別特定個人時	不適用個資法
新加坡		▲ (PDPC意見)	將個人資料轉換為無法用於識別任何特定個人之過程，且無論其是否可逆轉回復原始資料	不適用個資法
菲律賓		▲ (NPC意見)	將個人資料永久地轉換為非個人資料	不適用個資法

藍色：非法律明文規定

綜整立法例比較(2/8)

51

「匿名化」加工方式

國家		明文規範	加工方式
我國		▲	個人資料以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者
歐盟		X (WP29)	雜訊加入、排列變更、資料聚集與K匿名（如未刪除原始可識別資料，則仍屬個資）
英國		X	N/A
德國		X	N/A
美國	UPDPA	X	N/A
	CCPA	X	N/A
	HIPAA	O	1.專家核決：由具有統計學、科學原則及方法上適當知識及廣泛接受之經驗，以該適當的原則及方法認定資料接受者不論單獨利用或與其他合理可得之資料一併使用，皆僅有極小風險可識別特定個人，並以書面方式說明其方法及分析結果 2.安全港條款：依據隱私規則刪除18項識別因子，且無論受規範主體單獨使用或合併其他資訊，均無「實際具體知識」得識別健康資料之特定個人
日本		O ※施行規則	應刪除(替換)個人資料中之姓名、出生年月日及其他得識別特定個人之記述、個人識別符號 ※刪除(替換)連結個資相應措施之符號、特異記述，並考量構成資料庫之相當措施
韓國		X	N/A
新加坡		X (PDPC意見)	組織應自行評估狀況及營運環境，視資料類型採用最合適之匿名化技術，如假名化、資料彙集、取代、資料抑制、資料重組或概括化、資料清洗、遮蔽
菲律賓		X (NPC意見)	建議匿名化處理程序依照ISO/IEC 29100所訂之標準化作業流程辦理

藍色：非法律明文規定

綜整立法例比較(3/8)

52

「匿名化」管理措施

國家		明文規範	管理措施
歐盟		X (WP29)	政府資訊公開前，應進行風險評估（GDPR§35針對新技術處理個資前應先進行DPIA）
英國		X (ICO)	應注意匿名化授權及監督責任、員工培訓、識別可能需匿名化情形之程序、新指南或判例法之知識管理、相關行業組織、隱私影響評估、透明度、審查匿名程序後果、事故回復
德國		X	N/A
美國	UPDPA	X	N/A
	CCPA	O	1.採取所有合理措施確保資料未與消費者或家庭相關連；2.由進行研究之企業進行額外安全控制，限制對研究資料之存取，僅執行研究目的必要之人始得存取資料；3.防止資料外洩
	HIPAA	X	N/A
日本		O ※施行規則	匿名加工資料之作成、申訴對應處理機制及確保匿名資料受適當處理之其他必要措施 ※1.應明確處理者之權限及責任；2.應制定處理規範並評估進行改善；3.防止無權近用之措施
韓國		X	N/A
新加坡		X (PDPC意見)	重新識別風險的評估及管理：將單獨資料集進行合併處理前，組織應針對重新識別風險進行評估，考量是否可能存在資料集中識別出特定個人的可能性
菲律賓		X (NPC意見)	建議匿名化處理程序依照ISO/IEC 29100所訂之標準化作業流程辦理

藍色：非法律明文規定

綜整立法例比較(4/8)

53

「匿名化」義務要求

國家		明文規範	義務要求
歐盟		X (WP29)	禁止重新識別
德國			
英國		O (ICO)	禁止重新識別
美國	UPDPA	O	禁止重新識別或導致重新識別以蒐集或建立個人資料
	CCPA	O	1.公開承諾以去識別化方式維護與利用資料且不重新識別資料；2.以契約要求接收方遵循CCPA去識別化規定；3.以蒐集個資背景相關之研究目的為限；4.除研究必要外禁止重新識別
	HIPAA	X	N/A
日本		O ※施行規則	1.禁止重新識別；2.公告匿名加工資料所包含之個資類別及提供方式；3.向第三方明示其所提供為匿名加工資料 ※1.公告得以網路或其他適當方式；2.明示得以電子郵件或書面交付等其他適當方式
韓國		X	N/A
新加坡		O	禁止重新識別
菲律賓		X	N/A

藍色：非法律明文規定

綜整立法例比較(5/8)

54

「假名化」定義及效果

國家		明文規範	定義說明	效果
我國		X	N/A	N/A
歐盟		O	個人資料經處理後，在無額外資料的情形，無法識別特定個人	免個資事故通知、排除當事人權利行使
英國				
德國				
美國	UPDPA	O	不包含直接識別符的個人資料，無法合理與資料主體之身分相關連，或無法被維護以允許與資料主體進行個人化的溝通或處理	排除當事人複製權、更正權
美國	CCPA	O	在不使用額外資料的情形下，以不再連結特定消費者的方式處理個人資料	可供研究利用
美國	HIPAA	X	N/A	N/A
日本		O	個人資料經加工處理後，非與其他資料比對無法識別特定個人之資料	變更利用目的、免個資事故通知、排除當事人權利行使
韓國		O	個人資料經處理且不使用、結合其他供還原識別之額外資訊，無法識別特定個人之資料	可供科學利用、保存期限銷毀、免個資事故通知、排除當事人權利行使
新加坡		X	N/A	N/A
菲律賓		X (NPC意見)	將個人資料暫時地轉換為非個人資料	不適用個資法

藍色：非法律明文規定

綜整立法例比較(6/8)

55

「假名化」加工方式

國家		明文規範	加工方式
歐盟		X (WP29)	加密、雜湊函數、記號化
英國			
德國			
美國	UPDPA	X	N/A
美國	CCPA	X	N/A
美國	HIPAA	X	N/A
日本		O ※施行規則	應刪除(替換)個人資料中之姓名、出生年月日及其他得識別特定個人之記述、個人識別符號 ※刪除(替換)可能因非法使用所造成財產損失之記述
韓國		O	藉由刪除或替代個人資料之全部、部身分等方法，在沒有其他額外資料之情形下，就無法識別特定個人而為資料處理之過程
新加坡		X (PDPC意見)	利用其他方法替換個人識別符號，用編造數值替代身分辨識資訊
菲律賓		X (NPC意見)	電子金鑰加密傳輸

藍色：非法律明文規定

綜整立法例比較(7/8)

56

「假名化」管理措施

國家		明文規範	管理措施
歐盟		O (前言) (ENISA*)	應採取必要技術及組織措施確保處理過程符合本規則並將額外資訊分開存放 1.被假名化的機密應與假名化後的資料分開於不同的檔案夾，避免存放於不安全的媒體中； 2.組織應建立管理制度或準程，對於存取權限進行高強度管理，僅具權限相關人員始得存取被假名化的機密，存取紀錄應以log紀錄為之； 3.被假名化的機密應進行加密，並注意加密後之金鑰管理及存放
英國			
德國			
美國	UPDPA	X	N/A
	CCPA	O	額外資料單獨保存並確保採取資料無法識別或可識別消費者的技術上與組織上措施
	HIPAA	X	N/A
日本		O ※施行規則	「作成假名加工資料時」或「取得假名加工資料及所刪除資料時」應採取安全管理措施，避免第三方藉刪除之資料與假名加工資料進行比對以識別特定個人 ※1.應明確處理者之權限及責任；2.應制定處理規範並評估進行改善；3.防止無權近用之措施
韓國		O	組織應依照設置技術上、管理上及物理上之必要安全措施，將額外可還原辨識特定個人資料分別管理，以防止遺失、竊取、洩漏、變造及毀損等情事；而在處理該假名資料時，應依規定填載目的，並保存相關文件管理紀錄
新加坡		X	N/A
菲律賓		X	N/A

藍色：非法律明文規定

綜整立法例比較(8/8)

57

「假名化」義務要求

國家		明文規範	義務要求（限制）
歐盟		X	N/A（仍適用個資一般規範）
英國		O	禁止重新識別
德國		X	N/A（仍適用個資一般規範）
美國	UPDPA	O	禁止重新識別或導致重新識別以蒐集或建立個人資料
	CCPA	O	1.以蒐集個資背景相關之研究目的為限；2.除研究必要外禁止重新識別
	HIPAA	X	N/A
日本		O	1. 非依法令不得目的外利用；2. 須公告其利用目的，且不得僅向本人通知；3. 非依法令不得提供予第三方；4.禁止用於識別特定個人；5.禁止利用聯絡資訊
韓國		O	1.基於統計編制、科學研究及保存公益紀錄等目的為限
新加坡		X	N/A
菲律賓		X	N/A

藍色：非法律明文規定

「個人資料保護法相關議題」第 5 場產學專家學者諮詢會議—受託處理者義務

議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」及新加坡「個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於受託處理之法律概念、法律關係、責任義務及效果歸屬之探討。

貳、議程

一、 主席致詞

二、 報告事項

受託處理者義務之探討(國發會)

三、 討論事項

我國有關受託處理者之規定，主要規範於個資法第 4 條規定「受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。」、個資法施行細則第 7 條規

定「受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。」及第 8 條「委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。(第 1 項）前項監督至少應包含下列事項：一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。二、受託者就第十二條第二項採取之措施。三、有複委託者，其約定之受託者。四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。五、委託機關如對受託者有保留指示者，其保留指示之事項。六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。(第 2 項）第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。(第 3 項）受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。(第 4 項)」。

針對上述規定，蒐整實務相關函釋見解，進行比較法之分析。綜觀各國個資保護規範，無法僅聚焦於受託處理者之義務面向討論，而係應宏觀地析梳整體委託關係之相關議題。尤其，在資訊快速流通的時代，許多企業在專業化及整體成本的考量下，會選擇將非核心業務委由專業公司處理，而其中若涉及個人資料的委外，則會產生委外廠商蒐集、處理與利用個人資料之問題，而涉及並可能適用個資法上的委託關係之相關規範。

案由一、委託關係之定義

說明：

依據我國個資法第 4 條、個資法施行細則第 7 條以及第 8 條之規定，對於個資法上之「委託」、「委託機關」或「受託者」缺乏明確的概念定義。為釐清具體個案上是否為個資法上委託關係，個資法主政機關歷來已多次針對個案適用狀況做成函釋予以闡釋。

觀察比較法上其他國家在個資委託之規範，例如歐盟、英國及德國將決定個資處理目的及方式者，定義為資料控管者，而為資料控管者處理個資者為受託處理者；美國 CCPA 則係定義資料控管者為蒐集、決定個資處理目的及方式之營利事業，而為於營利目的內處理或接收個資之

服務提供者或承包商則為受託處理者;日本則是將個人資訊資料庫等供事業利用者定義為資料控管者,而受個人資料處理事業委託個人資料之處理者定義為受託處理者;韓國以委託他方處理個資業務者為資料控管者,而受託處理者係受託處理個資業務之人;最後,新加坡則以決定個資處理目的及方式為資料控管者,而代表組織並為其目的處理個資者為受託處理者。

小結：目前我國個資法對於「委託機關」及「受委託機關」並無定義，但綜觀國際間多數國家，多以是否決定個資處理（含蒐集、利用）之目的、方法，或僅依其指令處理，作為委託機關（控管者）、受委託機關（處理者）之定義。我國個資法是否有必要以定義方式釐清委託機關、受委託機關之意涵？若須定義，以是否決定個資處理之目的、方法作為判斷基礎是否恰當？

案由二、共同控管者概念

說明：

我國個資法目前對於不同組織間對個資處理之權利義務安排，僅有個資法第 4 條所定之「委託、被委託」關係。然而，在進入資料、數位經濟時代後，資料利用的樣態漸趨複雜,許多資料利用樣態似乎並非單純的委託與被委託關係。（例如 A 賣場欲蒐集客戶資料進行分析，以擬定行銷策略；而 B 資料統計公司希望藉由與 A 賣場合作，蒐集、處理與利用 A 賣場客戶資料訓練其所設計的精準商品推薦應用程序或完善其資料統計軟體，則雙方對客戶資料之蒐集、處理、利用，已非單純 A 賣場委託 B 公司之關係）。

歐盟為處理前述漸趨複雜的個資蒐集、處理、利用樣態，引入「共同控管者」概念，要求「共同決定資料處理目的或方法」的不同資料控管者，必須約定彼此對法定義務的責任安排。

小結：資料經濟時代下，個資的蒐集、處理、利用不只是單純的由單一業者基於其自身之需求而獨立蒐集處理個資，或透過委託第三方協助處理個資以達所需目的之情況，亦會出現共同

決定個資蒐集、處理、利用之目的、方法的情形。若參考歐盟共同控管者概念，是否有助於業者釐清彼此個資處理關係，而有利於產業運用個人資料？

案由三、個資法上委託關係之監督管理

說明：

我國目前個資法對於委託關係，僅於第 4 條中規定受委託機關於本法適用範圍內，視同委託機關。復於個資法施行細則第 8 條要求委託機關對受委託機關為適當之監督，並於第 2 項中臚列資料利用方法、安全維護措施、複委託、事故通知、保留指示及資料刪除、返還等應監督事項。

與此相較，本次研究範圍內之其他國家，則多以法律方式要求委託者與受委託者間，應以書面方式約定上述資料利用方法、安全維護措施、複委託等事項，並要求委託機關應監督其落實，並課予受委託機關安全維護、通報等責任。

小結：目前我國並未以法律規定委託關係間之監督管理責任，僅於施行細則中要求委託機關就特定事項監督受委託機關。

1. 參酌國際規範，我國個資法是否應以法律位階要求雙方應約定委託關係內之重要事項？此種約定是否應以書面為之？應約定之重要事項應包含哪些項目（如個資處理利用方法、安全維護措施、複委託、事故通知、保留指示及資料刪除、返還等）？

2. 我國個資法目前要求受委託機關於本法適用範圍內，視同委託機關，而須遵循委託機關適用的義務規定。但委託關係內的重要事項（如事故通報委託機關等）是否應以法律位階課予受委託機關遵循之義務？

受託處理者義務

國家發展委員會
111年 2月 25日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（假名化、匿名化）	受託處理者義務	國際傳輸	框架性討論	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25							

2

大綱

一 討論範圍

二 我國個資法相關規定

三 比較法及議題分析

四 附件

3

一、討論範圍

■ 討論範圍

以「受託處理者」為主軸，討論委託定義、委託關係、效果歸屬、責任義務之規範要件，不深究委託機關的規範，而有關罰則置於其他場次討論，並以「個資法」為主要討論範疇。

■比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員

國家發展委員會

4

大綱

一 討論範圍

二 我國個資法相關規定

三 比較法及議題分析

四 附件

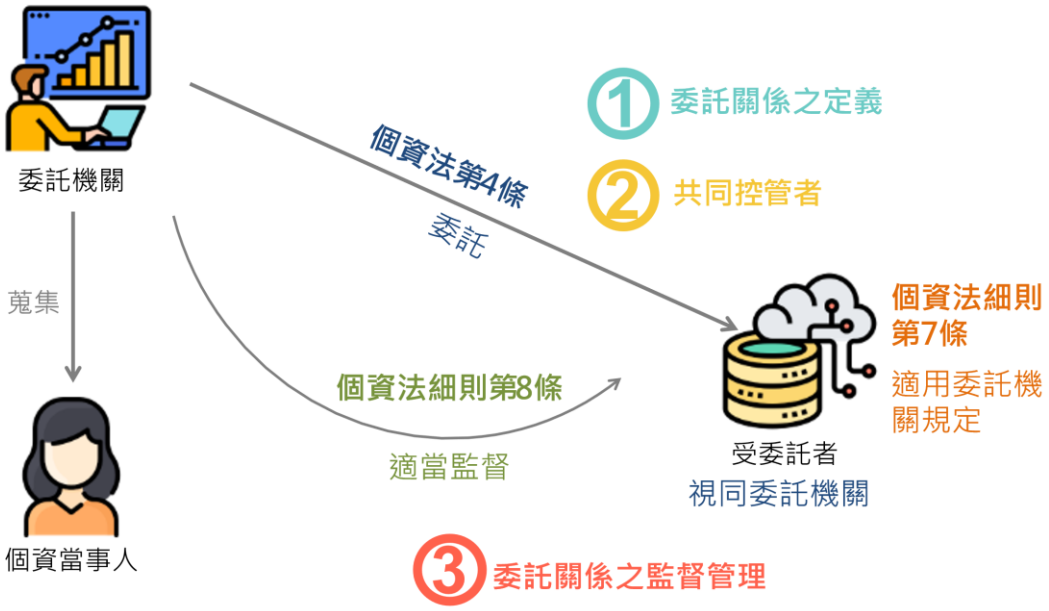
5

二、我國個資法相關規定（1/2）

個人資料保護法	個人資料保護法施行細則
第4條 受公務機關或非公務機關委託蒐集、處理或利用個人資料者，於本法適用範圍內，視同委託機關。	**第7條** 受委託蒐集、處理或利用個人資料之法人、團體或自然人，依委託機關應適用之規定為之。 **第8條** 委託他人蒐集、處理或利用個人資料時，委託機關應對受託者為適當之監督。 前項監督至少應包含下列事項： 一、預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間。 二、受託者就第十二條第二項採取之措施。 三、有複委託者，其約定之受託者。 四、受託者或其受僱人違反本法、其他個人資料保護法律或其法規命令時，應向委託機關通知之事項及採行之補救措施。 五、委託機關如對受託者有保留指示者，其保留指示之事項。 六、委託關係終止或解除時，個人資料載體之返還，及受託者履行委託契約以儲存方式而持有之個人資料之刪除。 第一項之監督，委託機關應定期確認受託者執行之狀況，並將確認結果記錄之。 受託者僅得於委託機關指示之範圍內，蒐集、處理或利用個人資料。受託者認委託機關之指示有違反本法、其他個人資料保護法律或其法規命令者，應立即通知委託機關。

二、我國個資法相關規定（2/2）

6



國家發展委員會

大綱

7

一 討論範圍

二 我國個資法相關規定

三 比較法及議題分析

四 附件

國家發展委員會

案由一、委託關係之定義(1/2)

8

		委託人	受託人	適用主體		
		定義		自然人	法人	團體
我國		N/A（委託蒐集、處理、利用個資）		O	O	O
歐盟		決定個資處理目的及方式	替資料控管者處理個資	O	O	O
德國						
英國						
美國	CCPA CPRA	蒐集、決定個資處理目的及方式的營利事業	替資料控管者於營利目的內處理或接收個資	O	O	O
	UDPDA	決定個資處理目的及方式	替資料控管者處理個資	O	O	O
日本		N/A（委託蒐集、處理、利用個資）		O	O	X
韓國		委託他方處理個資業務者	受託處理個資業務者	O	O	X
新加坡		決定個資處理目的及方式	代表組織並為其目的處理個資	O	O	O

國際間多數國家，多以是否決定個資處理（含蒐集、利用）之目的、方法，或僅依其指令處理，作為委託機關、受委託機關之定義。

國家發展委員會 National Development Council

案由一、委託關係之定義(2/2)

9

		委託人	受託人
		定義	
我國		N/A（委託蒐集、處理、利用個資）	
歐盟		決定個資處理目的及方式	替資料控管者處理個資
德國			
英國			
美國	CCPA CPRA	蒐集、決定個資處理目的及方式的營利事業	替資料控管者於營利目的內處理或接收個資
	UDPDA	決定個資處理目的及方式	替資料控管者處理個資
日本		N/A（委託蒐集、處理、利用個資）	
韓國		委託他方處理個資業務者	受託處理個資業務者
新加坡		決定個資處理目的及方式	代表組織並為其目的處理個資

Q 委託關係之定義

- 我國個資法是否有必要以定義方式釐清委託機關、受委託機關之意涵？
- 若須定義，以「是否決定個資處理之目的、方法」作為判斷基礎是否恰當？

國際間多數國家，多以是否決定個資處理（含蒐集、利用）之目的、方法，或僅依其指令處理，作為委託機關、受委託機關之定義。

國家發展委員會 National Development Council

10

案由二、共同控管者概念(1/2)

資料經濟時代下，個資的蒐集、處理、利用不只是單純的由單一業者基於其自身之需求而獨立蒐集處理個資，或透過委託第三方協助處理個資以達所需目的之情況，亦會**出現共同決定個資蒐集、處理、利用之目的、方法的情形**。

11

案由二、共同控管者概念(2/2)

	因應方法	效果
我國	分別適用委託或公務、非公務機關規範	
歐盟 德國 英國	共同控管者 （共同決定資料處理目的或方法）	約定彼此對法定義務的責任安排 （須共同處理當事人權利事項）

Q

共同控管者概念

若參考歐盟共同控管者概念，是否有助於業者釐清彼此個資處理關係，而有利於產業運用個人資料？

案由三、個資法上委託關係之監督管理（1/3）

12

- 個資法並未規範委託關係中之監督管理措施
- 施行細則中，要求委託機關監督受託者，並規範監督之必要項目：
  - 方法（預定蒐集、處理或利用個人資料之範圍、類別、特定目的及其期間）
  - 安全維護措施
  - 複委託之受託者
  - 事故通知委託機關
  - 保留指示事項
  - 關係中止解除之返還刪除
- 施行細則中，要求受託者認為指示違法時，應通知委託機關。

案由三、個資法上委託關係之監督管理（2/3）

13

	監督管理方法			受託者義務	規範形式
	約定	監督	約定或監督必要內容		
我國	X	○	方法、安維、複委託、事故通知、保留指示、刪除返還	指示違法通知	施行細則
歐盟	要式	○	方法（書面）、安維、複委託（書面）、保密、協助權利處理、協助安維、刪除返還、受監督	指示違法通知、事故通知	法律
德國					
英國					
美國 CCPA CPRA	要式	○	遵守指示、複委託（通知）		法律
美國 UDPDA	X			協助安維	法律
日本	指引建議	○	方法、安維、複委託		指引
韓國	要式	○	方法、安維、銷售之告知、受監督、訓練		法律
新加坡	要式		方法	事故通知	法律
			安維、受監督、刪除返還		指引

多要求以要示方法約定　　事故通知為法定義務　　多以法律位階規範

案由三、個資法上委託關係之監督管理（3/3）

14

個資法上委託關係之監督管理

目前我國並未以法律規定委託關係間之監督管理責任，僅於施行細則中要求委託機關就特定事項監督受委託機關。

（1）
我國個資法是否應以法律位階要求雙方應約定委託關係內之重要事項？
此種約定是否應以書面為之？
應約定之重要事項應包含哪些項目？
（如個資處理利用方法、安全維護措施、複委託、事故通報、保留指示及資料刪除、返還等）

（2）
我國個資法目前要求受委託機關於本法適用範圍內，視同委託機關，而須遵循委託機關適用的義務規定。
但委託關係內的重要事項（如事故通報委託機關等）是否應以法律位階課予受託機關遵循之義務？

議題討論

15

- **案由一、委託關係之定義**
  - 我國個資法是否有必要以定義方式釐清委託機關、受委託機關之意涵？
  - 若須定義，以「是否決定個資處理之目的、方法」作為判斷基礎是否恰當？
- **案由二、共同控管者概念**
  - 若參考歐盟共同控管者概念，是否有助於業者釐清彼此個資處理關係，而有利於產業運用個人資料？
- **案由三、個資法上委託關係之監督管理**

  目前我國並未以法律規定委託關係間之監督管理責任，僅於施行細則中要求委託機關就特定事項監督受委託機關。
  - （1）我國個資法是否應以法律位階要求雙方應約定委託關係內之重要事項？此種約定是否應以書面為之？應約定之重要事項應包含哪些項目？（如個資處理利用方法、安全維護措施、複委託、事故通報、保留指示及資料刪除、返還等）
  - （2）我國個資法目前要求受委託機關於本法適用範圍內，視同委託機關，而須遵循委託機關適用的義務規定。但委託關係內的重要事項（如事故通報委託機關等）是否應以法律位階課予受託機關遵循之義務？

16

大綱

一 討論範圍

二 我國個資法相關規定

三 比較法及議題分析

四 附件

17

歐盟GDPR

最近一次個資法修正：2016年（2018年施行）

適用主體	資料控管者（controller）	受託處理者（processor）
定義	決定個人資料處理目的及方式的人	替資料控管者處理個人資料的人
義務	• 盡GDPR第5條第1項資料保護原則 • 採取適當技術上、組織上的措施以確保資料處理符合GDPR要求 • 落實設計包含隱私原則 • 個資事故通知義務 應任用有效保證會採取適當技術上與組織上措施的受託處理者，且以書面契約委託、書面方式下指令	• 依資料控管者書面指令處理資料，如認為指令違反GDPR，應立即告知 • 全體員工盡保密義務 • 達到安全處理要求 • 複委託應取得資料控管者書面授權同意 • 協助資料控管者履行資料主體權利 • 協助資料控管者履行安全處理、資料保護影響評估、監管機關諮詢要求 • 刪除或歸還個人資料 • 提供資料控管者所有資料以證明遵循其義務 • 個資事故通知義務
	紀錄	

18

英國UK GDPR

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

適用主體	資料控管者（controller）	受託處理者（processor）
定義	決定個人資料處理目的及方式的人	替資料控管者處理個人資料的人
義務	• UK GDPR第5條第1項資料保護原則 • 採取適當技術上、組織上的措施以確保資料處理符合UK GDPR要求 • 落實設計包含隱私原則 • 個資事故通知義務	應任用有效保證會採取適當技術上與組織上措施的受託處理者，且以書面契約委託、書面方式下指令 • 依資料控管者書面指令處理資料，如認為指令違反UK GDPR，應立即告知 • 全體員工盡保密義務 • 達到安全處理要求 • 複委託應取得資料控管者書面授權同意 • 協助資料控管者履行資料主體權利 • 協助資料控管者履行安全處理、資料保護影響評估、監管機關諮詢要求 • 刪除或歸還個人資料 • 提供資料控管者所有資料以證明遵循其義務 • 個資事故通知義務
	紀錄	

國家發展委員會

19

德國BDSG

最近一次個資法修正：2021年6月23日
歐盟成員國

當事人	資料控管者（Oerantwortlicher）	受託處理者（AuftragsOerarbeiter）
• 資訊權 • 更正權 • 刪除權 • 處理限制權 • 損害賠償權	• 個資事故侵害事故之通報義務 • 重大個資事故侵害事故通知當事人	• 依指示處理 • 協力義務 • 文件紀錄義務 • 配合驗證 • 個資侵害事故之報告義務 • 返還、刪除或銷毀義務
處理者違反規定處理目的/方式時，視為資料控管者 • 損害賠償權	• 保密義務 • 確保資料安全的責任 • 涉及特種個資時，應採取適當且具體之措施	• 提供適當保障的責任 • 進行資料影響評估 • 非公務機關 任命資料保護長 • 複委託之要求

國家發展委員會

美國相關規定（1/2）

20

無聯邦個資法，加州消費者隱私法（CCPA）最近修正為2018年，修正CCPA的新法CPRA將於2023年實施，效力溯及2022年1月1日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

法規	CCPA & CPRA	UPDPA
處理人名稱	• 服務提供者：為營利事業的營利目的，依書面契約提供必要服務而處理個資者（*Cal. CiO. Code 1798.140 (O)*） • 承包商：自營利事業為營利目的，依書面契約獲得消費者個資者（*CPRA 1798.140 (j)(1)*）	處理者 （*UPDPA § 2(12)*）
控管人名稱	• 營利事業	• 控管者，含蒐集控管者（直接蒐集個資）、第三方控管者（另外決定個資的使用目的和方式）（*UPDPA § 2 (1)、(3)、(21).*）
是否須書面契約	• 是 （*Cal. CiO.* Code 1798.140(O)(w)、*CPRA 1798.140 (j)(1)*）	N/A
控管人監管處理人義務	營利事業應要求服務提供商及承包商： • 符合本法所定義務，並要求其具同樣隱私保護標準； • 賦予營利事業採取合理適當措施的權利，以確保服務提供商及承包商使用個人資料時的傳輸行為符合本法對營利事業的義務要求； • 於無法遵守本法規定之義務時告知營利事業。 • 賦予營利事業採取合理適當措施的權利，以停止或補救未經授權的個人資料使用。（*CPRA 1798.100 (d)**）	• 蒐集控管者應以合理努力確保第三方控管者和處理者行資料更正（*UPDPA § 5(b)*）

美國相關規定（2/2）

21

法規	CCPA & CPRA		UPDPA
處理人義務	**服務提供商**	**承包商**	• 協助控管者回應請求，包括提供個資或存取權限、修正個資 • 不在控管者請求外處理個資 • 實施、維持、更新資料隱私和資安評估 • 處理者如進行不相容或禁止的資料處理行為，應行補正（*UPDPA § 4(b)、5(b)、10(a)(b)*）
	皆須於契約內同意： • 不販售或分享個資 • 不在契約明定目的外保有、使用、揭露個資 • 不在與營利事業的直接商業關係外保有、使用揭露個資 • 不擅自將從營利事業獲得的個資，和從他處獲得或自己蒐集到的個資相結合（*Cal. CiO. Code 1798.140(O) (A)~(D)、CPRA 1798.140 (ag)(1)、CPRA 1798.14 (j)(1)* **承包商**並另須於契約中約定： • 提供承包商理解上述限制的證書 • 允許營利事業監管承包商合規性（*CPRA 1798.140 (j)(1)(A)~(C)*） **服務提供商及承包商**其他契約外義務： • 經營利事業依請求之指示刪除個資，並通知複委託對象 • 提供協助以利營利事業回應請求（*CPRA 1798.105(c)(3)*） **再委託：** • 服務提供商及承包商皆應告知營利事業再委託，並應有書面契約遵守CCPA及CPRA（*CPRA* 1798.140 *(j)(2)、(ag)(2)*）		
責任歸屬	• 服務提供商和承包商為自己的違反行為負責，並有義務協助營利事業回應請求，並有義務告知其他接收其個資的服務提供商和承包商。 • 服務提供商和承包商於違反規定時，須控管者揭露資料時不知悉違反意圖才不用負責。（*UPDPA § 4(b)、CPRA 1798.140 (i)(1)*）		• 如不相容或禁止的處理行為所處理的個資是由控管者蒐集，或由處理者處理，且控管者或處理者明知會有該處理行為且有防止義務時，控管者或處理者有責任（*UPDPA § 4(c)*）

22

日本情報法

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

	資料控管者	受託處理者
名稱	個人資料處理事業者 （個人情報取扱事業者）	受委託人（委託先）
概念	將個人資訊資料庫等供事業利用者	受個人資料處理事業委託個人資料之全部或部分處理者
義務	對受委託人之監督	X（法條解釋應負安全管理措施義務）

●監督義務之必要事項：
1. 選定適當之受託處理者 - 選定前應先確認受託處理者至少應符合第20條已採取必要且適當之安全管理措施。
2. 簽訂委託契約 - 雙方必須簽訂委託契約，契約內容應包括監督義務之必要事項及雙方同意之內容。
3. 掌握受託處理者對於個人資料處理之情形 - 應定期對受託處理者進行檢查及風險評估。

如有複委託情形，受託處理者應事前報告取得資料控管者同意，並對複委託者適用前述規定。
※針對醫療產業依次世代醫療基盤法之委託亦設有相似規定。

國家發展委員會

23

韓國PIPA（1/3）

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性認定進入最終程序

一、蒐集主體及受託處理者

- PIPA對於委託者與受託者的定義：

委託他方處理個人資料處理業務之個人資料處理者為「委託者」（「위탁자」）

受託處理該個人資料業者為「受託者」（「수탁자」）

部分對於委託方於委託業務之規定於受託者準用

- 受託者若發生個資事故，以致個資外洩，委託者亦須承擔責任。
- PIPA規定委託者應使個資當事人可隨時確認該委託業務內容以及受託者為何人。
  - 若有委託情形，應以文書訂明：委託之目的、禁止事項、適當安全維護措施；
  - 若涉及商品宣傳銷售、被委託業務內容及受託者有變更時，應履行告知義務；
  - 委託者應對受託者盡教育訓練、檢查及監督之責。

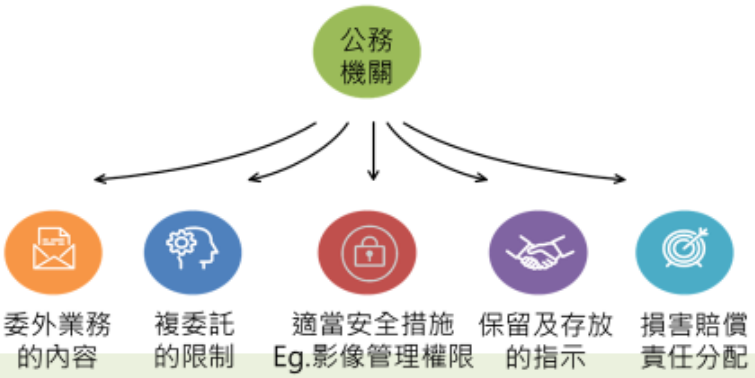
國家發展委員會

24

韓國PIPA（2/3）

二、關於影像處理者委外的特殊規定

- PIPA針對影像處理者委外的特殊規定在第25條第8項，影像資料處理設備的操作者得將有關設置或操作影像資料處理設備的相關事務委託第三方辦理。
- 公務機關設置或操作影像資料處理業務委託於第三方時，其程序及條件應依據個資施行細則規定。
- 根據個資法施行細則第26條，公務機關若將影像處理業務的設置及操作委外，應以書面形式說明以下內容，並應將委託方以下資訊及聯絡方式公告：

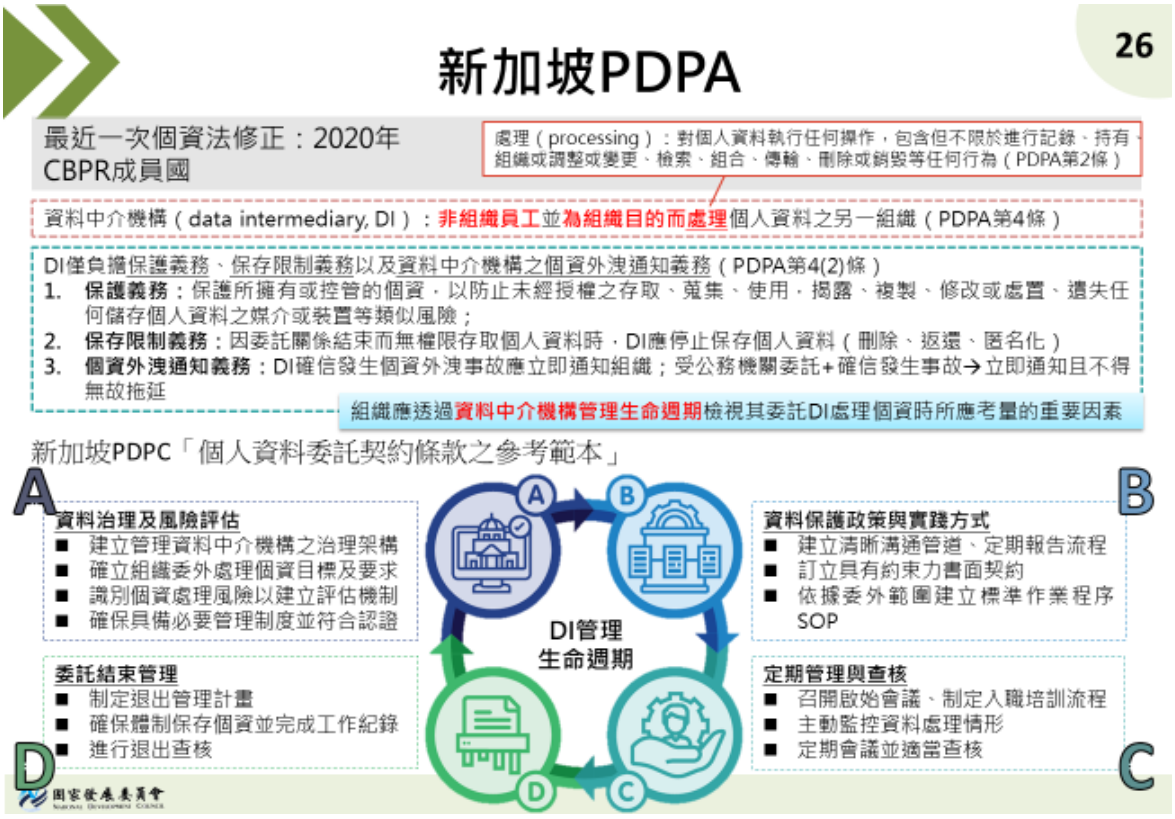


25

韓國PIPA（3/3）

三、個資委外的限制範圍

PIPA第26條委託處理個資業務之限制	內容
	• 個資處理者向第三方委託個人資料之處理業務時，應書面揭露： ➢ 履行委託事務目的外，禁止處理個資之相關事項； ➢ 保護個人資料之技術性、管理性等適當安全維護措施； ➢ 其他為個資法施行細則安全管理個人資料而定之事項。
	• 委託者應使個資當事人可隨時確認該委託業務內容及受託者 • 委託者發出要約或要約的引誘時，應依告知個資當事人被委託業務之內容及受託者；當被委託業務之內容及受託者有所變更時亦同。
	• 委託者應監督受託者是否安全的方式處理個資，以避免個資當事人之個人資料有遺失、竊取、洩漏、變造及毀損等情事。
	• 受託者利用或對第三方提供之個人資料，不得逾越個人資料處理者委託之業務範圍。
	• 受託者於處理與受託業務相關之個人資料過程中，因違反PIPA而發生損害賠償責任時，視為個人資料處理者。
PIPA第75條罰鍰	• 違反第26條第1項未揭露委託業務之書面內容且未包含同項各款所定者，以及違反第26條第2項未公開委託業務之內容及受託者，將課賦1千萬以下韓圜。


26
新加坡PDPA
最近一次個資法修正：2020年
CBPR成員國
處理（processing）：對個人資料執行任何操作，包含但不限於進行記錄、持有、組織或調整或變更、檢索、組合、傳輸、刪除或銷毀等任何行為（PDPA第2條）
資料中介機構（data intermediary, DI）：非組織員工並為組織目的而處理個人資料之另一組織（PDPA第4條）
DI僅負擔保護義務、保存限制義務以及資料中介機構之個資外洩通知義務（PDPA第4(2)條）
1. 保護義務：保護所擁有或控管的個資，以防止未經授權之存取、蒐集、使用、揭露、複製、修改或處置、遺失任何儲存個人資料之媒介或裝置等類似風險；
2. 保存限制義務：因委託關係結束而無權限存取個人資料時，DI應停止保存個人資料（刪除、返還、匿名化）
3. 個資外洩通知義務：DI確信發生個資外洩事故應立即通知組織；受公務機關委託+確信發生事故→立即通知且不得無故拖延
組織應透過資料中介機構管理生命週期檢視其委託DI處理個資時所應考量的重要因素
新加坡PDPC「個人資料委託契約條款之參考範本」
A
資料治理及風險評估
■ 建立管理資料中介機構之治理架構
■ 確立組織委外處理個資目標及要求
■ 識別個資處理風險以建立評估機制
■ 確保具備必要管理制度並符合認證
B
資料保護政策與實踐方式
■ 建立清晰溝通管道、定期報告流程
■ 訂立具有約束力書面契約
■ 依據委外範圍建立標準作業程序SOP
DI管理
生命週期
D
委託結束管理
■ 制定退出管理計畫
■ 確保體制保存個資並完成工作紀錄
■ 進行退出查核
C
定期管理與查核
■ 召開啟始會議、制定入職培訓流程
■ 主動監控資料處理情形
■ 定期會議並適當查核
國家發展委員會

「個人資料保護法相關議題」第 6 場產學專家學者諮詢會議—國際傳輸

議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、瑞士「聯邦個人資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及菲律賓「隱私保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於國際傳輸之探討。

貳、議程

一、 主席致詞

二、 報告事項

國際傳輸之探討（國發會）

三、 討論事項

我國有關個資國際傳輸之規定，規範於個資法第 2 條第 6 款「國際傳輸係指將個人資料作跨國（境）之處理或利用。」、第 21 條「非公務機關為國際傳輸個人資料，而有下列情形之一者，中

央目的事業主管機關得限制之：一、涉及國家重大利益。二、國際條約或協定有特別規定。三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。」針對上述規定，蒐整實務見解，並進行比較法之分析。綜觀各國個資保護規範，對於個資國際傳輸概可分為二大方向，一是偏向自由流通立場，如美國係基於資訊自由化及貿易自由的角度，鼓勵資料跨國流通及分享，採取「自由立場」；另一是偏向限制立場，如歐盟、日本、韓國，根據保護當事人隱私權、保障經濟利益及維護資訊主權等理由，主張限制個人資料跨國流通，採取「限制立場」。因應國際貿易頻繁，隨著網路快速發展使個資得輕易進行國際傳輸，故針對國際傳輸應採取之立場及合法要件，提出下列二項案由。

案由一、國際傳輸應採取之立場

說明：

我國依個資法第 2 條第 6 款有關國際傳輸之定義，對於機關內部之資料傳送，或將資料提供當事人以外第三人，若具有將個資作跨國（境）傳輸之客觀條件，不論為資料處理或利用行為，均該當於個資法之國際傳輸。依個資法第 21 條國際傳輸條款規定，中央目的事業主管機關發現有本條所列各款情形之一，應限制非公務機關國際傳輸個人資料者，得視事實狀況，以命令或個別之行政處分限制之。從法條觀之，原則上允許非公務機關進行個資之國際傳輸行為，僅於涉及國家利益、國際條約或協定有特別規定、接受國對於個人資料未有完善之法規及以迂迴方法向第三國（地區）傳輸個人資料規避本法等四種情形時，中央目的事業主管機關得限制之。

參照法務部 102 年 1 月 3 日法律字第 10100226680 號函釋意旨，「法律賦予中央目的事業主管機關，遇有該條所定各款情事之一時，對於人民自由權利限制之依據及裁量權。至於具體個案中央目的事業主管機關是否限制，仍應由主管機關本於權責審認。」復參照法務部 107 年 8 月 21 日法律字第 10703511390 號函釋意旨，「應由主管機關依非公務機關對個資之處理利用情形是否涉有國際傳輸行為，以及資料接受國對於個人資料之保護有無完善法規，本於權責審認。」例如：國家通訊傳播委員會依個資法第 21 條規定，於 101 年以大陸地區之個人資料保護法令尚未完備，限制通訊傳播事業經營者將

所屬用戶之個人資料傳遞至大陸地區(參照國家通訊傳播委員會 101 年 9 月 25 日通傳通訊字第 10141050780 號令)。

綜觀各國法制,由於當個資國際傳輸至外國後,即非其本國法律得規範之範圍,該外國法律究將提供何種程度之保護,亦已非其本國之立法者所得掌握。故國際上多數國家針對國際傳輸規範,已多採「原則限制,例外允許」模式,如歐盟體系僅於資料接收國個資保護水準相當或企業採取適當保護措施、具特定情形,始得例外允許進行國際傳輸。而亞洲國家如日本、韓國、新加坡、菲律賓亦均仿效此立法模式,其中韓國有採互惠主義,即當他國限制傳輸至韓國時,對他國得採相應之限制。而美國強調業者自律方式解決隱私權保護問題,故未針對國際傳輸進行規範,惟積極推動 APEC 跨境隱私保護規則體系(CBPRs),期能建構受信賴的資料自由流通環境,以隱私保護為社會信賴基礎。

有關國際傳輸限制之影響,對於企業可能增加營運成本,配合法規例外允許所要求之條件,甚至可能影響外國企業選擇退出本土市場;惟對於當事人而言,則有利個資被妥善保護,促進當事人對資料持有者之信賴,並作為本國發展資料經濟的重要因素,且亦有利於本土資料處理業者之發展。

小結:請產學專家提供建議,就我國現行國際傳輸採「原則開放,例外限制」模式,對於當事人保護是否足夠?需否參考比較立法例調整?或參考韓國互惠條款限制?如調整是否造成產業發展之阻礙?

案由二、國際傳輸之合法要件

說明:

觀察多數國家對於國際傳輸採取原則限制之立場,僅於符合國際傳輸之合法要件時,始得例外允許為之。經比較各國有關國際傳輸之例外允許模式,主要得區分為接收地之個資保護水準相當、企業提供適當保護措施或具有特定情形。普遍而言,多數國家為併同採行三種模式,並依照各模式有不同程度之要求,如下分別說明:

(一) 接收地之個資保護水準相當

綜觀各國法制，目前歐盟、英國、德國、瑞士、日本、新加坡對於例外允許國際傳輸之合法要件有採納「接收地之個資保護水準相當」。此要件之「相當性」認定條件，以歐盟體系適足性認定而言，須考量：(1) 須有個資保護相關法規，包括共通性與針對特定產業所為之立法；(2) 有無獨立專責監管機關，其具有適當之執法權力，以負責確保個資保護法規落實，並協助當事人行使其權利及提供諮詢，且負責與歐盟會員國之主管機關進行合作；(3) 有無與個資保護相關國際條約、參與之多邊或區域隱私規則體系。另參考日本白名單制度，則須考量：(1) 相關法規足以認定個資法義務得確保於國外履行之；(2) 須具有獨立專責監管機關；(3) 兩國於個資保護方面得相互理解合作；(4)保護個資必要範圍外不限制國際傳輸；(5) 允許有助於日本產業創新實現充滿活力的經濟社會及富裕民生。

有關接收地個資保護水準相當此一要件，概念相近於我國個資法第 21 條第 3 款規定「接受國對於個人資料保護未有完善之法規，致有損當事人權益之虞」。惟此要件屬於不確定法律概念，需依個案具體判斷，如考量有無個資保護相關法規、獨立專責機關、國際承諾等因素。另日本基於此要件允許國際傳輸時，賦予個資保護委員會認為當有必要保護國內個人權益時，仍得附加其他必要條件限制無須經當事人同意即可傳輸個資之範圍。

(二) 企業採取適當保護措施

綜觀各國法制，目前歐盟、英國、德國、瑞士、日本、韓國、新加坡、菲律賓對於例外允許國際傳輸之合法要件有採納「企業自主採用符合規範之適當保護措施」。此要件主要得區分以下類別：

1. 企業自我拘束規則

由企業將本國個資法規定訂於企業內規或章程、公司治理規範，並須經監管機關核定同意。其內容至少應包含：企業結構及聯絡資訊、個資流、內規規範效力、處理個資原則、當事人權利行使、承諾、告知義務、配置個資管理人員及教育訓練、紛爭解決機制、稽核及改善措施、事故通報、監管機關合作。目前歐盟、英國、德國、日本、新加

坡有採納此類型。

2. 標準契約條款

以制式的契約形式將本國個資法關於資料傳輸者與接收者雙方義務訂明，標準契約條款須經監管機關核定同意，或由監管機關訂定。歐盟執委會於 2021 年 6 月公布新版標準契約條款，得採用模組化方式針對控管者與受託處理者之間，因應不同關係選擇所適用之條款。目前有歐盟、英國、德國、瑞士、日本、新加坡、菲律賓採納此類型。

3. 行為守則

由同業公會、各產業團體、學術組織訂定行為守則，為自願性、責任性之法遵工具，作為各產業指標性工具書。行為守則須經監管機關核定同意，其內容至少應包含：處理個資原則、未成年人之資料提供、假名化、當事人權利行使、控管者職責、隱私納入設計、事故通報、國際傳輸、紛爭解決機制等。目前有歐盟、英國、德國採納此類型。

4. 認證

倘企業取得認證，將有助於證明其資料處理活動已遵行個資保護相關規範。認證係採自願申請，並透過透明程序，由第三方進行認證。認證之範圍僅限於流程，如公司內部治理流程及組織流程，並由認證機構或監管機關核發認證標章。有關認證規則應經監管機關核定同意，其內容至少應包含：處理個資原則、當事人權利行使、事故通報、隱私納入設計、資料保護影響評估、安全措施。目前有歐盟、英國、德國、日本、新加坡採納此類型。其中 APEC CBPR 為日本、新加坡所承認之認證制度之一，而韓國、菲律賓亦為 CBPR 會員國，爰亦鼓勵企業取得認證，以提升消費者對跨境資料傳輸的信賴，促進跨國商務發展。

有關企業採取適當保護措施此一要件，歐盟強調仍須配合補充措施，如契約上、技術上及組織上的措施，以確保接收方履行義務，包括適時回報接收地國家個資法規動態，以及個人資料保護程度是否會因法規變化而降低。而日本則強調透明性，因此企業仍需取得當事人事前同意並提供接收方國家個資法制及接收方採取之個資保護措施，並提供相關資訊確保接收

方持續實施。

(三) 具有特定情形

綜觀各國法制，目前歐盟、英國、德國、瑞士、日本、韓國、新加坡對於例外允許國際傳輸之合法要件有採納「因特定情形而得排除國際傳輸限制」。各國規範普遍以類型化方式規範特定情形，如告知當事人並取得明確同意、基於法令、履行契約、保護個人利益、保障公共利益、司法訴訟等。以下針對較多國家所採之類型說明：

1. 告知當事人並取得明確同意

經告知當事人國際傳輸之風險，並事前取得當事人之明確同意，且當事人得隨時撤回同意。目前採納此類型的國家有歐盟、英國、德國、日本、韓國、新加坡。其中韓國另要求須有保障措施，如確保個資處理安全、建立申訴爭議解決機制。

2. 保護個人利益

此利益應限於重大利益且事實上、法律上難以取得當事人同意為必要。目前有歐盟、英國、德國、日本、新加坡採納此類型。其中日本對於個人利益有採生命、身體、財產類型。

3. 保障公共利益

保障公共利益須具有重要性，各國類型化後的公共利益類型有所差異，但多數集中在國家高權、行政相關、公共衛生等類型。目前有歐盟、英國、德國、日本、新加坡採納此類型。

本要件係指於接收地未符合個資保護水準相當或企業未採行適當保護措施時，須符合特定情形，始得為國際傳輸，適用上應從嚴解釋，僅於偶發與非重複性之傳輸始得允許。而特定情形之類型化，仍須採取相應之配套措施，如當事人同意時須課予更嚴格之告知義務及保障措施、保護之個人利益限於重大利益及難以取得當事人同意、保障之公共利益須有重要性。

小結：根據以上觀察，擬請產學專家就以下議題提供建議：

（一） 歐盟體系、日本、新加坡對於國際傳輸例外許可，均有採納接收地之個資保護水準相當要件。倘我國個資法修正，需否納入此一要件，其認定條件為何？或參考日本於必要時仍得附加必要條件限制國際傳輸之範圍？

(二)多數國家均承認當企業提供適當保護措施時得例外允許國際傳輸。倘我國個資法修正，採納此一要件，則應包含哪些類型及相應補充措施？對於產業可能有何影響？

(三)多數國家於接收地國家未符合個資保護水準相當或企業未採行適當保護措施時，於特定情形得例外允許國際傳輸。倘我國個資法修正，採納此一要件，則應包含哪些類型及相應配套措施？對於當事人權利是否足以保護？

國際傳輸

國家發展委員會
111 年 3 月 2 日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（假名化、匿名化）	受託處理者義務	國際傳輸	框架性討論	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2						

2

大綱

一 討論目的及範圍

二 議題分析

三 附件

3

一、討論目的及範圍(1/4)

■ 討論範圍

以「國際傳輸」為主軸，討論應採取之立場及合法要件，有關獨立專責機關置於其他場次討論，並以「個資法」為主要討論範疇。

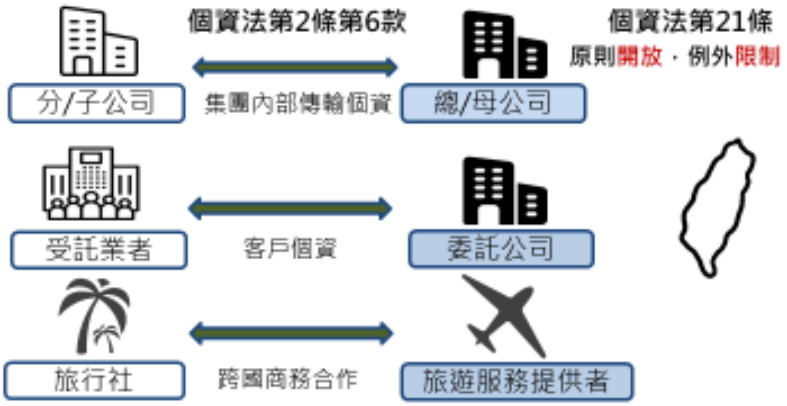
■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
瑞士	聯邦個人資料保護法	2021	GDPR適足性認定（指令時代取得）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2020	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員
菲律賓	隱私保護法	2012	

一、討論目的及範圍(2/4)

4

◆ 國際傳輸在國際貿易之重要性
- 傳統商業營運型態的擴大與升級：人工智慧、物聯網(IoT)、大數據(Big Data)
- 新型態商業模式興起：雲端服務、電子商務



一、討論目的及範圍(3/4)

5

■ 經整理各國有關國際傳輸之規定，得作以下區別：

類型	具體樣態	
原則開放，例外限制		
原則禁止，例外允許	接收地個資保護水準相當	適足性認定
	企業提供適當保護措施	企業自我拘束條款
		標準契約條款
		行為守則
		認證
	特定情形	當事人同意
		基於法令
		履行契約
		保護個人利益
		保障公共利益
		司法相關

一、討論目的及範圍(4/4)

6

- 國際上對於資料跨國流通的基本立場，得概分為：
  - 「自由立場」，基於資訊自由化及貿易自由的角度，鼓勵資料跨國流通及分享，如美國。
  - 「限制立場」，根據保護資料主體隱私權、抵禦文化侵略、保障經濟利益及維護資訊主權等理由，主張限制個人資料跨國流通，如歐盟、日本、韓國、新加坡等。
- 因應國際貿易頻繁，隨著網路快速發展使個資得輕易進行國際傳輸，可能使個資被傳輸至缺乏妥適保護的國家或地區，用以規避內國法規範，故本次會議提出二項案由：
  1. 國際傳輸應採取之立場，應為開放或限制？
  2. 允許國際傳輸之合法要件，多數國家有採資料接收地個資水準相當、企業提供適當保護措施、特定情形時得排除限制，倘我國個資法修正，應採納何種類型及相應配套措施？

大綱

7

一 討論目的及範圍
二 議題分析
三 附件

(一)我國個資法相關規定 (1/2)

8

■ 我國現行規定

個人資料保護法

第2條第6款

國際傳輸：指將個人資料作跨國（境）之處理或利用。

第21條

非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

一、涉及國家重大利益。

二、國際條約或協定有特別規定。

三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。

國家發展委員會

(一)我國個資法相關規定 (2/2)

9

■ 函釋見解

- 法律賦予中央目的事業主管機關，遇有該條所定各款情事之一時，對於人民自由權利限制之依據及裁量權。至於具體個案中央目的事業主管機關是否限制，仍應由主管機關本於權責審認。（法務部102年1月3日法律字第10100226680號函釋）
- 應由主管機關依非公務機關對個資之處理利用情形是否涉有國際傳輸行為，以及資料接受國對於個人資料之保護有無完善法規，本於權責審認。（法務部107年8月21日法律字第10703511390號函釋）

■ 目前依個資法第21條限制國際傳輸之情形

NCC 國家通訊傳播委員會

101年以大陸地區之個人資料保護法令尚未完備，限制通訊傳播事業經營者將所屬用戶之個人資料傳遞至大陸地區（通傳通訊字第10141050780號令）。

→依個資法第21條第3款「**接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞**」

國家發展委員會

議題一：國際傳輸應採取之立場(1/3)

10

■ 國際立法例比較

	原則	例外
我國	開放	限制
歐盟	禁止	允許
德國	禁止	允許
英國	禁止	允許
瑞士	禁止	允許
美國	開放（未規範）	
日本	禁止	允許
韓國	禁止	允許（依**互惠主義**得採他國相應之限制）
新加坡	禁止	允許
菲律賓	禁止	允許

歐盟體系

- 考量資料接收國**個資保護水準**落差，如個資得輕易傳輸至保護不足之他國，造成當事人損害則難以提供適當保護。故對國際傳輸採「**原則禁止，例外允許**」之模式。日本、韓國、新加坡、菲律賓均仿效此立法模式。

美國體系

- 強調**業者自律**方式解決隱私權保護，故未針對國際傳輸規範，惟積極推動APEC跨境隱私保護規則體系（CBPRs）。

國家發展委員會

議題一：國際傳輸應採取之立場(2/3)

11

□ 限制國際傳輸之影響

1 政府治理

正：強化國家對資料流向的掌控能力，有助於強化資料主權。
負：無論採行適足性認定（對其他國家）或適當保護措施（對企業），均增加行政負擔。

2 個資保護

正：避免因跨境流動而降低個資保護程度，有助當事人個資保護

3 產業發展

正：適當限制可能引導業者尋求在地資料處理/受託業者，有助本土資料處理業者發展
負：國際傳輸規範增加業者成本，可能調整營運型態或退出市場。

國家發展委員會

12

議題一：國際傳輸應採取之立場(3/3)

Q

我國對國際傳輸採「原則開放，例外限制」模式，對於當事人保護是否足夠？

需否參考比較立法例調整？或參考韓國互惠條款限制？如調整是否造成產業發展之阻礙？

13

議題二：國際傳輸之合法要件 (1/11)

- 比較各國法制，國際傳輸之**例外許可**模式，得區分為**個資保護水準相當**及**適當保護措施**、**特定情形**。
- 普遍而言，多數國家三種模式均有採行。

	接收地之個資保護水準相當	企業提供適當保護措施	特定情形
歐盟	○	○	○
英國	○	○	○
德國	○	○	○
瑞士	○	○	○
美國		未規範	
日本	○	○	○
韓國		○	○
新加坡	○	○	○
菲律賓		○	

議題二：國際傳輸之合法要件 (2/11)

14

主要國家國際傳輸規範

歐盟-適足性認定

由執委會認定接收國資料保護程度是否符合適當保護水準，須確保接收國提供之保護水準為「本質相當於歐盟之保護」，且接收國應提供資料有效與可執行之權利及方式。

日本-白名單

類似歐盟之適足性認定，由個人資料保護委員會將特定國家列入白名單。

新加坡-確保資料接收方提供與PDPA相當之保護標準

非經PDPC核准豁免國際傳輸限制，須具備法律效力之義務要求

韓國-國際傳輸規定

國際傳輸不得締結違背PIPA之契約，並應取得當事人同意及履行告知義務

國家發展委員會

議題二：國際傳輸之合法要件 (3/11)

15

1. 接收地之個資保護水準相當

	接收地之個資保護水準相當
歐盟	○
英國	○
德國	○
瑞士	○
美國	未規範
日本	○
韓國	
新加坡	○
菲律賓	

- 概念相近於我國個資法第21條第3款規定「**接受國對於個人資料保護未有完善之法規**，致有損當事人權益之虞」。
- 考量因素包括有無**相關法規**、**獨立專責機關**、**國際承諾**等。
- 日本賦予監管機關仍得於**必要時附加必要條件**限制個資國際傳輸之範圍。
- 韓國未採納此要件，強調應由企業取得當事人同意始得為之。

國家發展委員會

16

議題二：國際傳輸之合法要件 (4/11)

1. 接收地之個資保護水準相當 (續)

1

比較各國法制，歐盟體系、日本、新加坡對於國際傳輸例外許可，均有採納接收地之個資保護水準相當要件。倘我國個資法修正，需否納入此一要件，其認定條件為何？又需否參考日本於必要時仍得附加必要條件限制國際傳輸之範圍？

17

議題二：國際傳輸之合法要件 (5/11)

2. 適當保護措施

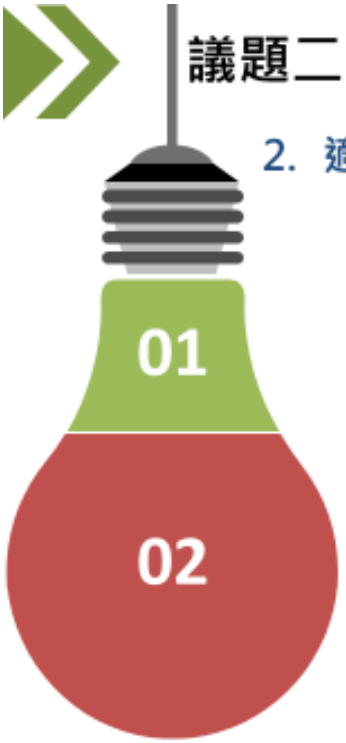
適當保護措施 / 國別	企業自我拘束條款	標準契約條款	行為守則	認證	其他
歐盟	○	○	○	○	
英國	○	○	○	○	
德國	○	○	○	○	
瑞士		○			
美國				△（CBPR）	
日本	○	○		○（CBPR）	
韓國	○			△（CBPR）	
新加坡	○	○		○（CBPR、PRP）	法律規定、具法律拘束之文件
菲律賓		○		△（CBPR）	指定管理人員並公告揭露

△：未明文規定

議題二：國際傳輸之合法要件 (6/11)

18

2. 適當保護措施 (續)



企業自我拘束條款*

1)將本國個資法訂於企業內規或章程，或公司治理
2)須經監管機關核定同意
3)內容至少應包含：企業結構及聯絡資訊、個資流、內部規範效力、處理個資原則、當事人權利行使、承諾、告知義務、配置個資管理人員及教育訓練、紛爭解決機制、稽核及改善措施、事故通報、監管機關合作

*歐、英、德、日、新

標準契約條款*

1)將本國個資法規定以制式的契約形式規範雙方
2)須由監管機關訂定，或經其核定同意
3)歐盟執委會於2021年6月4日公布新版標準契約條款，採用模組化方式處理不同關係所適用之條款

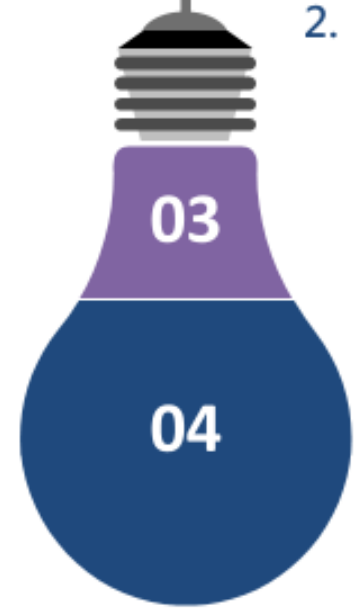
*歐、英、德、瑞、日、新、菲

國家發展委員會

議題二：國際傳輸之合法要件 (7/11)

19

2. 適當保護措施 (續)



行為守則*

1)自願性、責任性之法遵工具，為各產業指標性工具書
2)須經監管機關核定同意
3)內容應包含但不限於：處理個資原則、未成年人之資料提供、假名化、當事人權利行使、控管者職責、隱私納入設計、事故通報、國際傳輸、紛爭解決機制。

*歐、英、德

認證*

1)由第三方認證
2)認證規則應經監管機關核定同意
3)認證標章應由認證機構或監管機關核發
4)認證範圍限於流程，如公司內部治理流程及組織流程
5)認證規則內容應包含：處理個資原則、當事人權利行使、事故通報、隱私納入設計、資料保護影響評估、安全措施

*歐、英、德、日、新

國家發展委員會

議題二：國際傳輸之合法要件 (8/11)

20

2. 適當保護措施 (續)

- 歐盟強調適當保護措施必須配合補充措施，確保接收方履行義務，包括適時回報接收地國家個資法規動態，以及個人資料保護程度是否會因法規變化而降低。

- 日本強調透明性，企業採行適當保護措施仍需取得當事人事前同意並提供當事人有關接收方國家個資法制及接收方採取個資保護措施，且後續應持續提供相關資訊確保接收方實施。

2

比較各國法制，多數國家均承認當企業提供適當保護措施時得例外允許國際傳輸。倘我國個資法修正，是否需採納此一要件，應包含哪些類型及相應補充措施？對於產業可能有何影響？

國家發展委員會

議題二：國際傳輸之合法要件 (9/11)

21

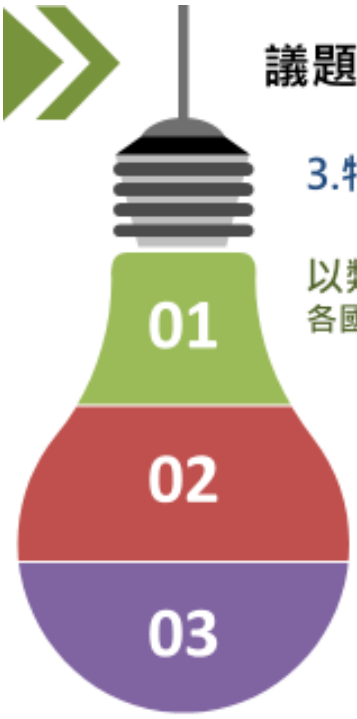
3.特定情形

特定情形 / 國別	告知+同意	基於法令	履行契約	保護個人利益	保障公共利益	司法相關	其他
歐盟	○（風險）		○（終止）	○（重大利益且法律上本人難同意）	○（重要）	○（訴訟、司法調查）	歐盟會員國立法授權公開資訊
英國							國家授權公開資訊
德國							公務機關執行職務必要+處理合法事由
瑞士							簽署國際法條約、特定事業主管機關制定具體保障當事人之措施
美國							
日本	○	○（法令、法定事務）		○（生命、身體、財產必要且難取得同意）	○（公衛、兒童發展必要且難取得同意）		
韓國	○（安全措施+申訴機制）						
新加坡	○		○	○（重要）	○（重要）		傳輸中資料、公開資料
菲律賓							

議題二：國際傳輸之合法要件 (10/11)

22

3.特定情形 (續)



以類型化為主
各國普遍以類型化方式規範特定情形。

當事人同意*
1)告知義務 - 使當事人明確瞭解國際傳輸之風險
2)取得同意 - 事前性、明確性、得隨時撤回
3)韓國要求保障措施，確保個資處理安全、建立申訴爭議解決機制
*歐、英、德、日、韓、新

保護個人利益或保障公共重要利益*
1)個人利益須重大，且難以取得本人同意為限
2)公共利益須重要，各國類型化後的公共利益類型有所差異，但多數集中在國家高權、行政相關、公共衛生等類型。
*歐、英、德、日、新

國家發展委員會

議題二：國際傳輸之合法要件 (11/11)

23

3.特定情形 (續)

- 於接收地未符合個資保護水準相當或企業未採行適當保護措施時，須符合特定情形，始得為國際傳輸，適用上應從嚴解釋，僅於偶發與非重複性之傳輸所允許。

- 特定情形類型化，其配套措施如當事人同意時須課予更嚴格之告知義務及保障措施、保護個人限於重大利益及難取得本人同意、保障公共利益須有重要性。

3

比較各國法制，多數國家採納當有特定情形時，得允許國際傳輸。倘我國個資法修正，採納此一要件，則應包含哪些類型及相應配套措施？對於當事人權利是否足以保護？

國家發展委員會

24

議題討論

案由一：國際傳輸應採取之立場

- 我國對國際傳輸採「原則開放，例外限制」模式，對於當事人保護是否足夠？需否參考比較立法例調整？或參考韓國互惠條款限制？如調整是否造成產業發展之阻礙？

案由二：國際傳輸之合法要件

- 歐盟體系、日本、新加坡對於國際傳輸例外許可，均有採納接收地國家之個資保護水準相當要件。倘我國個資法修正，需否納入此一要件，其認定條件為何？又需否參考日本於必要時仍得附加必要條件限制國際傳輸之範圍？
- 多數國家均承認當企業提供適當保護措施時得例外允許國際傳輸。倘我國個資法修正，採納此一要件，則應包含哪些類型及相應補充措施？對於產業可能有何影響？
- 多數國家於接收地國家未符合個資保護水準相當或企業未採行適當保護措施時，於特定情形得例外允許國際傳輸。倘我國個資法修正，採納此一要件，則應包含哪些類型及相應配套措施？對於當事人權利是否足以保護？

25

大綱

一 討論目的及範圍

二 議題分析

三 附件

26

歐盟相關規定

最近一次個資法修正：2016年（2018年施行）

國際傳輸定義及要件：
1. 依GDPR第3條第2項規定，情形適用GDPR
2. 由資料控管者或受託處理者提供給另一位資料控管者或受託處理者
3. 資料接收方實際位於第三國或是國際組織

原則禁止，例外允許

例外	一	二	三
	適足性認定	**適當保護措施+補充措施**	**例外條款**
	• 適足性認定考量要件：民主法治精神、人權與基本權力之尊重、第三國之個人資料保護法規體系、獨立個資監管機關等 • 取得適足性認定的國家：阿根廷、加拿大、以色列、紐西蘭、瑞士、日本、英國、韓國	• 標準契約條款（合約）：歐盟執委員會版本或監管機關自訂 • 企業自我拘束規則（跨國企業公司內規） • 行為守則+契約（業界常規） • 驗證+契約（第三方驗證）：驗證機構可是監管機關或是一般民營驗證機構；驗證規則須經監管機關及EDPB審查	• 明確同意 • 契約必要 • 重要公共利益必要 • 訴訟必要 • 保護生命利益必要 • 經立法授權之公眾諮詢系統清單 • 重大合法利益必要

27

英國相關規定

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國，GDPR適足性認定（2021）

原則禁止，例外允許

例外	一	二	三
	適足性認定 UK GDPR §45	**適當保護措施+補充措施 UK GDPR §46、47**	**例外條款 UK GDPR §49**
	基於適足性之情形而將個人資料傳輸到第三國或國際組織，此類轉讓無需任何特定授權。 （見 DPA 2018第17A條）	• 標準契約條款 • 企業自我拘束條款 • 行為守則 • 驗證 （見 DPA 2018第17B、17C、119A條）	• 明確同意 • 契約必要 • 重要公共利益 • 訴訟必要 • 保護生命利益 • 登記冊 （見 DPA 2018第18條）

UK GDPR §50　針對第三國和國際組織，ICO應採取適當措施

• 制定國際合作機制	• 立法提供國際互助	• 利害關係人討論、活動	• 立法交流紀錄、文件，包含第三國管轄

德國相關規定

28

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

一般性規定

傳輸機關	傳輸對象	合法要件		其他要求
		一般個資	特種個資	
公務機關	公務機關	履行職務之必要+合法事由(§23)	各自之前提要件(左邊)+GDPR §9 II合法事由/ BDSG §22合法事由+安排適當且具體之措施	僅能就特定目的內處理，目的外利用應具備合法事由(§23)
	非公務機關	須具備合法事由(§25 II)		僅能就特定目的內處理，目的外利用須具備合法事由(§25)+傳輸機關之同意
非公務機關	須符合GDPR §44-50之要求規定			

國家發展委員會

瑞士相關規定

29

最近一次個資法修正：2020年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

定義	• 瑞士《2020年聯邦資料保護法》（DSG 2020）規定的「披露」（Bekanntgeben個人資料行為包含：「傳輸個人資料」和「提供個人資料」 • 瑞士最高行政機關「聯邦委員會」（Bundesrat）針對個人資料國際傳輸行為，具有事前審查的權力

管理規定	• 瑞士聯邦委員會針對「在國外披露個人資料行為」的事前審查，將審查是否具備以下項目之一
	  • 目標國家或國際組織是否和瑞士簽署國際法定義上的條約
	  • 個人資料控制者或個人資料處理者，與位在目標國家或國際組織的合作對象，是否已簽署經「聯邦資料保護及資訊專員」（Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, EDÖB）確認的個人資料保護協議
	  • 特定事業的瑞士聯邦主管機關是否針對個人資料國際傳輸行為，制訂具體保障個人資料當事人權利的措施，並經EDÖB確認
	  • EDÖB是否針對個人資料國際傳輸行為，事先批准並發布個人資料保護協議範本
	  • 目標國家或國際組織的個人資料主管機關是否提出說明，其個人資料保護規範與瑞士DSG 2020具備同等保護效力

國家發展委員會

30

美國相關規定(1/2)

無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

CBPRs 採 APEC 隱私權保護綱領九大隱私原則	內容
(1)預防損害原則（Preventing Harm）	• 認同個人對於隱私的合理期待之利益，認知到濫用個人資料而可能造成損害的風險，對此應承擔特定的義務，並應根據蒐集、利用和轉移個人資料所造成的損害的可能性和嚴重性，採取適當的補救措施。
(2)告知原則（Notice）	• 個人資料的控管者應就個人資料的實務和政策提供清晰、易於近用之聲明。
(3)蒐集限制（Collection Limitation）	• 個人資料之蒐集應限於與蒐集目的有關的範圍，依合法或正當方法為之，並在適當的情況下告知當事人或取得其同意。
(4)個人資料之利用（Uses of Personal Information）	• 除取得當事人本人同意、為提供當事人所要求之產品或服務所必要者、或法律或其他法定文件明文規定者，個人資料的利用僅限於與蒐集目的相同或有關的範圍內。

美國對於個人資料之國際傳輸並未有相關限制，惟其積極推動亞太經合會跨境隱私保護規則體系APEC CBPRs，促進亞太區域資料跨境傳輸與數位經濟之發展。

31

美國相關規定(2/2)

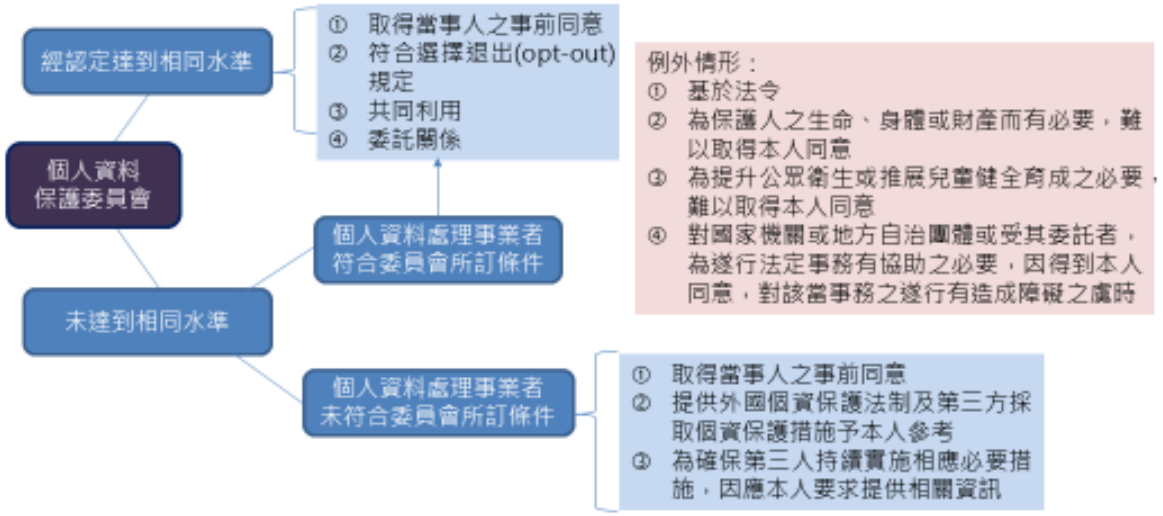
無聯邦個資法，加州消費者隱私法最近修正為 2018年；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

九大隱私原則（續）	內容
(5)當事人自主（Choice）	• 情況允許時，個人資料控管者應提供當事人可就其個人資料之蒐集、利用及揭露選擇之機會，該選擇機會必須清晰、易懂、可近用及可負擔。如資料已為為公開可得的資料時，本規定不適用。
(6)個人資料完整性（Integrity of Personal Information）	• 個人資料應正確、完整並依其用途為必要更新。
(7)安全管理（Security Safeguards）	• 個人資料管理者應妥善的保護個人資料的安全，如防止未經授權的不當截取、利用、修改或揭露個人資料或濫用個人資料之行為。個人資料管理者所採取的保護措施應與發生個人資料濫用的機率及可能造成損害、個人資料的敏感度和內容成比例，並應定期檢視及重新評估保護措施。
(8)近用、更正（Access and Correction）	• 當事人應可自個人資料管理者取得關於其是否持有當事人個人資料的資訊；且在提供足以進行識別的個人資料後，當事人應可和個人資料管理者在合理期間內以合理、一般可得理解之方式取得其個人資料，如有收費不得過高；當事人應可挑戰關於其個人資料的正確性，並合適及可能的情況下，更正、補充或請求刪除該筆資料。
(9)問責（Accountability）	• 個人資料管理者應負責確保上列的原則之實踐。於傳遞個人資料於第三人時，無論是否為跨境傳輸，個人資料管理者皆應取得個人的同意，或必須盡力確保該第三人會採取和此一隱私保護綱領一致的措施以保護個人資訊隱私之安全。

32

日本相關規定

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）



33

韓國相關規定(1/2)

最近一次個資法修正：2020年
CBPR成員國、GDPR適足性（2021）

- 韓國於2021年12月17日，歐洲個人資料保護委員會（European Data Protection Board, EDPB）通過韓國個人資料保護適足性認定之意見，採「原則禁止、例外允許」的模式。

PIPA增訂條文：

- 資通訊服務提供者不得以違反PIPA的內容締約
- 提高違法規範之裁罰金額
- 須取得同意、履行告知義務及具備適當安全維護措施（施行細則第48條之10）
  - 符合施行細則第48-2條規定
  - 具備處理個資爭議解決
  - 保護個資所需的其他措施

排除適用：

- 排除宗教活動、政黨提名候選人所處理個人資料及金融機構信用資料傳輸
- 金融機構仍需透過標準契約條款（SCC）進行個人信用資料的國際傳輸
- 僅涉及歐盟人民個人資料移轉至韓國國內，而無韓國人民個資移轉至歐盟

34

韓國相關規定(2/2)

國際傳輸的限制範圍

應達成第39條之12各款的要求，始可例外傳輸	內容
	• 資通訊服務提供者等，就有關使用者個人資料部分，不得以與PIPA相違背之內容締結國際契約
	• 資通訊服務提供者等如欲對外提供、委託處理、傳輸個人資料，應依第17條第3項取得個資當事人同意；但若該項各款應告知事由皆已依施行細則規定公告周知或由電子郵件向個資當事人告知，則得例外不取得同意
	• 資通訊服務提供者如欲取得個資當事人同意，應事先將下列各款事項全部告知使用者： （1） 移轉個資項目 （2） 個資轉入國家、移轉時間暨方法 （3） 個資移轉接收者之姓名（或法人名稱及個資管理者聯繫方式） （4） 個資移轉接收者對個資利用目的及保有利用的期間
	• 資通訊服務提供者依照第二項本文取得同意並將個資移轉至國外時，應依照PIPA施行細則採行適當安全維護措施
第39條之13互惠原則	• 對於限制個資向國外轉移之國家的資通訊服務提供者，得依該國標準為相應之限制，但履行條約或其他國際協定所必要，則例外不在此限

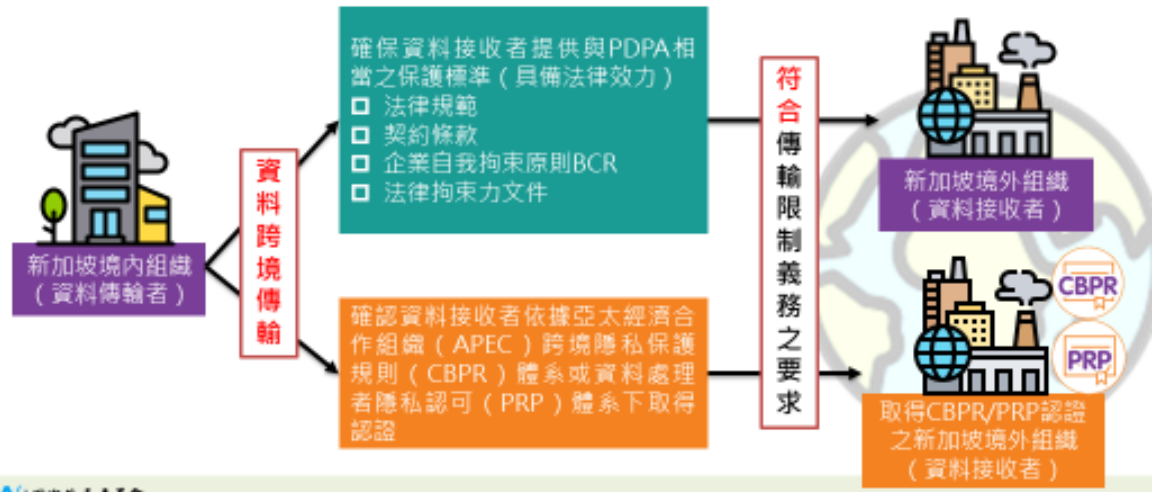
國家發展委員會

35

新加坡相關規定

最近一次個資法修正：2020年
CBPR成員國

PDPA第26條：傳輸限制義務（Transfer Limitation Obligation）
- 原則禁止：不得將任何個人資料傳輸到新加坡以外之國家或地區
- 例外允許：確保個人資料將受到法律強制義務所保護→具備法律效力、取得CBPR/PRP認證



國家發展委員會

菲律賓相關規定

最近一次個資法修正：2012年（2017年、2019年分別提出修正案，尚未完成立法程序）

定義	• 《資料隱私法》未特別規定國際傳輸「原則允許、例外禁止」或是「原則禁止、例外允許」，而是要求進行個人資料傳輸（無論國內傳輸或國際傳輸）的個人資料控制者（Personal Information Controller, PIC），均要遵守《資料隱私法》等相關法規關於PIC的規定

管理規定	• 《資料隱私法》要求：PIC國際傳輸個人資料給第三方時，PIC需落實以下二點：
	  • 「符合DPA 2012規定的保護標準的合理手段」（如與第三方簽訂個人資料保護協議或個人資料共享協議（Data Sharing Agreement, DSA））
	  • 「指定一名或多名可以確認第三方有確實遵守DPA 2012規定的人員」
	• 個人資料保護安全的合理手段例示如下：
	  • 簽署DSA的各方，都需要採取包含組織、物理和技術的安全措施
	  • 簽署DSA的各方，都需要建立「個人資料事故發生時的應變與管理程序」

國家發展委員會

黑字：《資料隱私法》《資料隱私法施行細則》規定內容
藍字：菲律賓國家隱私委員會諮詢意見（具有拘束效力）

「個人資料保護法相關議題」第 7 場產學專家學者諮詢會議—規範主體、行為區分與特定目的之解釋議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」及新加坡「個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於個資法共通性規範模式之探討。

貳、議程

一、 主席致詞

二、 報告事項

規範主體、行為區分與特定目的之解釋探討(國發會)

三、 討論事項

歸納歷次專家諮詢會議意見，對於具共通性之個資保護規範模式，包含規範主體區分為公務/非公務機關、規範行為區分為蒐集/處理/利用之分類方法，以及特定目的之解釋方式等議題，蒐整實務相關函釋見解，進行比較法之分析，並研提討論事項如下：

案由一、規範主體之分類

說明：

我國個資法將受規範之主體依照其組織性質區分為公務機關及非公務機關。依照個資法第 2 條第 7 款及第 8 款之規定，公務機關指依法行使公權力之中央或地方機關或行政法人；非公務機關則為公務機關以外之自然人、法人或其他團體。我國個資法除了在特種個資之蒐集、處理、利用合法要件上，將公務、非公務機關為同一規範外，整體個資法架構，係以公務機關、非公務機關作為區分，分別於第二章及第三章規範不同適用項目。

然而，目前公務機關、非公務機關分別規範之模式，實務上除產生同類機關適用不同規範之疑義外(如公私立醫院、公私立學校等)，部分機關亦因無法明確區分屬公務或非公務機關，而須仰賴法律解釋機關或主管機關針對特定組織函釋釐清(如：法務部 101 年 11 月 21 日法律字第 10103109040 號、法務部 101 年 11 月 21 日法律字第 10100113630 號、內政部 102 年 1 月 29 日台內民字第 10200892752 號、法務部 102 年 4 月 3 日法律字第 10203502560 號及法務部 104 年 1 月 30 日法律字第 10403500490 號等，分別針對公私立學校、農會、寺廟、農田水利會及醫院等性質特別進行解釋)。

從國際比較立法例觀察，目前除美國及新加坡個資法規範本就排除公務機關適用外，各國並無明顯的規範選擇偏好，而採取了不同的立法模式。其中歐盟、英國、韓國於章節架構及個資運用合法要件上並未區分公務、非公務機關，僅有部分條文為特別規定；而現行之德國法亦未於章節架構上區分公務機關及非公務機關，但於個資運用的合法要件上，特別加以區分，並規定公務機關之私法行為適用非公務機關之規定；日本則與我國相同，依照組織型態的不同，於個資運用合法要件及章節架構上，分別以公務及非公務機關加以規定。從立法歷程觀察，我國電腦處理個人資料保護法立法時係參考當時有效之德國法，採取公務機關、非公務機關分別訂定不同個資運用要件、並以不同章節分別管理的模式，而德國已於 2017 年時，配合歐盟 GDPR 的立法，調整法律章節結構，僅於個資運用合法要件上，保留公務、非公務機關的區分方式。

在章節結構安排上，日本係將資料運用合法要件、組織責任、當事人權利等，皆以「公務、非公務機關」的區分模式，依照組織性質分別放在不同章節規範。這或許跟日本原先採取個人情報保護法、行政機關保有個人情報保護法分別立法的模式有關，雖近年已將兩者併為同一部個資法，但「公務、非公務機關」區分規範模式仍未改變。而歐盟則與日本相反，完全依照規範之性質，將個資保護與管理事項分成基本原則、當事人權利、組織責任（控管者與處理者、國際傳輸）等，分別以不同章節規定。我國則介於其中，部分相同事項（如當事人權利、個資保護基本原則等）於總則規定，個資運用合法要件以及安全維護事項等，則分別於第二章及第三章規範公務機關及非公務機關應遵循之規範。

從立法模式而論，區分公務機關、非公務機關的立法模式，其假設公務與非公務機關性質有別，應以不同規範規定；而不區分兩者的立法模式，則認為個資運用與管理之基礎原則相通，因此以同一規定處理為原則，僅於例外部分為特別規定。前者理論上可依機關性質量身打造適合的規範，但立法上須避免掛一漏萬而造成適用困難；後者則雖然大多數要件可一體適用，較不易有涵蓋不足問題，但立法時需以「原則-例外」方式設定要件。總體而論，尚無明顯之優、劣。

小結：請產學專家學者就以下議題提供建議：

1. 我國公務、非公務機關有關個資運用之合法要件，（除依法定職權外）是否有必須分別規定之處？

2. 我國個資運用合法要件若不採公務、非公務機關分別規定的規範模式，能否減少適用上困擾？

3. 若個資運用合法要件仍區分公務、非公務機關，公務機關於私法關係上，是否得參酌德國法，適用非公務機關規定？

4. 若有調整規範主體之必要，則整體章節結構應如何規劃較為妥適？或是否可於不變動現有結構下進行調整？

案由二、規範行為之分類

說明：

我國個資法目前將個人資料之運用，分為蒐集、處理、利用三種不同樣態。其中，蒐集指以任何方式取得個人資料；處理指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送；利用指將蒐集之個人資料為處理以外之使用。而在個資運用的合法要件上，除特種個資並未區分蒐集、處理、利用規範不同合法要件外，在一般個資上則是採取分別規範的模式，蒐集、處理適用個資法第 15 條、第 19 條中合法要件之規定；利用則於第 16 條、第 20 條規範合法要件。

然而，隨著技術之發展，處理及利用在今日的資料運用上已經很難區分，容易衍生後續法規適用上之疑義。以機器學習為例，其演算法之運算，就可能同時涵蓋上述處理定義中所列的編輯、複製、檢索、連結等行為，亦可能有未能於上述定義涵蓋的其他被歸類為「利用」的行為。若將演算過程區分為處理、利用行為，在法律適用上會較為複雜。

從國際立法例觀察，按照運用行為區分個資運用合法性要件者多為亞洲國家，如我國、日本、韓國及新加坡；而未以運用行為區分的，則以歐美國家為主，包含歐盟、英國、德國及美國。我國在電腦處理個人資料保護法立法時，係參考德國當時有效的德國聯邦個人資料保護法，將個人資料運用分為蒐集、處理及利用這三個不同型態，惟德國在合法性要件上則是分別規定蒐集之合法要件及「處理、利用」之合法要件；而德國在 2017 年修法時，已配合 GDPR 規定不再區分個資運用的行為樣態，皆以「處理」規範之。日本、韓國及新加坡雖區分個資運用行為，惟其規定是將「提供（第三人）」的行為與其他處理樣態分開，形成「（蒐集）、處理、提供」的規範模式，與我國規範模式仍有差異。而「蒐集」涉及資料之取得，「提供」涉及資料控制權限之轉移，其風險型態確實與其他的處理程序有別。

小結：請產學專家學者就以下議題提供建議：

1. 我國現行「蒐集、處理、利用」的區分方式，對於實務適用上是否有所不便？是否有改變需要？

2. 若如歐、美等國改採不區分運用型態的合法性要件規範模式，是否有不妥之處？

3. 若仍採取區分模式，如參考日、韓、新模式，僅針對蒐集、提供等風險性質不同之運用型態另做規範，是否恰當？於實務運用上是否有難以執行之處？

案由三、特定目的之解釋方式

說明：

我國目前在（一般）個人資料之運用上，係要求個人資料蒐集時，需確定個資蒐集之目的（即「特定目的」），後續的處理、利用行為原則上需於蒐集的特定目的範圍內進行，並針對原蒐集之特定目的外之利用行為，定有目的外利用之合法性要件。比較法上，歐盟則要求若其他利用行為之目的，與原先之蒐集目的不一致時，須取得當事人之同意或會員國依照 GDPR 授權之特別法規定，方可為個資處理；否則須通過「相容性檢驗」（compatibility test），確保進階處理（further process）的目的與蒐集的目的相容。此種相容性檢驗，須考量以下因素：蒐集目的與進階處理目的間之連結（link）、蒐集之脈絡（context，尤其是當事人與控管者間關係）、資料本身之性質（例如是否為特種個資）、進階處理對當事人可能之後果、所採取之適當保護措施。

簡言之，歐盟將進階處理行為分成三種不同型態：

一、 若新目的與蒐集目的不相容，則須取得當事人同意或有會員國的特別立法始得合法進行，此與我國特定目的外利用之型態較為類似。

二、 若進階處理之特定目的與原蒐集目的完全相同，則可直接利用。

三、若不完全相同，則須以相容性檢驗確認二者目的相容。

此種相容性檢驗的要求，我國個資法及施行細則雖無相同規定，但函釋曾援引相似概念，要求處理、利用行為之特定目的須與蒐集之法定事由具有「正當合理關聯」以「合乎社會通念下當事人對隱私權之合理期待」。（法務部 98 年 1 月 8 日法律字第 0970038035 號函、法務部 102 年 7 月 5 日法律字第 10203507340 號函參照）

這種相容性檢驗的規範模式，各有優勢及劣勢：

一、 其優勢在於可以強化個資保護程度。因為若可以「相容性檢驗」的方式，將類似但不完全相同的運用目的包含在原蒐集之特定目的範圍內，則可避免控管者擔心資料利用受限，而主張較為寬泛的蒐集目的，反而讓當事人不易預見資料可能被處理的樣態。且相容性檢驗這種考量處理行為之脈絡、影響的作法，似乎可以取代「有利於當事人權益」等要件，要求控管者在進行與原始蒐集目的不同之處理行為時，考量脈絡、影響等因素，以強化對當事人個資安全之要求。

二、 其劣勢在於相容性檢驗的複雜性也可能造成執行上的困難。質言之，相容性檢驗判斷過程須考量眾多不確定因素且難度高，對控管者而言，可能增加法遵風險；對當事人而言，也增加確認處理行為合法性的困難度。

小結：請產學專家學者就以下議題提供建議：

1. 歐盟的相容性檢驗模式，是否有助於強化個資保護程度？（如有利於要求蒐集目的之明確性、有助於當事人預見資料處理範圍等）

2. 相容性概念之操作，對非公務機關執行上是否有困難？

3. 目前依函釋引入「合理關聯」要求作法是否足夠？有無進一步以法律明文規範之必要？

規範主體、行為區分與特定目的之解釋

國家發展委員會
111年4月6日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	**規範主體、行為區分與特定目的之解釋**	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6					

2

大綱

一 討論範圍

二 規範主體之分類

三 規範行為之分類

四 特定目的之解釋方式

3

一、討論範圍（1/2）

- 討論範圍
  - ◆歸納歷次專家諮詢會議蒐集意見中，對於個資保護規範內具有共通性之規範模式，包含公務/非公務機關的規範主體區分模式；規範行為的分類方法；及特定目的解釋方式等，有關個案規範或個資主管機關規範模式，則於其餘場次討論。
- 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法（令和3年法37號修訂版）	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員

4

一、討論範圍（2/2）

① 規範主體之分類

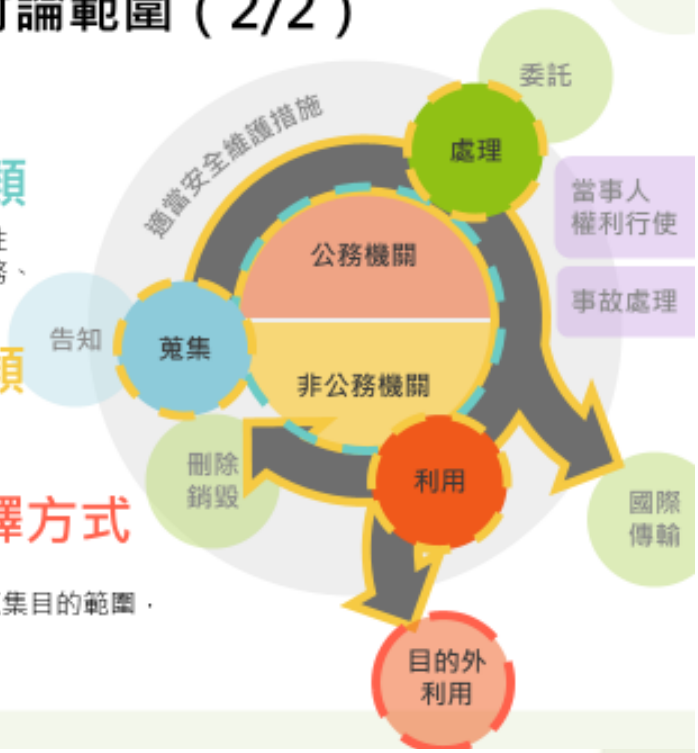
對於蒐集、處理、利用合法性要件之規定，是否須採取公務、非公務機關之分類

② 規範行為之分類

應將對個資採取的行為，分為哪些種類加以規範？

③ 特定目的之解釋方式

歐盟以「相容性檢驗」判斷進階處理之目的是否屬於原蒐集目的範圍，是否有參酌可能？



5

大綱

一 討論範圍

二 規範主體之分類

三 規範行為之分類

四 特定目的之解釋方式

二、規範主體之分類
（一）我國個資法相關規定（1/3）

6

● 個資法按照 **組織性質** 區分公務、非公務機關

個人資料保護法
第2條第7款、第8款 七、公務機關：指依法行使公權力之中央或地方機關或行政法人。 八、非公務機關：指前款以外之自然人、法人或其他團體。

● 實務上由於公務、非公務機關適用法律不同，法律解釋機關或主管機關已針對特定組織屬於公務或非公務機關**數次做出函釋**，如

函釋字號	解釋重點
法務部101年11月21日法律字第10103109040號	**公立學校**為個資法公務機關； **私立學校**為個資法非公務機關
法務部101年11月21日法律字第10100113630號	**農會**為個資法非公務機關
內政部102年1月29日台內民字第10200892752號	**寺廟**為個資法非公務機關
法務部102年4月3日法律字第10203502560號	**農田水利會**為個資法公務機關
法務部104年1月30日法律字第10403500490號	**公立醫院**為個資法公務機關

國家發展委員會

二、規範主體之分類
（一）我國個資法相關規定（2/3）

7

● 我國個資運用合法要件上採 **公務、非公務機關 分別規定**；個資法章節安排上，除當事人權利、個資基本原則、告知規定、特種個資運用等外，亦分兩章節規定。

● 公務機關、非公務機關兩章，除共通有個資運用合法要件、安全維護要求規定外，分別針對公務機關、非公務機關行政管理及蒐集個資公告等事項分別規定。

總則	立法目的、定義、當事人權利、委託、基本原則、特種資料、告知、事故通知
公務機關	合法要件（15、16）、安全維護（18）、公開供查閱事項（17）
非公務機關	合法要件（19、20）、安全維護（27）、行政檢查（22-24、26）、糾正措施（25）
損害賠償及團體訴訟	
罰則	
附則	

國家發展委員會

二、規範主體之分類
（一）我國個資法相關規定（3/3）

8

- 公務、非公務機關區分規範適用上的情況
  - 同類機關因組織法差異，適用不同規範
    - 例：私立學校適用非公務機關規定，行銷時有特殊規定；公立學校適用公務機關規定，無行銷特殊規定。
  - 公務機關亦可能有私法行為
    - 例：公務機關可能與私人有契約或類似契約關係，但公務機關卻無此蒐集、處理及利用當事人資料的具體要件事由。

二、規範主體之分類
（二）比較與分析（1/3）

9

- 國際立法例觀察

立法型態	國家	備註
合法要件及**章節架構**公務、非公務機關分別規定	我國*、日本	
個別條文公務、非公務機關分別規定（例如合法要件）	**德國**	**公務機關私法行為適用非公務機關規定**
未區分	歐盟、英國、韓國	仍得依機關特性有特別規定
不適用公務機關	美國、新加坡	

合併規範利於一體適用；分別規定適合量身打造，各有法制特色

*特種個資之合法要件未區分

- 德國
  - 我國電腦處理個人資料保護法參考當時德國法，採取章節、合法要件區分模式
  - 舊法（1990年版BDSG）採章節、合法要件區分模式
  - 新法（2017年版BDSG）配合GDPR立法，僅合法要件區分公務、非公務機關，**其餘章節架構已不再以公務、非公務機關區分**

國家發展委員會

二、規範主體之分類（二）比較與分析（2/3）

10

● 不同章節架構之比較立法例

公務、非公務機關分別規定		不分別規定
日本：依**組織性質**分章	我國：依**組織&規範性質**分章	歐盟：依**規範性質**分章
第一章 總則 第二章 國家及地方公團責任 第三章 個資保護政策 第四章 非公務機關 第五章 公務機關 第六章 個資保護委員會 第七章 雜則 第八章 罰則 部份章節處理行政組織與執法，損害填補與處罰規定，施行相關規定，與本題討論無關	第一章 總則 第二章 公務機關 第三章 非公務機關 第四章 損害賠償及團體訴訟 第五章 罰則 第六章 附則	第一章 總則 第二章 原則規定 第三章 資料當事人權利 第四章 控管者與處理者 第五章 國際傳輸 第六章 獨立監督機關 第七章 合作及一致性 第八章 救濟、損害賠償、罰則 第九章 特殊處理情形 第十章 授權法及施行法 第十一章 最終條款

我國	公務	合法要件、安全維護、公開供查閱事項
	非公務	合法要件、安全維護、國際傳輸、行政檢查、糾正措施
日本	公務	合法要件、責任規定、安全維護、國際傳輸、事故報告、當事人權利
	非公務	合法要件、責任規定、安全維護、國際傳輸、事故報告、當事人權利

我國規範於總則

*註：日本法原採取非公務機關、公務機關分別立法之立法模式，近年才合併為單一法律

二、規範主體之分類（二）比較與分析（3/3）

11

● 立法模式比較分析

立法模式	公務、非公務機關分別規定	不分別規定
基礎假設	認為公務與非公務機關性質有別，應以不同規範規定	認為個資運用合法性上原則相同，因此原則以同一規定處理，於例外處特別規定
規範形式	◘ 個資運用的合法性要件分別規定 ◘ 通常為兩者分別規定整套管理架構（我國、日本皆以不同章節規定）	◘ 原則上，公務與非公務機關適用相同規範 ◘ 特定要件上可能另外規定（如僅公務機關得基於國家安全等理由蒐集個資）
比較分析	◘ 理論上可依機關性質量身打造適合的規範 ◘ 立法上須小心掛一漏萬而造成適用困難	◘ 大多數要件可一體適用，較不易有涵蓋不足問題 ◘ 立法時需以「原則-例外」方式設定要件

二、規範主體之分類
（三）討論議題

12

Q

1. 我國公務、非公務機關有關個資運用之合法要件，（除依法定職權外）是否有必須分別規定之處？
2. 我國個資運用合法要件若不採公務、非公務機關分別規定的規範模式，能否減少適用上困擾？
3. 若個資運用合法要件仍區分公務、非公務機關，公務機關於私法關係上，是否得參酌德國法，適用非公務機關規定？
4. 若有調整規範主體之必要，則整體章節結構應如何規劃較為妥適？或是否可於不變動現有結構下進行調整？

13

大綱

一 討論範圍

二 規範主體之分類

三 規範行為之分類

四 特定目的之解釋方式

三、規範行為之分類
（一）我國個資法相關規定（1/3）

14

● 個資法將對個資之運用，
分為蒐集、處理、利用三種不同樣態

個人資料保護法
第2條第3款、第4款、第5款
三、蒐集：指以任何方式取得個人資料。
四、處理：指為建立或利用個人資料檔案所為資料之記錄、輸入、儲存、編輯、更正、複製、檢索、刪除、輸出、連結或內部傳送。
五、利用：指將蒐集之個人資料為處理以外之使用。

三、規範行為之分類
（一）我國個資法相關規定（2/3）

15

● 一般個資採取「蒐集處理」、「（目的外）利用」規範模式

	公務機關	非公務機關
蒐集處理	第 15 條 公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、執行法定職務必要範圍內。 二、經當事人同意。 三、對當事人權益無侵害。	第 19 條 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 一、法律明文規定。 二、與當事人有契約或類似契約之關係，且已採取適當之安全措施。 三、當事人自行公開或其他已合法公開之個人資料。 四、學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 五、經當事人同意。 六、為增進公共利益所必要。 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 八、對當事人權益無侵害。 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。
利用	第 16 條 公務機關對個人資料之利用，除第六條第一項所規定資料外，應於執行法定職務必要範圍內為之，並與蒐集之特定目的相符，但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為維護國家安全或增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、有利於當事人權益。 七、經當事人同意。	第 20 條 非公務機關對個人資料之利用，除第六條第一項所規定資料外，應於蒐集之特定目的必要範圍內為之，但有下列情形之一者，得為特定目的外之利用： 一、法律明文規定。 二、為增進公共利益所必要。 三、為免除當事人之生命、身體、自由或財產上之危險。 四、為防止他人權益之重大危害。 五、公務機關或學術研究機構基於公共利益為統計或學術研究而有必要，且資料經過提供者處理後或經蒐集者依其揭露方式無從識別特定之當事人。 六、經當事人同意。 七、有利於當事人權益。 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。 非公務機關於首次行銷時，應提供當事人表示拒絕接受行銷之方式，並支付所需費用。

三、規範行為之分類
（一）我國個資法相關規定（3/3）

16

- 我國將「蒐集」以外的其他運用個資行為分為「處理」及「利用」兩種態樣，但處理及利用在今日的資料運用上已經很難區分，容易衍生後續法規適用上之疑義。

可能包含**處理**、
利用行為

三、規範行為之分類
（二）比較與分析（1/3）

17

- 國際立法例觀察

合法性要件立法型態	包含國家	備註
未區分不同行為	歐盟、英國、**德國**、美國	仍得針對特定行為做特別規定
區分不同行為	我國、日本、韓國、新加坡	

- 德國
  - 我國電腦處理個人資料保護法、個人資料保護法重要參考對象
  - 舊法（1990年版BDSG）將個資法上行為分為蒐集、處理、利用
    但**處理跟利用適用相同合法要件**
  - 新法（2017年版BDSG）配合GDPR立法，**已不再區分蒐集、處理、利用行為**

德國雖也曾區分為蒐集、處理、利用，
但似乎並未給予處理、利用行為不同合法要件。

三、規範行為之分類
（二）比較與分析（2/3）

18

● 採區分不同行為立法型態之立法例之區分方式

國家		個資生命流程		
我國	目的內	蒐集、處理	利用	
	目的外		利用	
日本	目的內/外	處理（取り扱）		提供
韓國	目的內	蒐集、處理		提供
	目的外	處理、提供		
新加坡		蒐集	處理	提供

1. 蒐集以外的個資運用行為，僅我國將其分為處理、利用，其餘則僅單獨將提供區分出來。
2. 蒐集為取得資料過程；提供為將資料交付第三人的行為，風險可能與其他運用行為有別。

*僅就法條外觀觀察呈現

三、規範行為之分類
（三）討論議題

19

Q

1. 我國現行「蒐集、處理、利用」的區分方式，對於實務適用上是否有所不便？是否有改變需要？
2. 若如歐、美等國改採不區分運用型態的合法性要件規範模式，是否有不妥之處？
3. 若仍採取區分模式，如參考日、韓、新模式，僅針對蒐集、提供等風險性質不同之運用型態另做規範，是否恰當？於實務運用上是否有難以執行之處？

20

大綱

一 討論範圍

二 規範主體之分類

三 規範行為之分類

四 特定目的之解釋方式

21

四、特定目的之解釋方式
（一）我國個資法相關規定

- 我國一般個資採取目的內、外分別有不同合法要件模式，特種個資則目的內、外皆共用相同合法要件。
- 我國並未要求新、舊目的間須通過相容性檢驗。

個資種類	合法性要件規定
一般個資	蒐集、處理合法性要件（第15條、19條）與目的外利用要件（第16、20條）分別規定。 目的外利用並不含新舊目的相容性檢驗要求。
特種個資	不區分蒐集處理及目的外利用要件。（第6條）

四、特定目的之解釋方式（二）比較與分析（1/4）

22

- 國際立法例觀察：歐盟（1/2）
  - 一般個資與原始蒐集目的不同之處理行為合法要件：
    1. 當事人同意
    2. 會員國基於國家安全、國防、公共安全、犯罪之偵查追溯、刑罰之執行、公共利益（如公衛、稅賦）、司法程序、職業道德之預防、調查、追溯、公務機關之監管、權利及自由保護、民事請求執行等理由所為特別立法
    3. 通過相容性檢驗，考量下列事項，確保進階處理之目的與原蒐集目的相容
       - 蒐集目的與進階處理目的間之連結（link）
       - 蒐集之脈絡（context）（尤其是資料主體與控管者間關係）
       - 資料本身之性質（例如是否為特種個資）
       - 進階處理對資料主體可能之影響
       - 所採取之適當保護措施

國家發展委員會

四、特定目的之解釋方式（二）比較與分析（2/4）

23

- 國際立法例觀察：歐盟（2/2）相容性檢驗之操作案例

酒測紀錄做出勤紀錄案

公車駕駛於出車前，**基於「確保無酒駕」目的**，以酒測器量測並紀錄酒精濃度及時間。公車公司可否在未取得當事人同意情形下將此一紀錄做為出勤確認之紀錄？

不行。除「確保駕駛安全」與「出勤紀錄」兩目的間**不具有相關性**外；此行為對當事人有**潛在的負面影響**、酒精濃度屬**敏感性個資**等因素亦可佐證兩目的不相容。

智慧電網資料做詐欺偵測案

電網營運者可否利用智慧電錶資料，利用智慧化統計分析系統，在採行技術、組織、程序方法以降低對當事人個資事故風險，並以透明方法告知當事人後，產出匿名之用戶使用型態模型以偵測可能的電錶詐欺行為？

可以。即便該資料有敏感性（犯罪可能）且對當事人有高度負面影響可能，但仍因下列因素認符合相容性要求：

（1）兩目的雖不完全相同，但計價與對計價的詐欺偵測有兩目的緊密相連；
（2）消費者得合理預期業者在採取合理、何比例狀況下進一步使用相關資料；
（3）採取此一措施對其他合法付費用戶具有利益；
（4）採取額外的安全措施。

國家發展委員會

四、特定目的之解釋方式（二）比較與分析（3/4）

24

● 我國與歐盟立法例之比較分析

	利用時之目的		
我國	與蒐集之特定目的相符		於蒐集之特定目的外利用
	得直接利用		須符合16條各款或20條1項各款要件
歐盟	與蒐集目的完全相同	新目的與蒐集目的相容	新目的與蒐集目的不相容
	得直接利用	相容性檢驗	當事人同意或會員國特別立法

個資法第5條 個人資料之蒐集、處理或利用，應尊重當事人之權益，依誠實及信用方法為之，不得逾越特定目的之必要範圍，並應與蒐集之目的具有正當合理之關聯

函釋曾有類似概念 法務部98年1月8日法律字第0970038035號函、102年7月5日法律字第10203507340號函

非公務機關使用基於契約或類似契約關係下取得之個人資料，對該個人當事人進行行銷，應**合乎社會通念下當事人對隱私權之合理期待**，故「行銷行為內容」與「契約或類似契約」二者間，**應有正當合理之關聯**，始符合本法……規定特定目的內利用之範疇，……。如行銷**與當事人契約或類似契約內容無涉之商品或服務資訊**，則除符合本法第20條第1項但書第1款至第5款事由外……，應依同條項第6款規定經當事人書面同意者……，始得為之，……。

四、特定目的之解釋方式（二）比較與分析（4/4）

25

● 相容性檢驗立法模式優劣分析

◆ 優勢：強化個資保護程度

- 允許在考量相容性後為進階處理，有助於對蒐集目的明確性之要求。（避免控管者擔心資料利用受限，而主張較為寬泛的蒐集目的，反而讓當事人不易預見資料可能被處理的樣態）
- 相容性考量似乎可以部份取代「有利於當事人權益」等要件，要求控管者在進行與原始蒐集目的不同之處理行為時，考量脈絡、影響等因素，以強化對當事人個資安全之要求。

◆ 劣勢：複雜性可能造成執行困難

- 相容性檢驗判斷過程須考量眾多不確定因素且難度高，對控管者而言，可能增加法遵風險。
- 相容性的複雜判斷過程，可能使當事人不易確認控管者行為是否合法。

四、特定目的之解釋方式（三）小結與討論議題

26

Q

1. 歐盟的相容性檢驗模式，是否有助於強化個資保護程度？（如有利於要求蒐集目的之明確性、有助於當事人預見資料處理範圍等）
2. 相容性概念之操作，對非公務機關執行上是否有困難？
3. 目前依函釋引入「合理關聯」要求作法是否足夠？有無進一步以法律明文規範之必要？

討論議題

27

- 規範主體之分類
  - 我國公務、非公務機關有關個資運用之合法要件，（除依法定職權外）是否有必須分別規定之處？
  - 我國個資運用合法要件若不採公務、非公務機關分別規定的規範模式，能否減少適用上困擾？
  - 若個資運用合法要件仍區分公務、非公務機關，公務機關於私法關係上，是否得參酌德國法，適用非公務機關規定？
  - 若有調整規範主體之必要，則整體章節結構應如何規劃較為妥適？或是否可於不變動現有結構下進行調整？
- 規範行為之分類
  - 我國現行「蒐集、處理、利用」的區分方式，對於實務適用上是否有所不便？是否有改變需要？
  - 若如歐、美等國改採不區分運用型態的合法性要件規範模式，是否有不妥之處？
  - 若仍採取區分模式，如參考日、韓、新模式，僅針對蒐集、提供等風險性質不同之運用型態另做規範，是否恰當？於實務運用上是否有難以執行之處？
- 特定目的之解釋方式
  - 歐盟的相容性檢驗模式，是否有助於強化個資保護程度？（如有利於要求蒐集目的之明確性、有助於當事人預見資料處理範圍等）
  - 相容性概念之操作，對非公務機關執行上是否有困難？
  - 目前依函釋引入「合理關聯」要求作法是否足夠？有無進一步以法律明文規範之必要？

國家發展委員會

「個人資料保護法相關議題」第 8 場產學專家學者諮詢會議—資料可攜權、被遺忘權議程

壹、 背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（資料可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州消費者隱私法」(CCPA)、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及澳洲「消費者資料權法」(CDR)規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於資料可攜權、被遺忘權之探討。

貳、議程

一、 主席致詞

二、 報告事項

資料可攜權、被遺忘權之探討（國發會）

三、 討論事項

為因應數位時代來臨，在強化當事人權利方面，主要以「資料可攜權、被遺忘權」作為新興資料自主權之代表。所謂「資料

可攜權」係賦予當事人要求控管者提供一定通用格式之個人資料檔案，以方便當事人將其資料在不同控管者間移動；而「被遺忘權」則係為回應數位時代個人資料被搜尋引擎及其他類似網路服務鉅細靡遺記錄，並永久保存、無法抹滅之具體機制，而賦予當事人得在控管者無正當理由保存相關資料之情形下，請求移除或刪除已無運用目的必要之資訊，並被社會所遺忘之權利。然而目前我國個資法並未明文承認當事人具有「資料可攜權、被遺忘權」，惟有論者認為可從個資法第 3 條第 1 款查詢或閱覽請求權與第 2 款複製請求權導引出當事人具有資料可攜之權利，以及從個資法第 3 條第 5 款刪除請求權及第 11 條第 3 項導引出當事人具有被遺忘之權利。針對上述規定，蒐集實務相關函釋見解，進行比較法之分析，整理有關「資料可攜權、被遺忘權」之定義、行使要件、法律效果及限制規定等討論內容，並提出下列二項案由。

案由一、資料可攜權之探討

說明：

一、 我國個資法規定及實務現況

我國個資法第 3 條賦予當事人就其個人資料得行使之權利有第 1 款「查詢或請求閱覽」及第 2 款「請求製給複製本」；又第 10 條規定「公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限：一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。二、妨害公務機關執行法定職務。三、妨害該蒐集機關或第三人之重大利益」。

實務有認為「本法第 3 條規定當事人查詢或請求閱覽、請求製給複製本係保障個人資料當事人對其個人資料之使用有知悉與控制權。當事人依本法第 3 條、第 10 條及第 11 條所得行使之權利，除有第 10 條或第 11 條所定之除外情形，自得依本法規定行使之。」（參照法務部 101 年 6 月 22 日法律字第 10103104090 號函釋、法務部 102 年 3 月 12 日法律字第 10100271950 號函釋）；又有認為「本法明文保障當事人對於保有其個人資料之公務機關或非公務機關，有查詢、請求閱覽或製給複製本之權利，係司法院釋字第 603 號解釋所揭示人民對其個人資料之使用有知悉與控制權之具體展現。」（參照法務部 102 年 7 月 4 日法律字第 10200118830 號函釋），然而所謂資料可攜權應具有取得及移轉之

特性，且至少得請求以電子形式向當事人或第三方傳輸。惟目前尚難從我國個資法有關當事人權利之法條文義及相關實務見解推論當事人賦有得請求資料可攜之權利。

二、 外國相關立法例

綜觀各國法制，多數國家對於資料可攜權之定義，係指當事人應有權要求以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並在不受原控管者阻礙下，有權將資料傳輸給其他控管者；而部分國家僅規定控管者提供電子形式及當事人得請求控管者將資料向其或第三方傳輸之權利，即認為屬資料可攜權。

目前有明文承認資料可攜權之國家，對於資料可攜權所規定之主要要件，說明如下：

(一) 歐盟 GDPR 體系國家(例如德國)、英國、韓國、新加坡對於資料可攜權之規範主要可分為三點：

1. 資料可攜權之請求範圍須為與當事人相關之個人資料，且係由當事人有意識且積極提供之資料，若控管者透過內部分析方法或演算系統，所衍生之資訊或模型等資料，則未包含在內；

2. 資料可攜權之行使僅限於以同意或履行契約為合法處理要件的情形，且以自動化程序處理資料為必要，以其他合法處理要件處理資料則無資料可攜權之適用，亦不適用於資料控管者處理公共事務之情形；

3. 針對資料可攜權之限制規定，包括不得妨礙刪除權之行使、行使時不得損害他人自由及權利、該權利不適用於符合公共利益執行職務或資料控管者受託行使公權力而為必要處理之情形。

(二) 澳洲 CDR：強調消費者資料權之行使要件僅限於同意，且接收方須取得澳洲競爭與消費者委員會之認證以符合適格性要求，包括隱私、資訊安全、爭端解決程序及保險等項目。

(三) 美國 CCPA：一般性承認當事人具有資料可攜之權利，僅

須經身分驗證為消費者本人或有權代表之人即可行使該權利。

三、 其他專業領域之資料可攜權制度

資料可攜權除了於一般性之個資法規定以外，澳洲 CDR 屬於競爭法領域之特別規定，並分別指定於金融、電信、能源業分階段逐步實施。亦有在金融領域實施開放銀行制度而另定特別法，如歐盟的支付服務指令（PSD2）、美國公平信用報告法（FCRA）；或是透過相關政策推動，如英國 midata、德國 LETsmart、日本資料銀行、韓國 My Data、新加坡之金融資料交換（SGFinDex），皆仍會輔以配套制度。資料可攜權雖旨在強化當事人對其個資之掌控，並賦予當事人對其個資之運用有選擇權利之工具，然於產業實施上仍存在技術、資安、成本等各方面挑戰，難以實現其資料可攜之目的。

四、 小結

根據以上觀察，請產學專家就以下議題提供建議：

(一) 我國目前未明文承認當事人具有資料可攜權，惟已有許多國家承認此一權利，需否予以納入規範？

(二) 如明定資料可攜權於個資法，其形式上應包含哪些行使要件？需否如歐盟 GDPR 體系國家、英國規定為保障公共利益或他人自由及權利等情形下得予以限制？

(三) 對於資料可攜權於特定領域應用或推動之建議為何？

案由二、被遺忘權之探討

說明：

一、 我國個資法規定及實務現況

我國個資法第 3 條第 5 款規定當事人就其個人資料具有「請求刪除權」，第 11 條第 3 項規定「個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限」。又第 19 條第 1 項第 7 款及第 19 條第 2 項規定

當事人對取自一般可得來源之個人資料禁止處理或利用者，蒐集或處理者應主動或依當事人之請求，刪除、停止處理或利用該個人資料。

過去實務有認為「有關民眾陳情移除透過網際網路 google 及 yahoo 搜尋引擎搜尋功能出現之商業登記資料，是否符合個資法第 19 條第 1 項第 7 款及第 2 項規定，應先釐清網際網路搜尋引擎搜尋出現個人資料，是否屬本法所稱之蒐集、處理或利用個人資料之行為，如屬上開行為者，宜由個人資料之蒐集或處理者，依個資法第 19 條第 1 項第 7 款規定衡量相較於個人資料之蒐集或特定目的，當事人是否顯有更值得保護之重大利益」（參照法務部 104 年 3 月 11 日法律字第 10403502390 號函）；又有認為「被遺忘權係指要求移除自己負面或過時之個人身分資訊搜尋結果之權利，惟被遺忘權並非我國現行法所承認之權利」（參照臺灣臺北地方法院民事判決 105 年度訴字第 3517 號）。

然而近期實務有認為「資訊主體主張應將其個人身分資訊經搜尋引擎所得搜尋結果刪除時，應就搜尋結果所連結內容之資訊目的、公開資訊之目的及其社會意義、要求刪除事項之性質是否與公共利益有關、公開資訊對被害人造成損害之程度、被害人以何種行為導致發生此種侵害、被害人是否為公眾人物等因素為通盤考量，惟於衡量結果仍不足以正當化該搜尋結果，始得認為有被遺忘權存在」（參照臺灣高等法院 106 年度上字第 1160 號判決）；及「個資主體對於曾經合法公開之個資，因時間經過，其被蒐集、處理或利用之特定目的已不存在，或已逾越該目的之必要範圍，自得請求該資料之蒐集或處理者予以刪除。關於必要性存否之認定，應就個資主體之資訊隱私權與公眾知的權利之公益為法益衡量」（參照最高法院 109 年度台上字第 489 號民事判決）；又有認為「雖因我國並非歐盟會員國，並無 GDPR 之適用或受其拘束，然依釋字第 603 號闡釋資訊隱私權所立足之資訊自主權意涵，被遺忘權顯然已涵蓋在隱私權之範疇，固應受憲法保障至明」（參照臺灣高等法院臺南分院 110 年度上易字第 55 號刑事判決）。

綜上，過去實務雖未承認被遺忘權，然近期實務見解已有逐漸承認被遺忘權之趨勢，肯認被遺忘權為憲法所保障隱私權之內涵，惟強調仍應回歸個資法規定作法益衡量，且應將時間、處理目的、公益等納入判斷標準之考量。

二、 外國相關立法例

(一) 源起

歐盟法院在 2014 年 Google Spain v AEPD and Costeja 一案認為，當與當事人有關的特定資料因時間之流逝有變得不適當、不相關或不再相關、或過當之情形，且該資料可透由在搜尋引擎鍵入當事人姓名而經特定連結近用時，即便系爭資料之公開為合法，搜尋引擎的營運者有義務個案衡量當事人提出的要求，刪除特定連結，以避免對當事人隱私與資料保護權利之侵害。

(二) 被遺忘權之內容

綜觀各國法制，目前歐盟 GDPR 體系國家(例如德國)、英國、美國 CCPA 均已明文承認當事人享有被遺忘之權利，而我國、日本、韓國則僅有刪除權之規定，雖被遺忘權係從刪除權所延伸之權利，惟有明文立法例之國家，其所得請求刪除個人資料之範圍更廣，包括所有與其個人資料相關之連結、複製或仿製等。其他立法例之特點，再詳為說明如下：

1. 歐盟 GDPR 體系國家(例如德國)、英國規定當事人於特定情事下，有權要求資料控管者刪除其個資，控管者因而有義務刪除該個資且不得無故拖延；如控管者已公開該個資，在考量現有科技及執行成本後，該控管者應採取合理步驟及相關措施（包括數位通訊方式），通知其他處理上開公開個資之控管者，有關當事人已提出上開刪除所有與其個資相關之連結、複製或仿製的請求之情事。

2. 美國 CCPA 規定當事人得請求控管者刪除其個資，且控管者應通知其他控管者刪除該個資相關紀錄，除控管者得證明刪除為不可能或所費不貲，始得拒絕。

(三) 被遺忘權之行使要件

1. 歐盟 GDPR 體系國家(例如德國)、英國

目前歐盟 GDPR 體系國家(例如德國)、英國明定被遺忘權之行使要件，包括：（1）蒐集或處理該個人資料時之目的已不再需要；（2）當事人撤回處理該個人資料所需之同意，且該處理欠缺其他法律依據；（3）當事人依拒絕權之相關規定對處理提出異議，且該處理欠缺更為優先之正當事由；（4）該個人資料遭違法運用；（5）控管者依相關規定，有義務刪除該個人資料時；（6）該個

人資料係為向未成年人提供資訊社會服務所蒐集，故係以個資之特定目的消失、欠缺法律依據或正當事由、非法運用等類型為主。

2. 美國 CCPA

美國 CCPA 廣泛賦予當事人刪除請求權，未有特定情形下始得行使之要求。

(四) 限制被遺忘權行使之例外事由

被遺忘權並非絕對之權利，不論歐盟 GDPR 體系國家(例如德國)、英國或美國 CCPA 均明定於例外情形，得限制當事人行使被遺忘權，說明如下：

1. 歐盟 GDPR 體系國家(例如德國)、英國

明定之例外情形包括基於言論自由、執行公權力、公共衛生、科學研究及司法訴訟。

2. 美國 CCPA

則包括基於言論自由、執行公權力、科學研究及履行契約等。

3. 共通限制情形之探討

綜上而言，例外情形主要集中於言論自由、執行公權力、科學研究，內容說明如下：

(1) 基於言論自由之限制，應考量資料之性質、機敏性、對網路使用者資料取得自由之影響、對當事人公眾生活之影響等因素；

(2) 基於法定職務或義務等公權力行使之限制，仍應限於公共利益必要之情形；

(3) 基於科學研究目的之限制，仍應限於可能造成重大妨礙或無法實現之情形。

雖然被遺忘權係賦予當事人得控制其個人相關資料之權利，強化個人之自決權，然而被遺忘權在實施上可能存在技術層面之侷限，且有私人審查言論及寒蟬效應等爭

議性。

三、 小結

根據以上觀察，請產學專家就以下議題提供建議：

(一) 我國目前未明文承認當事人具有被遺忘權，惟歐盟 GDPR 體系國家、英國及美國 CCPA 均已承認此一權利，需否予以納入規範？

(二) 如個資法明定當事人賦有被遺忘權，則需否如歐盟 GDPR 體系國家、英國對被遺忘權定有行使要件，又應包含哪些類型？或如美國 CCPA 一般性承認當事人得行使被遺忘權？

(三) 由於被遺忘權涉及言論自由、公共利益等之衡平判斷，如肯認當事人於個資法上具有被遺忘之權利，則需否設有限制規定？又應包含哪些類型？對產業可能造成之影響為何？

資料可攜權、被遺忘權

國家發展委員會
111 年 5 月 20日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	規範主體、行為區分與特定目的之解釋	資料可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6	111/5/20				

2

大綱

一 討論範圍

二 資料可攜權之探討

三 被遺忘權之探討

四 附件

3

一、討論範圍（1/2）

■ 討論範圍

以「資料可攜權及被遺忘權」為主軸，討論定義及行使要件、法律效果、限制規定，有關其他權利限制規定置於其他場次討論，並以「個資法」為主要討論範疇。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州消費者保護法（CCPA）	2018	CBPR成員 統一個資保護法**非實定法律**，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員
澳洲	消費者資料權法（CDR）	2019	非一般性之個資法規定，屬於競爭法

一、討論範圍（2/2）

4

■ 自從歐盟GDPR正式施行，在當事人權利之強化方面，新增「資料可攜權」與「被遺忘權」。

- 「資料可攜權」係賦予當事人要求控管者提供一定通用格式之個人資料檔案，以方便當事人將其資料在不同控管者間移動（例如：從某一社群網站移轉至另一社群網站）。

- 「被遺忘權」係賦予當事人得以在控管者無正當理由保存相關資料之情形下，得請求移除或刪除已無運用目的必要之資訊，並被社會所遺忘之權利（例如：移除搜尋結果、連結）。

■ 因應數位時代來臨及國際貿易日益頻繁，國際普遍強化當事人對其個人資料之掌控，故本次會議提出二項案由，討論下列問題：

1. 我國個資法有無資料可攜權？倘明定於個資法，需否予以規範其形式、行使要件、限制規定？對於資料可攜權於特定領域應用或推動之建議為何？
2. 我國個資法之刪除權有無延伸被遺忘權利？倘明定於個資法，需否予以規範其行使要件、限制規定？對產業可能造成之影響為何？

國家發展委員會

大綱

5

一 討論範圍

二 資料可攜權之探討

三 被遺忘權之探討

四 附件

國家發展委員會

二、資料可攜權之探討
（一）我國個資法規定及實務現況（1/2）

6

● 個資法賦予當事人查詢或請求閱覽、製給複製本之權利

個人資料保護法	個人資料保護法施行細則
第3條第1款、第2款 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之： 一、查詢或請求閱覽。 二、請求製給複製本。 **第10條** 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限： 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。 二、妨害公務機關執行法定職務。 三、妨害該蒐集機關或第三人之重大利益。	**第18條** 本法第10條但書第3款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

二、資料可攜權之探討
（一）我國個資法規定及實務現況（2/2）

7

● 實務見解

- 本法第3條規定當事人查詢或請求閱覽、請求製給複製本係保障個人資料當事人對其個人資料之使用有知悉與控制權。當事人依本法第3條、第10條及第11條所得行使之權利，除有第10條或第11條所定之除外情形，自得依本法規定行使之。（法務部101年6月22日法律字第10103104090號函釋）
- 如病患依本法第3條規定向醫療機構申請，請求閱覽本人之病歷資料，考量病歷資料之性質，倘有妨害該蒐集機關之重大利益者（例如：病歷有遭受毀損、滅失、塗改或散佚之虞而無其他方法防止者），本得依第10條但書規定拒絕提供閱覽，否則應依當事人之請求閱覽而提供閱覽，亦不得以製給複製本代替。（法務部102年3月12日法律字第10100271950號函釋）
- 本法明文保障當事人對於保有其個人資料之公務機關或非公務機關，有查詢、請求閱覽或製給複製本之權利，係司法院釋字第603號解釋所揭示人民對其個人資料之使用有知悉與控制權之具體展現。（法務部102年7月4日法律字第10200118830號函釋）

資料可攜權具有取得及移轉之特性，至少得請求以電子形式向當事人或第三方傳輸。惟目前尚難從我國個資法有關當事人權利之法條文義及相關實務見解推論當事人賦有得請求資料可攜之權利。

二、資料可攜權之探討（二）外國相關立法例（1/4）

8

當事人應有權要求以有結構的、通常使用的、機器可讀的形式，接收其提供予控管者之資料，並在不受原控管者阻礙下，有權將資料傳輸給其他控管者。

● 國際立法例 - 資料可攜權之形式

*韓國、新加坡尚未施行資料可攜權

國家	明文	形式			傳輸對象
		結構性	通用性	機器可讀性	
歐盟GDPR	O	O	O	O	當事人、第三方
英國	O	O	O	O	當事人、第三方
德國	O	O	O	O	當事人、第三方
美國 CCPA	O	O	O	O	當事人、第三方
美國 UPDPA	X	無規定			
日本	▲	X	X	O（電子形式）	當事人
韓國*	O	O	O	O	當事人、第三方
新加坡*	O	X	O	O（電子形式）	當事人、第三方
澳洲CDR	O	X	X	O	當事人、第三方

1. 多數國家對於資料可攜權之定義，係指當事人應有權要求以有結構性、通用性、機器可讀性之形式，接收其提供予控管者之資料，並在不受原控管者阻礙下，有權將資料傳輸給其他控管者。
2. 部分國家僅規定控管者提供電子形式及當事人得請求控管者將資料向其或第三方傳輸之權利，即認為屬資料可攜權。
3. 日本之開示請求權雖賦予當事人得請求控管者以電磁紀錄方式提供個資，惟如同我國之查詢或閱覽及複製請求權僅限於向當事人傳輸之情形，故亦非等同GDPR之資料可攜權。

國家發展委員會

二、資料可攜權之探討（二）外國相關立法例（2/4）

9

● 資料可攜權之行使要件

名稱	行使要件	包含國家
資料可攜權	同意 / 履行契約+自動化決策	歐盟GDPR、英國、德國、韓國、新加坡
消費者資料權	同意 + 接收方須取得適格認證	澳洲CDR
知的權利	須經驗證為消費者本人或有權代表之人	美國CCPA
未明定	無	我國、日本、美國UPDPA

歐盟GDPR體系（如德國）、英國、韓國、新加坡之資料可攜權

- 資料可攜權之請求範圍須為與當事人相關之個人資料，且係由當事人有意識且積極提供之資料，若控管者透過內部分析方法或演算系統，所衍生之資訊或模型等資料，則未包含在內。
- 資料可攜權之行使僅限於以同意或履行契約為合法處理要件的情形，且以自動化程序處理資料為必要，以其他合法處理要件處理資料則無資料可攜權之適用，亦不適用於資料控管者處理公共事務之情形

澳洲CDR

- 強調消費者資料權之行使僅限於同意，且接收方取得「澳洲競爭與消費者委員會」（Australian Competition and Consumer Commission, ACCC）認證以符合適格性要求，包括隱私、資訊安全、爭端解決程序及保險等項目。

美國CCPA

- 一般性承認當事人具有資料可攜之權利，僅須經身分驗證為消費者本人或有權代表之人即可行使該權利。

國家發展委員會

二、資料可攜權之探討（二）外國相關立法例（3/4）

10

●資料可攜權之限制規定

- 歐盟GDPR體系
  1. 不得妨礙刪除權之行使；
  2. 行使時不得損害他人自由及權利；
  3. 該權利不適用於符合公共利益執行職務，或資料控管者受託行使公權力而為必要處理之情形。
- 美國CCPA、澳洲CDR
  - 如符合行使要件之規定，則一般性承認當事人具有資料可攜之權利，故未對資料可攜權行使上予以例外限制。

歐盟GDPR體系對資料可攜權採取限制之情形，以公共利益、他人自由及權利等類型為主。

二、資料可攜權之探討（二）外國相關立法例（4/4）

11

□ 有關資料可攜權於產業應用之國際觀察

- 歐盟GDPR體系、美國CCPA
  - 個資法所賦予當事人之資料可攜權於所有行業均一般通用。
- 澳洲CDR
  - 由財政部長指定特定行業實施資料可攜制度，首先於銀行業分階段逐步實施，並預計2022年11月於能源、電信業試行。
- 其他專業領域之資料可攜權制度
  - 特別法：歐盟的支付服務指令（PSD2）、美國公平信用報告法（FCRA）
  - 相關政策：英國midata、德國LETsmart、日本資料銀行、韓國My Data、新加坡之金融資料交換（SGFinDex）。

資料可攜權除了於一般性之個資法規定以外，澳洲CDR屬於競爭法領域之特別規定；亦有在金融領域實施開放銀行制度而另定特別法，或是透過相關政策推動，皆仍會輔以配套制度。

二、資料可攜權之探討
（三）小結與討論議題

12

Q

1. 我國目前未明文承認當事人具有資料可攜權，惟已有許多國家承認此一權利，需否予以納入規範？
2. 如明定資料可攜權於個資法，其形式上應包含哪些行使要件？需否如歐盟GDPR體系國家、英國規定為保障公共利益或他人自由及權利等情形下得予以限制？
3. 對於資料可攜權於特定領域應用或推動之建議為何？

大綱

13

一 討論範圍
二 資料可攜權之探討
三 被遺忘權之探討
四 附件

三、被遺忘權之探討
（一）我國個資法規定及實務現況（1/3）

14

● 個資法賦予當事人之刪除權

個人資料保護法	個人資料保護法施行細則
第3條第5款 當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之： 五、請求刪除。 **第11條第3項** 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 **第11條第4項** 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。 **第19條第1項第7款** 非公務機關對個人資料之蒐集或處理，除第六條第一項所規定資料外，應有特定目的，並符合下列情形之一者： 七、個人資料取自於一般可得之來源。但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 **第19條第2項** 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。	**第20條** 本法第十一條第三項所稱特定目的消失，指下列各款情形之一： 一、公務機關經裁撤或改組而無承受業務機關。 二、非公務機關歇業、解散而無承受機關，或所營事業營業項目變更而與原蒐集目的不符。 三、特定目的已達成而無繼續處理或利用之必要。 四、其他事由足認該特定目的已無法達成或不存在。 **第21條** 有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須： 一、有法令規定或契約約定之保存期限。 二、有理由足認刪除將侵害當事人值得保護之利益。 三、其他不能刪除之正當事由。

三、被遺忘權之探討
（一）我國個資法規定及實務現況（2/3）

15

● 早期實務見解

- 有關民眾陳情移除透過網際網路google及yahoo搜尋引擎搜尋功能出現之商業登記資料，是否符合個資法第19條第1項第7款及第2項規定，應先釐清網際網路搜尋引擎搜尋出現個人資料，是否屬本法所稱之蒐集、處理或利用個人資料之行為，如屬上開行為者，宜由個人資料之蒐集或處理者，依個資法第19條第1項第7款規定衡量相較於個人資料之蒐集或特定目的，當事人是否顯有更值得保護之重大利益。（法務部104年3月11日法律字第10403502390號函）
- 被遺忘權係指要求移除自己負面或過時之個人身分資訊搜尋結果之權利，惟被遺忘權並非我國現行法所承認之權利。（臺灣臺北地方法院105年度訴字第3517號民事判決）

1. 由於被遺忘權之行使得基於法令、運用目的消失、欠缺法律依據或正當事由、非法運用等情形為之；且請求對象主要為搜尋引擎、社群媒體等資料控管者，得請求其將搜尋結果、連結等刪除。
2. 惟從目前我國個資法當事人刪除權之法條文義及過去實務見解，尚難論定搜尋引擎等網路服務提供者究屬蒐集、處理或利用者，則當事人得否逕向搜尋引擎請求刪除亦存有疑義，難認已具有「被遺忘權」之概念。

三、被遺忘權之探討
（一）我國個資法規定及實務現況（3/3）

16

● 近期實務見解

- 資訊主體主張應將其個人身分資訊經搜尋引擎所得搜尋結果刪除時，應就搜尋結果所連結內容之資訊目的、公開資訊之目的及其社會意義、要求刪除事項之性質是否與公共利益有關、公開資訊對被害人造成損害之程度、被害人以何種行為導致發生此種侵害、被害人是否為公眾人物等因素為通盤考量，惟於衡量結果仍不足以正當化該搜尋結果，始得認為有被遺忘權存在。（臺灣高等法院106年度上字第1160號民事判決）
- 個資主體對於曾經合法公開之個資，因時間經過，其被蒐集、處理或利用之特定目的已不存在，或已逾越該目的之必要範圍，自得請求該資料之蒐集或處理者予以刪除。關於必要性存否之認定，應就個資主體之資訊隱私權與公眾知的權利之公益為法益衡量。（最高法院109年度台上字第489號民事判決）
- 雖因我國並非歐盟會員國，並無GDPR之適用或受其拘束，然依釋字第603號闡釋資訊隱私權所立足之資訊自主權意涵，被遺忘權顯然已涵蓋在隱私權之範疇，固應受憲法保障至明。（臺灣高等法院臺南分院110年度上易字第55號刑事判決）

近期實務見解已逐漸承認「被遺忘權」為憲法所保障隱私權之內涵，惟仍應回歸個資法規定作法益衡量，並在判斷標準上應將時間、處理目的、公益等納入考量。

國家發展委員會

三、被遺忘權之探討
（二）外國相關立法例（1/4）

17

● 被遺忘權之源起

2014年*Google Spain v AEPD and Costeja*，歐盟法院認為當與資料主體有關的特定資料因時間之流逝有變得不適當、不相關或不再相關、或過當之情形，且該資料可透由在搜尋引擎鍵入資料主體姓名而經特定連結近用時，即便系爭資料之公開為合法，搜尋引擎的營運者有義務個案衡量資料主體提出的要求，刪除特定連結，以避免對資料主體隱私與資料保護權利之侵害。

◆ 「被遺忘權」係賦予當事人得以在控管者無正當理由保存相關資料之情形下，得請求移除或刪除已無運用目的必要之資訊，並被社會所遺忘之權利（例如：移除搜尋結果、連結）。

被遺忘權係從刪除權所延伸之權利，當事人得向搜尋引擎、社群媒體等網路服務提供者請求，刪除與其個人資料相關之搜尋結果、連結、複製等。

國家發展委員會

三、被遺忘權之探討
（二）外國相關立法例（2/4）

18

國際立法例觀察：刪除權之內容		包含國家
刪除權（被遺忘權）	歐盟GDPR體系、英國： • 當事人於特定情事下，有權要求資料控管者刪除其個資，控管者有義務刪除該個資且不得無故拖延。 • 如控管者已公開該個資，在考量現有科技及執行成本後，該控管者應採取合理步驟及相關措施（包括數位通訊方式），通知其他處理上開個資之控管者，有關當事人已提出上開刪除所有與其個資相關之連結、複製或仿製的請求之情事。 美國CCPA： • 當事人得請求控管者刪除其個資，且控管者應通知其他控管者刪除該個資相關紀錄，除控管者得證明刪除為不可能或所費不貲，始得拒絕	歐盟GDPR體系國家（德國）、英國、美國CCPA
刪除權	當事人有權請求控管者刪除其個人資料。（控管者在特定目的消失或期限屆滿等情形，始負有刪除義務）	我國、日本、韓國
未明定	無	美國UPDPA、新加坡

1. 被遺忘權相較於刪除權而言，得請求刪除之範圍更廣，包括所有與其個人資料相關之連結、複製或仿製等。
2. 被遺忘權要求控管者在考量現有科技及執行成本，應採取適當措施與技術形式向其他控管者踐行通知義務，因此如搜尋引擎等其他控管者亦負有刪除義務。

三、被遺忘權之探討
（二）外國相關立法例（3/4）

19

- 被遺忘權之行使要件
  - ◆ 歐盟GDPR體系、英國：
    - ■蒐集或處理該個人資料時之目的已不再需要；
    - ■當事人撤回處理該個人資料所需之同意，且該處理欠缺其他法律依據；
    - ■當事人依拒絕權之相關規定對處理提出異議，且該處理欠缺更為優先之正當事由；
    - ■該個人資料遭違法運用；
    - ■控管者依相關規定，有義務刪除該個人資料時；
    - ■該個人資料係為向未成年人提供資訊社會服務所蒐集。
  - ◆ 美國CCPA：
    - ■未規定當事人須符合特定要件始得請求刪除。

1. 歐盟GDPR體系、英國明定被遺忘權之行使要件，主要以個資之特定目的消失、欠缺法律依據或正當事由、非法運用等類型。
2. 美國CCPA廣泛賦予當事人刪除請求權，未有特定情形下始得行使之要求。

三、被遺忘權之探討
（二）外國相關立法例（4/4）

20

● 被遺忘權之限制規定

	言論自由	法定職務或義務	公共衛生	科學研究	司法訴訟	履行契約	其他
歐盟GDPR	○	○	○	○	○		
美國CCPA	○	○		○		○	• 為確保資料安全及完整性； • 用於修復現有預期功能的錯誤； • 基於合理期待於內部使用。

1. 基於言論自由之限制，應考量資料之性質、機敏性、對網路使用者資料取得自由之影響、對當事人公眾生活之影響等因素。
2. 基於法定職務或義務等公權力行使之限制，仍應限於公共利益必要之情形。
3. 基於科學研究目的之限制，仍應限於可能造成重大妨礙或無法實現之情形。

被遺忘權並非絕對，在例外情形得限制當事人行使被遺忘權，主要限於言論自由、公權力行使、科學研究之類型。

國家發展委員會

三、被遺忘權之探討
（三）小結與討論議題

21

Q

1. 我國目前未明文承認當事人具有被遺忘權，惟歐盟GDPR體系國家、英國及美國CCPA均已承認此一權利，需否予以納入規範？
2. 如個資法明定當事人賦有被遺忘權，則需否如歐盟GDPR體系國家、英國對被遺忘權定有行使要件，又應包含哪些類型？或如美國CCPA一般性承認當事人得行使被遺忘權？
3. 由於被遺忘權涉及言論自由、公共利益等之衡平判斷，如肯認當事人於個資法上具有被遺忘之權利，則需否設有限制規定？又應包含哪些類型？對產業可能造成之影響為何？

國家發展委員會

22

討論議題

案由一、資料可攜權之探討

- 我國目前未明文承認當事人具有資料可攜權，惟已有許多國家承認此一權利，需否予以納入規範？
- 如明定資料可攜權於個資法，其形式上應包含哪些行使要件？需否如歐盟GDPR體系國家、英國規定為保障公共利益或他人自由及權利等情形下得予以限制？
- 對於資料可攜權於特定領域應用或推動之建議為何？

案由二、被遺忘權之探討

- 我國目前未明文承認當事人具有被遺忘權，惟歐盟GDPR體系國家、英國及美國CCPA均已承認此一權利，需否予以納入規範？
- 如個資法明定當事人賦有被遺忘權，則需否如歐盟GDPR體系國家、英國對被遺忘權定有行使要件，又應包含哪些類型？或如美國CCPA一般性承認當事人得行使被遺忘權？
- 由於被遺忘權涉及言論自由、公共利益等之衡平判斷，如肯認當事人於個資法上具有被遺忘之權利，則需否設有限制規定？又應包含哪些類型？對產業可能造成之影響為何？

國家發展委員會

23

大綱

一 討論範圍

二 資料可攜權之探討

三 被遺忘權之探討

四 附件

國家發展委員會

24

歐盟相關規定（1/4）

最近一次個資法修正：2016年（2018年施行）

	資料可攜權（right to data portability）
立法討論	• 為使個人資料的掌控權回歸到民眾手中 • 為促進資料控管者間資料無阻礙傳輸
定義	1. 從資料控管者端取得與資料主體相關的個人資料，並無阻礙的將該資料傳輸給其他資料控管者 2. 技術允許時，原資料控管者直接將資料主體個人資料傳輸給其他資料控管者
權利行使要件	• 個人資料必須是有結構性、通用性、機器可讀取性之格式 • 僅限於使用同意為合法處理要件或依契約為合法處理要件的情形 • 以自動化模式處理資料
數位金融產業資料可攜權應用	《支付服務指令2》（Payment Services Directive, PSD 2） • 資料可攜權的強制應用 • 消費者得以將資料以數位化的方式傳輸於銀行與第三方服務業者之間 • 銀行必須採用適當的技術措施

國家發展委員會

25

歐盟相關規定（2/4）

有關資料可攜權實施後之檢視-以歐盟為例*

* From EUROPEAN COMMISSION [EC], "Data Portability Implementation Status", JRC Conference and Workshop Report, Unfolding opportunities from the use of APIs in Europe (2021)

正面影響	常見實務爭議問題
1) 促進電子化個人資料服務之提供與加值應用； 2) 促進產品創新； 3) 促進市場公平競爭； 4) 增加以資料所賺取的商業利益； 5) 當事人可選擇將資料與小型公司分享，防止資料被大型科技巨頭掌握。	1) 資料未以機器可讀之形式傳輸，如資料標準化機制之建置、自動化資料輸入及輸出管道； 2) 在技術方面及資訊安全風險上極為難以提供資料； 3) 透過資料夾所提供之資料不實用或不完整； 4) 資料之提供已超過法定期限； 5) 當事人行使資料可攜權的經驗落差大，許多企業會向當事人索取更多資訊，欲使當事人放棄繼續行使資料可攜權； 6) 企業認為當事人資料可攜權之請求極為繁瑣，有些企業直接向當事人提出刪除帳號的方案，而非確實行使資料可攜權。

1. 強化當事人對其個資之掌控，並賦予當事人對其個資之運用有選擇權利之工具。
2. 實施上仍存在技術、資安、成本等各方面挑戰，難以實現目的。

國家發展委員會

26

歐盟相關規定（3/4）

最近一次個資法修正：2016年（2018年施行）

	被遺忘權（right to erasure、right to be forgotten）
定義	資料主體有權要求資料控管者刪除其個人資料，資料控管者不得無故拖延
歐盟法院 *Google Spain v AEPD and Costeja* 案→ EDPB 對權利行使要件、權利限制規定發布指引	
權利行使要件	• 個人資料對於蒐集或處理該資料之特定目無必要 • 採用同意作為處理資料之合法處理要件，而資料主體收回同意且無其他合法處理要件之適用 • 對公共利益處理要件、合法利益處理要件行使拒絕權，且資料控管者無法證明有其他重要的合法依據比資料主體的利益、權利、自由重要 • 非法處理個人資料 • 因必須遵守歐盟或是歐盟成員國法律，資料控管者必須刪除個人資料 • 對未成年人提供資訊社會服務
權利限制規定	• 資料傳輸因落實言論自由、資訊取得自由而必要 • 資料傳輸因資料控管者必須遵循歐盟或歐盟成員國法律，或執行公共利益職務，或執行法定職務而必要 • 資料傳輸因公共衛生公共利益而必要 • 資料傳輸因建檔、科學研究、歷史研究、統計目的而必要，但被遺忘權之行使有可能嚴重影響研究成果或使研究無法執行 • 資料傳輸因法律案件而必要

國家發展委員會

27

歐盟相關規定（4/4）

有關被遺忘權實施後之檢視-以歐盟為例*

正面影響	1) 保護個資之基本人權 2) 強化當事人之資訊自主權 3) 尊重個人私生活及家庭生活
常見實務爭議問題	1) 落實上有技術層面上的侷限，例如：控管者範圍過於廣泛、適當之通知方式、刪除之方式及範圍等 2) 可能阻礙正當資訊之自由流通，言論自由與知的權利（比例原則法益衡量）之衝突，且涉及私人審查言論之妥適性 3) 控管者如拒絕刪除負有舉證責任，且為避免受罰，故傾向接受多數刪除資料之要求

1. 被遺忘權賦予當事人控制其個人相關資料之權利，強化個人資訊自決權。
2. 實施上可能有技術層面侷限，且有私人審查言論及寒蟬效應等爭議性。

國家發展委員會

28

英國相關規定（1/2）

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

資料可攜權	
定義	● 資料主體有權以**有結構的、通常使用的、機器可讀**的形式，接收其提供予控管者之資料，並有權將之傳輸給其他控管者，而不受控管者之妨礙。（UK GDPR §20 I） ● 如果技術許可，資料主體也有權使個人資料由一控管者直接傳輸給另一個控管者。（UK GDPR §20 II）
立法	引用自歐盟GDPR
行使要件	● 基於資料主體之同意取得個資/依契約方式取得個資 ● 控管者處理是以自動化方式進行（UK GDPR §20 I）
限制規定	**會妨礙或嚴重損害公共利益目的的實現時**，出於公共利益的存檔目的而處理的個人資料將無法行使資料可攜權（DPA 2018 附件二 §28 I II）
應用	讓消費者能夠以可攜式和電子格式近用他們的個人資料，使用這些資料來幫助了解自己的消費行為和模式，並做出更明智、更合適的消費決策。 ● 金融：midata、開放銀行、Smart Data ● 電信：midata、Smart Data ● 能源：midata、Smart Data

國家發展委員會

29

英國相關規定（2/2）

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

刪除權（被遺忘權）	
定義	個人有權要求其個人資料被刪除
行使要件	(a)就蒐集或處理之目的不再存在 (b)資料主體撤回同意 (c)資料主體依拒絕權對處理提出異議 (d)該個人資料遭違法處理者 (e)控管者依國內法有義務刪除個人資料者 (f)兒童的個人資料是基於本人或法定代理人之同意，為了提供資訊社會服務所蒐集者（UK GDPR§17 I）
限制規定	(a)為行使表意自由及資訊權 (b)履行法律義務/公共利益職務執行/行使公權力 (c)基於公共衛生領域之公共利益 (d)公共利益、科學或歷史研究目的或統計目的 (e)為了建立、行使或防禦法律上之請求者 （UK GDPR§17 III）
重大案件	NT1 & NT2 v Google LLC(2018)，運用The Article 29 Working Party Guidelines規則

國家發展委員會

30

德國相關規定（1/2）

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

一、**資料可攜權**

- **立法目的**：提供資料主體對自身個人資料的掌控權利+開放資料流通的限制
- **影響**：過去受限於高密度的監管要求，被要求以封閉式方式傳遞或處理個人資料，但透過資料可攜權的行使，得於符合一定條件下打破相關封閉式的資料流通限制。
- **行使條件**：依GDPR第20條規定。
- **提供方式**
  - **直接提供資料**（Direkt bereitgestellte Daten）：以資料主體本人之個人相關資料，例如姓名、地址等由資料主體為中心所提供之資料。
  - **間接提供資料**（Indirekt bereitgestellte Daten）：係透過使用線上服務或聯網設備所生成之資料，例如帳戶交易記錄、健身活動之生理監測數據等，因資料控管者衍生或生成的資料。

31

德國相關規定（2/2）

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

二、**被遺忘權**

- **行使條件**：依GDPR第17條第1項規定。
- **例外不得行使刪除權**：
  - ✓ 依GDPR第17條第3項規定；
  - ✓ 另BDSG第35條第1項補充，除違法處理之情形，如符合下列事由者，亦無刪除權之適用：
    - 非自動化處理之情形+
    - 特殊類型的儲存/需透過不合比例的努力，才能刪除資料+
    - 刪除資料對於資料主體利益較低

32

美國（1/2）

無聯邦個資法，加州消費者隱私法（CCPA）最近修正為2018年，修正CCPA的新法CPRA將於2023年實施，效力溯及2022年1月1日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

法規	CCPA & CPRA	UPDPA
資料可攜權定義及規定	• 營利事業提供特定個人資料時，須在對平均消費者而言易懂、技術可行的前提下，以「有體系的（structured）、常用的（commonly used）、機器可讀的形式（machine-readable format）提供」（*CPRA§1798.130 (a)(3)(B)(iii)*）	• 資料主體可請求資料複本 • 無便攜形式規定（*UPDPA § 5、§ 4(a)(1)*）
資料可攜權行使要件	(1) 消費者須為加州居民，且 (2) 該請求須是可以商業上合理方式驗證消費者身分之「可驗證的消費者請求」（verifiable consumer request）（*CPRA§1798.130(a)(3)(A)*）	• 資料主體須經身分驗證（*UPDPA § 5(a)*）
資料可攜權制定理由、贊同及反對意見	• 取得消費者對自己個人資料控制權 • 贊同意見：應與其他數位服務或產品一起不受阻礙地使用格式 • 反對意見：資訊獲知範圍應排除安全、保密、完整性目的之資料	• 受批評：未賦予資料主體請求「機器可讀」形式
法規	**特定產業應用之相關聯邦法律**	
	• 消費者信用：依《公平信用報告法》（Fair Credit Reporting Act），涉及消費者信用的金融機構提供及使用信用資料、消費者信用報告揭露須以書面為之，或經消費者授權以書面以外形式提供。（*FCRA §610*） • 醫療保險：依《健康保險可攜與責任保險法》（Health Insurance Portability and Accountability Act，HIPAA）經個人要求，受規範機構必須以個人要求之形式提供其PHI，如不能輕易產製該形式之PHI，仍須以雙方同意的可讀形式提供。（*HIPAA § 164.524 (c)(2)*）	

33

美國（2/2）

法規	CCPA & CPRA	UPDPA

刪除權（被遺忘權）	**對營利事業請求：**
	• 消費者有權請求**刪除個人資料**（*CPRA§1798.105 (a)*）
	• **營利事業**須**揭露**消費者有請求刪除權利、應刪除紀錄、通知其他曾自營利事業收受之第三方刪除資料（*CPRA§1798.105 (b)、(c)、§1798.130*）
	  • 例外1：可證明**刪除不可能**或所費成本不成比例（*CPRA§1798.105 (c)(1)*）
	  • 例外2：其他本法允許事由可保留一份**刪除請求機密紀錄**（*CPRA §1798.105 (c)(2)*）
	服務提供者、承包商須協助營利事業刪除
	• 於營利事業通知刪除後應協助處理
	• 再通知其他服務提供者、承包商或第三方，除非可證明該刪除為不可能或所費甚鉅不符比例（*CPRA§1798.105 (c)(3)*）
	  ➢ 如消費者直接向服務提供商或承包商請求刪除，兩者不須遵從（*CPRA§1798.105(c)(3)*）
	營利事業、服務提供者和承包商為達成下列目的，無義務刪除個人資料：
	（1）為了完成該個資蒐集目的之交易、履行保證條款、履行與消費者間的契約等；
	（2）為了協助確保安全性和完整性之目的，個資使用是合理必要；
	（3）除錯、修復損害現有預期功能的錯誤；
	（4）行使言論自由，確保其他消費者言論自由權或其他法定權利
	（5）根據加州《刑法典》的要求遵守《加州電子通訊隱私法》；
	（6）符合所有其他適用之道德和隱私法的前提下，從事公共或經同儕評鑑的科學、歷史或統計研究，且消費者已提供知情同意，而企業刪除資料可能嚴重損害完成該研究的能力或導致不可能完成；
	（7）消費者依其與企業的關係所生的合理期待，於消費者資料提供背景相一致的內部使用；
	（8）履行法定義務。（*CPRA§1798.105(d)*）
		• 無規定
		• UPDPA的主要考量是避免企業法遵和監管成本過重（*2021/6 草案版本 Prefatory Note*）
		• 考量控制者和處理者保有個人資料的正當性範圍廣大，且現今資料儲存、處理的方式而言，要確保任何特定資料主體的資料是否已刪除，實屬困難（*2021年6月草案版本§4 comment*）

34

日本相關規定（1/2）

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

一、資料可攜權之規定

- **日本個人資料保護委員會之法制研究報告**
  - ✓ 資料可攜權之定義與相關法律規定

資料可攜權之對應用語	**ポータビリティ**（portability）
資料可攜權之類似規定	本人得請求公開電磁紀錄或紙本之規定(§33)

- **日本公平交易委員會之競爭政策研究報告**

資料可攜權涉及競爭政策：因為既存業者有資訊的優位性，法制度中加入資料可攜權之設計會對欲加入該產業者較為友善。

- **日本資料可攜權之類似制度**

情報銀行、my portal、電話號碼之資料可攜權。

35

日本相關規定（2/2）

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

二、被遺忘權之規定

- **個人資料保護委員會**
  - ✓ 被遺忘權應同於刪除權（消去権）。
  - ✓ 日本刪除權可見於日本個資法第35條。
- **判例介紹**
  - ✓ 最高裁判所決定(平成29年1月31日)、針對提供檢索結果之行為是否違法訂出判斷標準，如下：

① 依某人該屬於隱私之事實其性質以及內容
② 該URL等資訊被提供後事實之傳達範圍與某人所遭受具體被害之程度
③ 某人之社會地位與影響力
④ 該記事的目的與意義
⑤ 該記事等被刊登後社會的狀況與其後發展
⑥ 前揭事實記載之必要性等
⑦ 該事實不公開之法律上利益與該URL等資訊表示為檢索結果之理由等比較衡量

36

韓國相關規定（1/2）

韓國政府於2021年9月28日提出「個人資料保護法修正草案」
（以下簡稱草案，惟目前仍在國會審議中）

	資料可攜權（right to data portability）
立法討論	• 現行PIPA未將資料資料可攜權明文化 • 然為配合政府發展「My Data」政策，期望能在保護個人資料的前提下，創建公開資料與非公開資料相互融合的生態系，並於數位時代下保護國民對於自身資料的自主權，故於本次提出修正案，將資料可攜權明文化
定義	• 資料主體可要求個人資料控制者將其個人資料傳輸給本人、其他個人資料管控者或者專門的個人資料管理機構（草案 §35-2 ）
權利行使要件	• 僅限於取得當事人同意或依契約為合法處理要件的情形（現行PIPA§15 I①、④） • 當資料當事人要求傳輸時，個人資料在合理的時間、成本及技術可行的情況下，資料須是有架構性、常規使用性、機器可讀取性之格式 • 不得侵害他人權利或利益
數位金融產業資料可攜權應用	韓國參考 PSD2，於2018年6月第四屆工業革命網絡國家論壇通過「資料產業振興戰略」，推出「My Data試行計畫」，由個人資料信用管理業務試辦： • 自願自律模式，採許可證的管理制度 • 消費者得以將資料以數位化的方式傳輸於銀行與第三方服務業者之間 • 除設有最低資本額限制，以及責任保險要求，加入「MyData」試辦的企業，亦須具備個人資料保護制度及相關適當安全管理措施，以確保制度的順利推行

國家發展委員會

37

韓國相關規定（2/2）

	刪除權（right to erasure）
定義	個資當事人在閱覽其個資後，得就該個人資料向資料處理者提出更正或刪除的要求。
被遺忘權的討論	• 因應2014年的Google案，韓國通信委員會（Korea Communications Commission, KCC）成立被遺忘權研究小組。 • 2016年4月29日KCC發布了關於「被遺忘權指南」，並於同年6月生效。 • 根據指南，個資當事人得要求線上網路服務業者，限制其用戶在網路上搜尋或閱讀該個資當事人過去上傳的內容。
權力行使要件	• 現行PIPA於第36條明文規定個資當事人得行使刪除權（삭제권）。 • 刪除權的權力行使方式為資料當事人根據第35條閱覽自己個資後，就該個資得向個資處理者提出更正或刪除之要求。 • 個資處理者應在接收到刪除請求時，應於10日內作出回復，並根據請求進行更正或刪除。 • 個資處理者接獲資料當事人提出的刪除要求時，應立即進行調查，不得遲延，並應將結果告知資料當事人。 • 個資處理者依刪除個資時，應設置使該資料不會回復或重製之措施。 • 個資處理者接獲當事人提出要求時，若在進行調查而有必要時，得向當事人請求提交必要的證明文件。
權利限制規定	• 其他法令明定不可刪除時，則例外不得刪除。 • 例外不得刪除時，資料處理者應立即告知當事人，說明拒絕的決定與理由，以及如何申訴等管道。

國家發展委員會

新加坡相關規定

38

最近一次個資法修正：2020年
CBPR成員國

資料可攜（data portability）：有，即將施行
個人得向移轉組織提出請求（稱為資料移轉請求），請求移轉組織將資料移轉請求中指定之個人適用資料傳輸至接收組織。（PDPA草案第26H條第一項）（尚未生效）

行使要件
僅適用於移轉組織於收到與適用資料有關的資料移轉請求之日，以電子形式提供之適用資料；及移轉組織於收到與適用資料有關的資料移轉請求之日前，在規定期限內蒐集或建立適用資料之情形。（PDPA第26F條）（尚未生效）

例外規定
若組織**合理預期**資料傳輸將可能威脅到與適用資料相關的個人以外之**個人安全或身心健康**、對適用資料所涉及之個人安全或身心健康造成直接或嚴重傷害、**違反國家利益**；或是接收適用資料傳輸之接收組織是或屬於被規定為排除接收組織之組織類別；或是**PDPC指示移轉組織勿傳輸適用資料**，則組織可不傳輸相關資料。（PDPA附表12）（尚未生效）

被遺忘權：無

澳洲相關規定

39

2019年8月通過《2019年消費者資料權法》，針對《2010年競爭及消費者法》、《2010年澳洲資訊專員法》及《1988年隱私法》增訂「消費者資料權」相關規定

消費者資料	• 經財政部長依法指定行業的資料種類及其衍生資料，包含客戶資料（Customer Data）、帳戶（Account Data）及交易資料（Transaction Data）
權利主體	• 包含個人（individuals）與法人團體（bodies corporate），即因產品或服務之提供而可透過消費者資料識別或可合理識別該特定人或與該特定人有關聯之人
請求方式	• 「商品資料請求」（Product Data Requests） • 「CDR消費者請求其消費者資料」（Consumer Data Requests Made by CDR Consumers） • 「消費者授權他人請求消費者資料」（Consumer Data Requests Made on Behalf of CDR Consumer）
管理規定	• 資料接受者應通過「澳洲競爭與消費者委員會」（Australian Competition and Consumer Commission, ACCC）認證以符合適格性要求，包括資安措施、爭端解決程序及保險等項目。 • 由政府指定特定行業適用消費者資料權相關規定，即目前的「開放銀行」制度，消費者得要求銀行與經認證資料接受者共享該名請求權人之消費者資料。

「個人資料保護法相關議題」第 9 場產學專家學者諮詢會議—權利限制規定議程

壹、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、瑞士「聯邦個人資料保護法」、美國「加州消費者隱私法」、日本「個人資料保護法」、韓國「個人資料保護法」及新加坡「個人資料保護法」規範內容並於個別討論時，視情況納入廣受討論之外國特別法規範（包含美國「聯邦健康保險流通與責任法案（HIPAA）」及日本「次世代醫療基盤法」），借鏡並擬定我國個資法之法制調適取向，此次討論會議聚焦於我國個資法現有各項權利之權利限制規定。

貳、議程

一、 主席致詞

二、 報告事項

權利限制規定之探討(國發會)

三、 討論事項

我國個資法第 3 條規定，當事人有「查詢或請求閱覽」、「請求製給複製本」、「請求補充或更正」、「請求停止蒐集、處理或利

用」及「請求刪除」等權利。本次討論將上述權利分為「近用權」、「更正權」及「刪除/停止蒐集處理利用權」等三大類，分別與其他國家規範進行比較，並提出以下三項案由。

案由一、近用權之權利限制

說明：

我國個資法第 10 條規定，公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本，該條但書並訂定 3 種限制權利行使之要件，若有以下情形，公務或非公務機關可以不答覆查詢、提供閱覽或製給複製本：

1. 妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

2. 妨害公務機關執行法定職務。

3. 妨害該蒐集機關或第三人之重大利益。（依個資法施行細則第 18 條規定，此處之第三人重大利益指有害於第三人個人之生命、身體、自由、財產或其他重大利益。）

比較其他國家個資保護規範中關於近用權之權利限制要件，可概分為：「國家利益」、「公共安全或秩序維護」、「司法或訴訟程序」、「公務機關法定職務、非公務機關法定義務或其他法律規定」、「當事人或第三人重大利益」、「公務或非公務機關之利益或業務」、「專業倫理考量」、「新聞」、「考試」、「特定資料類別」、「成本或執行可能性」、「權利行使之頻率」、「權利行使合理性」及其他等類別。與我國相關規定較有顯著差異者，為以下三項：

1. 部分國家(如歐盟、德國、英國、瑞士、美國、日本等)將「公共安全或秩序維護」及「司法或訴訟程序」列入近用權限制，我國則未將其納入。但公共安全、秩序維護、司法權之行使等，或可解釋為「公務機關執行法定職務」之一種。

2. 英國、美國、日本、韓國及新加坡等國，針對特定資料或業務型態，如：考試業務、新聞業務、健康資料、教育資料、兒童虐待資料、家戶裝置資料及非商業活動資料等之近用，有限制規定。我國個資法並無此類規定，但可能在特別法中有規定（如兒童及少年福利與權益保障法等）。

3. 美國、新加坡等國考量資料之執行成本或避免權利濫用，規定可以基於重複申請或請求不合理等事由，限制當事人之近用，或對於近用權、訂有免費行使頻率之限制。

小結：根據以上觀察，請專家學者就以下議題提供建議：

1. 針對公共秩序維護、警察權行使、司法訴訟相關業務等，我國是否有必要明定為近用權之限制要件？

2. 針對特定資料類型（如兒童虐待資料等）或業務型態近用權之限制，是否均適合規定於個資法？

3. 是否有必要限制近用權行使方式或頻率？

案由二、更正權之權利限制

說明：

我國個資法對於個人資料更正權，依第 11 條第 1 項規定，公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。針對更正權的行使，我國未規定權利限制要件。

觀察國際立法例，有部分國家訂有更正權之限制要件。其中，日本僅規定在有其他法律限制的狀況下，得拒絕更正權之行使，此應為法律解釋之必然結果。歐盟 GDPR 則列出得由會員國立法之限制要件。而英國個資法於第 26 條及附件二、三對於更正權則訂有多項限制規定，美國加州消費者隱私保護法及新加坡個資法亦同。

小結：根據以上觀察，請專家學者就以下議題提供建議：

「維持個資正確性」為各國個資保護規範共通之原則，除英國、美國加州及新加坡外，各國普遍未限制更正權之行使。依我國更正權行使之實務經驗，是否有增訂限制權利行使要件之需要？

案由三、刪除/停止蒐集處理利用權之權利限制

說明：

刪除或停止蒐集處理利用為一種當事人對於資料蒐集後的

事後控制權利。綜觀各國個資保護規範，除同意之撤回外，其他對於個資事後控制以停止利用或刪除之規定，大致上可分為以下三類狀況：

(一) 針對特定的個資利用方式請求刪除或停止蒐集處理利用

於公務或非公務機關對個資進行某些特定方式的運用時，規定當事人針對該種狀況，得請求停止運用或刪除的權利。

1. 當事人權利行使要件

目前，我國、歐盟（以及與其規範近乎相同之英國、德國）、美國（包含加州消費者隱私法及聯邦健康保險流通與責任法案）及日本（包含個資法及次世代醫療基盤法）皆有針對特定個人資料利用之方式，賦予當事人可以請求停止蒐集處理利用或刪除其個人資料之權利。

我國則於個資法第 20 條規定，非公務機關利用當事人資料進行行銷時，當事人得要求停止利用其個資行銷。

2. 權利限制要件

在權利限制要件上，歐盟針對與學術研究相關以及與未成年人保護相關兩個權利行使，有限制規定。簡要分述如下：

於基於科學、歷史研究或統計目的利用個資時，如資料之控管者可證明該統計或研究係基於公共利益執行職務，得不停止蒐集處理利用個人資料。

另外，為提供未成年人資訊社會服務利用個資時，可基於以下原因，不停止蒐集處理利用個人資料：言論、資訊自由；遵守法定義務；基於公共利益執行職務、受託行使公權力；基於公共衛生之公益目的由專業人員操作或採取適當安全措施；基於公共利益目的之建檔、科學或歷史研究、統計且退出會嚴重妨害目的達成；建立、行使或防禦法律上請求。德國並進一步規定，若刪除將涉及不成比例的努力或不可行，得以限制處理替代。

(二) 針對特定蒐集處理利用合法要件請求刪除或停止蒐集處理利用

於公務或非公務機關以某些特定要件蒐集個人資料之狀況，規定當事人得提出異議，請求停止蒐集處理利用或刪除其個人資料。

1. 當事人權利行使要件

目前，我國、歐盟（以及與其規範近乎相同之英國、德國）及新加坡皆有賦予當事人針對特定的蒐集合法要件，提出異議，要求停止蒐集處理利用或刪除之規定。

我國個資法第 19 條第 1 項第 7 款、第 2 項規定，非公務機關依「取自一般可得來源」蒐集一般個人資料時，如果禁止使用該個資對當事人顯然有更值得保護之重大利益時，當事人可請求刪除、停止處理或利用該個資。

歐盟則針對基於（1）公共利益執行職務或受託執行公權力；（2）正當利益等 2 個條件所蒐集的資料，賦予當事人異議、請求停止蒐集處理利用之權利。

新加坡個資法則規定，以「視為同意」蒐集個資之情形，賦予當事人「撤回同意」之權限。

2. 權利限制要件

我國個資法對於第 19 條第 1 項第 7 款、第 2 項，無權利行使限制規定。

歐盟則規定若資料控管者可以證明其對此一資料的處理，有「具說服力的正當利益」（compelling legitimate interests），或係涉及與司法訴訟及相關權利主張或答辯等事宜，則可以拒絕當事人行使權利。

新加坡則規定一旦當事人提出申請，就應該要停止該個資的蒐集處理利用，並無權利限制規定。

(三) 一般性請求停止蒐集處理利用或刪除個資

與上述針對特定的個資蒐集情境或特定的個資運用情境不同，此一類型係一般性的賦予當事人請求停止蒐集處理利用或刪除之規定。

1. 當事人權利行使要件

目前，我國、歐盟（以及與其規範近乎相同之英國、德國）、美國加州、日本及韓國皆有賦予當事人一般性對於個人資料要求停止蒐集處理利用或刪除的規定。

我國主要規定於個資法第 11 條第 2 項至第 4 項，內容包含：

- 第 2 項規定：對個人資料正確性有爭議時，當事人可請求停止處理或利用；但因執行職務或業務所必須，或經當事人書面同意，並註明其爭議者可不停止處理或利用。
- 第 3 項規定：個人資料蒐集之特定目的消失或期限屆滿後，當事人可請求刪除、停止處理或利用該個資；但因執行職務或業務所必須，或經當事人書面同意者，得不停止處理利用或刪除。
- 第 4 項規定：個人資料蒐集、處理或利用違反個資法規定，當事人可請求刪除、停止蒐集處理或利用個人資料。

2. 權利限制要件

在權利限制要件上，許多國家對於當事人請求停止蒐集處理利用或刪除個資，都有限制之規定。其內容大致可分類如下：

- 法律規定、法定職務或義務要求：我國、歐盟、美國加州（限於直接向當事人蒐集之個資）、韓國（可請求停止蒐集處理利用及刪除）。
- 言論自由、資訊自由：歐盟、美國加州（限於直接向當事人蒐集之個資）。
- 契約履行、合理預期之商務運用、維護基本服務等：美國加州（直接向當事人蒐集之個資或敏感性個資皆可）、韓國（限於請求停止蒐集處理利用）。
- 公共衛生、科學或歷史研究、統計、建檔等：歐盟、

美國加州（限於直接向當事人蒐集之個資）。

- 難以刪除或成本過鉅：德國、日本、美國加州（限於直接向當事人蒐集之個資）。
- 其他：司法訴訟（歐盟）、主管機關許可（美國加州限於敏感性個資）、防止他人權利侵害（韓國，但限於請求停止蒐集處理利用）。

綜觀上述各國對於刪除、停止蒐集處理利用權利限制要件之規定，以下三項特別值得注意：

1. 歐盟對學術研究之特別安排：歐盟規定學術研究為停止蒐集處理利用之權利行使要件，但同時也是刪除權的權利限制要件。

2. 我國與歐盟對當事人權利保護衡平之差異：我國個資法規定只有在當事人權利需要保護時才可以請求刪除或停止處理、利用個人資料；但歐盟則是要求控管者須證明其利用相較於當事人權利更需要保護。

3. 德國、美國及日本將刪除難以執行、成本過鉅等因素納入刪除權限制要件；但德國、日本要求採取替代措施（如停止利用），美國則無採取替代措施之規定。目前，確實有部分科技之應用（如分散式帳本技術），會使記載之資料難以刪除。

小結：根據以上觀察，請專家學者就以下議題提供建議：

1. 歐盟雖允許當事人請求於一定條件下停止將資料應用於學術研究，但限制當事人行使刪除權。此種資料保護與學術研究之衡平方式，是否值得我國參酌？

2. 相較於我國要求於「當事人更需要保護」時，才可以停止利用，歐盟則是「控管者更需要利用」才可以不停止利用。此二種對資料控管者與當事人衡平的作法，何者較適合？

3. 部分資訊技術可能使資料難以或無法刪除，我國是否有需要參考他國規定，允許改採停止處理利用等其他措施？

4. 我國刪除權等事後控制權之限制措施，是否有其他須調整事項？

權利限制規定

國家發展委員會
111 年 6 月 20日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	規範主體、行為區分與特定目的之解釋	可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6	111/5/20	111/6/20			

2

大綱

一 討論範圍

二 近用權之權利限制

三 更正權之權利限制

四 刪除/停止蒐集處理利用權之權利限制

五 附件

3

一、討論範圍（1/2）

■ 討論範圍

以「權利限制規定」為主軸，討論當事人不同權利之限制類型，並以「個資法」為主要討論範疇（但於刪除/停止處理利用權時，兼及重要部門性規範），有關個案規範或個資主管機關規範模式，則於其餘場次討論。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
瑞士	聯邦個人資料保護法	2021	GDPR適足性認定（指令時代取得）
美國	加州消費者保護法（CCPA）	2018	CBPR成員
日本	個人資料保護法	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員

4

一、討論範圍（2/2）

■ 我國現有權利種類

個人資料保護法

第3條

當事人就其個人資料依本法規定行使之下列權利，不得預先拋棄或以特約限制之：

一、查詢或請求閱覽。
二、請求製給複製本。
三、請求補充或更正。
四、請求停止蒐集、處理或利用。
五、請求刪除。

近用權

更正權

刪除/停止蒐集處理利用權

國家發展委員會

5

大綱

一 討論範圍

二 近用權之權利限制

三 更正權之權利限制

四 刪除/停止蒐集處理利用權之權利限制

五 附件

國家發展委員會

二、近用權之權利限制
（一）我國規範

6

個人資料保護法	個人資料保護法施行細則
第10條 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，答覆查詢、提供閱覽或製給複製本。但有下列情形之一者，不在此限： 一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。 二、妨害公務機關執行法定職務。 三、妨害該蒐集機關或第三人之重大利益。	**第18條** 本法第10條但書第3款所稱妨害第三人之重大利益，指有害於第三人個人之生命、身體、自由、財產或其他重大利益。

二、近用權之權利限制
（二）各國規範比較（1/2）

7

部分可解釋為法定職務的一部分

限制要件	國家利益	公安/秩序	司法/訴訟	職務/義務/他法	重大利益	其他 →次頁補充整理
我國	O			O	O	機關利益
歐盟*	O	O	O	O	O	專業倫理
德國	O	O	O	O	O	專業倫理、成本
英國	O	O	O	O	O	保密、特定資料、新聞、研究、考試、稅務、移民、藝術
瑞士	O	O	O	O	O	新聞
美國	X（州法）	O	O	O	O	頻率限制、特定資料、成本、不合理請求
日本	O	O	O	O	O	機關業務、特定資料、審查公正性
韓國	O	O		O	O	考試、補償撫慰金申請
新加坡			O含仲裁	O		考試、信託、內部評估、商業機密、重複申請、不合理請求

 *歐盟僅規範得限制之要件，具體要件須由各會員國自行規定

二、近用權之權利限制
（二）各國規範比較（2/2）

8

考量執行成本/避免濫用

其他限制要件	機關利益/業務	專業倫理	新聞	考試	特定資料	成本/可能性	頻率/重複	不合理請求	其他
我國	O								
歐盟*		O							
德國		O							
英國			O	O	O				研究、稅務、移民、藝術
瑞士			O						
美國					O	O	免費頻率限制	O	
日本	O				O				影響審查公正性
韓國				O					補償撫慰金申請
新加坡	O			O	O		O	O	

各國依照資料或業務敏感程度，個別規定。
如：英國限制健康資料、教育資料、兒童虐待資料之近用
美國限制家戶裝置資料及非商業活動資料等

 *歐盟僅規範得限制之要件，其體要件須由各會員國自行規定

二、近用權之權利限制
（三）討論議題

9

Q

1. 針對公共秩序維護、警察權行使、司法訴訟相關業務等，我國是否有必要明定為近用權之限制要件？（例如非公務機關是否可以主張司法訴訟而拒絕近用）
2. 針對特定不適合給予當事人知悉之資料類型（如兒童虐待資料等）或業務型態，是否均適合規定於個資法？
3. 是否有必要限制近用權行使方式或頻率？

10

大綱

一 討論範圍

二 近用權之權利限制

三 更正權之權利限制

四 刪除/停止蒐集處理利用權之權利限制

五 附件

11

三、更正權之權利限制

（一）我國規範及各國規範比較

個人資料保護法

第11條第1項
公務機關或非公務機關應維護個人資料之正確，並應主動或依當事人之請求更正或補充之。

- 各國規範比較

限制要件	國家利益	公安/秩序	司法/訴訟	職務/義務/他法	重大利益	其他
我國						
歐盟*	O	O	O	O	O	
德國						
英國	O	O	O	O	O	特定資料、新聞、研究、考試、稅務、移民、藝術
瑞士						
美國		O	O	O	O	特定資料、成本、不合理請求
日本				其他法律規定		
韓國						
新加坡			O含仲裁			考試、信託、內部評估、推論出之資料

 *歐盟僅規範得限制之要件，具體要件須由各會員國自行規定

三、更正權之權利限制
（二）討論議題

12

Q

「維持個資正確性」為各國個資保護規範共通之原則，除英國、美國加州及新加坡外，各國普遍未限制更正權之行使。依我國更正權行使之實務經驗，是否有增訂限制權利行使要件之需要？

大綱

13

一 討論範圍

二 近用權之權利限制

三 更正權之權利限制

四 刪除/停止蒐集處理利用權之權利限制

五 附件

國家發展委員會

四、刪除/停止蒐集處理利用權之權利限制

14

（一）我國規範

個人資料保護法	個人資料保護法施行細則
第11條第2項~第4項 個人資料正確性有爭議者，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。 個人資料蒐集之特定目的消失或期限屆滿時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。 違反本法規定蒐集、處理或利用個人資料者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。 **第19條第2項（非公務機關）** 蒐集或處理者知悉或經當事人通知依前項第七款但書*規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。 *個人資料取自於一般可得之來源，但當事人對該資料之禁止處理或利用，顯有更值得保護之重大利益者，不在此限。 **第20條第2項（非公務機關）** 非公務機關依前項規定利用個人資料行銷者，當事人表示拒絕接受行銷時，應即停止利用其個人資料行銷。	**第21條** 有下列各款情形之一者，屬於本法第十一條第三項但書所定因執行職務或業務所必須： 一、有法令規定或契約約定之保存期限。 二、有理由足認刪除將侵害當事人值得保護之利益。 三、其他不能刪除之正當事由。

國家發展委員會

四、刪除/停止蒐集處理利用權之權利限制

15

（二）刪除/停止蒐集處理利用權的類型化

類型 / 國家	1. 針對特定個資利用方式請求刪除或停止處理利用	2. 針對特定蒐集處理利用合法要件請求刪除或停止處理利用	3. 一般性請求停止利用或刪除個資
我國	■ 非公務機關行銷	■ 非公務機關+個資取自一般可得來源	■ 正確性爭議 ■ 特定目的消失、期限屆滿 ■ 違法運用
歐盟、英、德	■ 行銷 ■ 科學、歷史研究、統計 ■ 未成年人資訊社會服務	■ 因公共利益執行職務或受委託行使公權力 ■ 正當利益	■ 特定目的無必要（被遺忘權） ■ 非法處理 ■ 法律要求 ■ 正確性爭議
美國CPRA	■ 販賣 ■ 跨情境行為廣告分享	無	■ 自消費者處取得之個資 ■ 敏感性個資
美國HIPAA	■ 募款活動	無	無
日本個資法	■ 以「有效通知、通報主管機關」方式提供個資給第三人	無	■ 事故、違法運用、可能侵權 ■ 已無利用必要（被遺忘權）
日本次世代醫療基盤法	■ 以「有效通知、主管機關許可」方式提供個資給匿名加工業者匿名加工	無	無
韓國	無	無	■ 一般性停止利用或刪除
新加坡	無	■ 視為同意	無

國家發展委員會

四、刪除/停止蒐集處理利用權之權利限制 16

類型1: 針對特定個資利用方式

	權利行使要件	權利限制要件	效果
我國	非公務機關、行銷（20）		停止利用
歐盟、英、德	行銷	歐盟一般限制要件	停止蒐集處理利用
	科學、歷史研究及統計	為公共利益執行任務、歐盟一般限制要件	停止蒐集處理利用
	未成年人資訊社會服務	言論自由、資訊自由；法定職務或義務；法律規定；公共衛生公益目的；公益目的建檔、科學、歷史研究、統計；司法訴訟相關 歐盟一般限制要件	刪除
	單純自動化決策處理（禁令，非權利類型）		
美國CPRA	販賣或跨情境行為廣告*分享個資（16歲以下opt-in）		停止蒐集處理利用
美國HIPAA	募款活動		停止蒐集處理利用
日本個資法	以「將法定告知事項告知本人（或置於本人得知悉狀態），且向個資委員會申報」為由將個資提供給第三人		停止蒐集處理利用
日本次世代醫療	以「將法定告知事項告知本人，且經主管機關許可」為由將個資提供匿名加工業者匿名化		停止蒐集處理利用

德國：若刪除不可行可改為限制處理

*跨情境行為廣告：消費者並未有意與特定業者互動並提供個資，但該業者運用用戶追蹤之方式，鎖定消費者投放廣告

四、刪除/停止蒐集處理利用權之權利限制 17

類型2: 針對特定蒐集處理利用合法要件

	權利行使要件	權利限制要件	效果
我國	非公務機關+資料取自一般可得來源 + **當事人有更值得保護利益（19）**		刪除、 停止處理利用
歐盟、英、德	公共利益執行職務或委託行使公權力 正當利益	資料控管者對資料有「**具說服力的正當利益**」或司法訴訟、司法請求有關 歐盟一般限制要件	刪除、 停止蒐集處理利用
新加坡	視為同意*		停止蒐集處理利用

我國與歐盟在資料價值與當事人權利保護之平衡點取捨有差異

*視為同意包含新加坡個資法附件一、二情形：符合當事人切身利益、影響公共事項、合法利益、商業交易目的、商業改進目的、公共利益研究等（此種情形下當事人可撤回同意）

四、刪除/停止蒐集處理利用權之權利限制

18

類型3: 一般性請求停止蒐集處理利用或刪除個資（1/2）

	權利行使要件	權利限制要件	效果
我國	正確性爭議（11 II）	書面同意or執行業務或職務必須	停止處理利用
	特定目的消失or期限屆滿（11 III）	書面同意or執行業務或職務必須	刪除、停止處理利用
	非法蒐集處理利用（11 IV）		刪除、停止蒐集處理利用
歐盟、英、德	特定目的無必要（被遺忘權）	言論自由、資訊自由；法定職務或義務；法律規定；公共衛生公益目的；公益目的建檔、科學、歷史研究、統計；司法訴訟相關。 歐盟一般限制要件 德國：若刪除不可行可改為限制處理	刪除、停止蒐集處理利用
	非法處理		
	法律要求		
	正確性爭議	歐盟一般限制要件	停止蒐集處理利用
美國CPRA	自消費者處蒐集之個資（1789.105）	完成蒐集目的之交易、履行契約、依法召回、提供服務必須、維持商業或契約；確保安全及完整性；確保服務安全；言論自由；法律規定/義務；經知情同意、同儕審查或公益目的之科學、歷史、統計研究；符合期待的內部使用；**不可能刪除或耗費過鉅**	刪除
	敏感性個資（1798.121(a)）	提供服務商品必要、提供特定法定服務、主管機關許可	刪除
日本	事故、可能侵權（35）	非公務機關：**成本過高或有困難+採取必要替代措施** 公務機關：他法另訂特別程序、法定事務執行	刪除、停止蒐集處理利用
	非法處理（35、98）		
	已無利用必要（35）		
韓國	一般性刪除權（36）	其他法律禁止	刪除
	一般性停止利用權（37）	法定義務/職務；危害他人生命、身體、財產或其他利益；契約履行	停止蒐集處理利用

四、刪除/停止蒐集處理利用權之權利限制

19

類型3: 一般性請求停止蒐集處理利用或刪除個資（2/2）

- 權利限制要件的類型化分析
  - **法律規定、法定職務或義務要求：**
    我國、歐盟、美國加州（直接蒐集）、韓國（停止蒐集處理利用、刪除）
  - **言論自由、資訊自由**：歐盟、美國加州（直接蒐集）
    - 原係為平衡被遺忘權效果
  - **契約履行、合理預期之商務運用、維護基本服務等：**
    美國加州（直接蒐集、敏感個資）、韓國（停止蒐集處理利用）
    - 或許係因退出要件較為寬鬆
  - **公共衛生、科學或歷史研究、統計、建檔等：**
    歐盟、美國加州（直接蒐集）
    - 賦予學術研究特殊地位
  - **難以刪除或成本過鉅：**
    德國、美國加州、日本
  - **其他**：司法訴訟（歐盟）、主管機關許可（美國加州敏感性個資）、防止他人權利侵害（韓國停止蒐集處理利用）

四、刪除/停止蒐集處理利用權之權利限制
（三）小結

20

- **歐盟對學術研究之特別安排：**
  學術研究為停止處理利用之權利行使要件；
  也是刪除權的權利限制要件。
- **我國與歐盟對當事人權利保護衡平之差異：**
  我國：由當事人證明其更需要保護
  歐盟：控管者須證明其利用更需保護
- **刪除之可能性：**
  德國、美國及日本將刪除難以執行*、成本過鉅等因素納入刪除權限制要件；但德國、日本要求採取替代措施（如停止利用）
  * 例如：**分散式帳本**等技術

四、刪除/停止蒐集處理利用權之權利限制
（四）討論議題

21

Q

1. 歐盟雖允許當事人請求於一定條件下停止將資料應用於學術研究，但限制當事人行使刪除權。此種資料保護與學術研究之衡平方式，是否值得我國參酌？
2. 相較於我國要求於「當事人更需要保護」時，才可以停止利用，歐盟則是「控管者更需要利用」才可以不停止利用。此二種對資料控管者與當事人衡平的作法，何者較適合？
3. 部分資訊技術可能使資料難以或無法刪除，我國是否有需要參考他國規定，允許改採停止利用等其他措施？
4. 我國刪除權等事後控制權之限制措施，是否有其他須調整事項？

22

討論議題

案由一、近用權之權利限制

- 針對公共秩序維護、警察權行使、司法訴訟相關業務等，我國是否有必要明定為近用權之限制要件？（例如非公務機關是否可以主張司法訴訟而拒絕近用）
- 針對特定不適合給予當事人知悉之資料類型（如兒童虐待資料等）或業務型態，是否均適合規定於個資法？
- 是否有必要限制近用權行使方式或頻率？

案由二、更正權之權利限制

- 「維持個資正確性」為各國個資保護規範共通之原則，除英國、美國加州及新加坡外，各國普遍未限制更正權之行使。依我國更正權行使之實務經驗，是否有增訂限制權利行使要件之需要？

案由三、刪除/停止處理利用權之權利限制

- 歐盟雖允許當事人請求於一定條件下停止將資料應用於學術研究，但限制當事人行使刪除權。此種資料保護與學術研究之衡平方式，是否值得我國參酌？
- 相較於我國要求於「當事人更需要保護」時，才可以停止利用，歐盟則是「控管者更需要利用」才可以不停止利用。此二種對資料控管者與當事人衡平的作法，何者較適合？
- 部分資訊技術可能使資料難以或無法刪除，我國是否有需要參考他國規定，允許改採停止利用等其他措施？
- 我國刪除權等事後控制權之限制措施，是否有其他須調整事項？

23

大綱

一 討論範圍
二 近用權之權利限制
三 更正權之權利限制
四 刪除/停止蒐集處理利用權之權利限制
五 附件

歐盟相關規定（1/2）

最近一次個資法修正：2016年（2018年施行）

權利限制	國內法限制+尊重基本權利與自由+必要性+比例性
可受限制之權利	近用權、更正權、刪除權、限制處理權、可攜權、拒絕權
限制事由	1. 國家安全 2. 國防 3. 公共安全 4. 刑事犯罪相關事項 5. 歐盟及成員國之經濟利益 6. 司法 7. 專業行業之倫理規範相關事項 8. 執行公務機關之監督、調查、執法職務 9. 保護資料主體或第三方之權利與自由 10. 民事案件之執行

歐盟相關規定（2/2）

最近一次個資法修正：2016年（2018年施行）

限制事由應有法律依據，法律內容應包含：

1. 資料處理之目的或資料處理之類型
2. 個人資料之種類
3. 權利限制之範圍
4. 防止濫用或非法存取或傳輸之措施
5. 明列資料控管者或資料控管者之種類
6. 資料保存期限，及所採取的適當安全措施
7. 資料主體權利及自由的風險
8. 賦予資料主體有被告知權利限制之權利

英國相關規定（1/2）

26

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

UK GDPR		
§23	可能被限制之權利	第 12 條至第22條
	權利限制要件	(1)內閣大臣（The Secretary of State）以立法程序為之 (2)立法符合第12條至第22條所定權利與義務 (3)尊重基本權及自由之本質 (4)民主社會中必要且適當 (5)確保下列目的： (c)公共安全、(d)預防、調查、偵查及追訴犯罪或執行刑罰、(e)一般公共利益的其他重要目標（財政、預算及稅、公共衛生及社會安全）、(f)司法獨立性及司法程序之保障、(g)預防、調查、偵查及追訴違反特定職業之道德規範、(h)公務機關行使其監督、檢查或監管功能、(i)保護資料主體或他人之權利及自由之保障、(j)民事執行
§85(2)	可能被限制之權利	第三章（資料主體之權利）
	權利限制要件	(1)基於新聞目的或學術、藝術或文學表意目的所為之處理 (2)為平衡個人資料保護及表意及資訊自由權利而有必要

英國相關規定（2/2）

27

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

DPA 2018 §15及其附件：UK GDPR的權利豁免的細則規定

DPA 2018		
	被限制之情狀	可能被限制之權利
附件二	(1)犯罪、稅務、移民 (2)維持公眾保護功能、監察功能等公共機能 (3)衛生、社會、教育工作者進行數據測試時 (4)其他如：法律專業特權、自證其罪、企業融資等情狀 (5)新聞、學術、藝術、文學等與表意自由相關 (6)研究、統計、公益目的之歸檔	(1)UK GDPR §13~21 (2)UK GDPR §13~21 (3)UK GDPR §15(1)~(3) (4)UK GDPR §13~15 (5)UK GDPR §13~21 (6)UK GDPR §15~16、§18~21
附件三	以資料性質做限制（如健康資料、教育資料）	UK GDPR §13~18、§20~21
附件四	被英國其他法律禁止或限制的資料公開揭露情況（如人類受精和胚胎資訊）	UK GDPR §15(1)~(3)
第26條	國家安全與防衛目的	UK GDPR CH3（資料主體之權利）

13：告知（直接蒐集） 14：告知（間接蒐集） 15：近用權 16：更正權 17：刪除權
18：限制處理權 19：刪除之通知 20：可攜權 21：拒絕權

德國相關規定

28

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

權利限制類型	BDSG
個資蒐集當事人應被告知之權利	直接蒐集：進階處理之利益可被視為微乎其微、法定職務必要、公共安全秩序、司法訴訟、公務機密性資料 間接蒐集：(1)公部門-法定職務必要、公共安全秩序、國家安全；(2)私部門-司法訴訟、公共安全秩序
近用權	司法訴訟、公共安全秩序、國家安全、法定保留紀錄不得刪除時
刪除權	非自動化個資處理情形因特定儲存模式極難刪除、當事人對刪除之利益可被視為微乎其微、與法規或契約之保留期限相衝突、對當事人之合法利益產生不利影響、司法訴訟必要
拒絕權	大於當事人利益之急迫性公共利益、基於法令
自動化決策與分析的權利	基於申請醫療保險金且已採取適當措施應保留人工干預之權利

瑞士相關規定

29

最近一次個資法修正：2020年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

知情權之限制	一般規定（§26）	• 資料控管者得向當事人拒絕或限制、延遲提供資訊之特定條件包括： 1. 依法律規定，如履行保密義務 2. 為保護第三方之重大利益 3. 當該請求並無根據可能違反資料保護或明顯有爭議 • 聯邦機構得向當事人拒絕或限制、推遲提供資訊之特定條件包括： 1. 基於重要公共利益以及國家安全 2. 基於可能嚴重影響司法調查程序 • 拒絕或限制、延遲提供時，必須向當事人說明原因 • 當特定條件消失，應盡速提供予當事人
	對新聞媒體之特別規定（§27）	• 新聞記者身為資料控管者得向當事人拒絕或限制、延遲提供資訊之特定條件包括： 1. 個人資料可能揭露資訊來源 2. 已向當事人提供報導初稿 3. 公開發表意見之自由可能受到損害 4. 當個人資料僅是用於作為工作輔助時
可攜權之限制	一般規定（§29）	• 資料控管者得向當事人拒絕或限制、延遲轉移之特定條件包括： 1. 依法律規定，如履行保密義務 2. 為保護第三方之重大利益 • 拒絕或限制、延遲提供時，必須向當事人說明原因

30

美國相關規定（1/2）

無聯邦個資法，加州消費者隱私法（ CCPA）最近修正為 2018年，修正 CCPA 的新法 CPRA 將於 2023年實施，效力溯及 2022 年 1 月 1 日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

CCPA&CPRA權利類型	個別權利限制規定			一般權利限制規定
刪除權	• 須為**可驗證的消費者請求** • 可因法遵、其他法定目的保留一份刪除請求的機密紀錄 • 無義務刪除：基於契約以達成契約目的、確保安全性和完整性的合理必要使用、除錯、確保其他消費者言論自由或其他法定權利、加州法遵、知情同意之研究、合理之內部使用、履行法定義務（*CPRA§1798.105*） • 不適用依法規所持有學生、教育成績（*§1798.145(q)*） • 不適用當事人已同意的高成本實體產出，如有照片的學校年冊（*§1798.145(r)*）		不適用家戶裝置資料	課予營利事業之義務不應限制下列事項： • 聯邦、州、當地法遵 • 法院令狀要求提供資訊 • 政府機關之民刑行政監管要求、調查、傳票、傳喚 • 善意相信潛在違法行為與執法機構合作 • 生命身體緊急危險 • 法律權利行使、防禦 • 其他消費者自由與權利 • 個資已去識別或匯總化 • 排除個資類型：勞雇情境的應徵資訊、應徵之緊急聯絡資訊(但企業須通知蒐集之資訊)；工作上溝通之資訊(但員工仍可退出販售或分享) • 不及於非商業活動 • 其他法定事由（*§1798.145*）
更正權	• 須為**可驗證的消費者請求**（*§1798.106*）			
知的權利	**知悉蒐集之資料與資訊近用（*§1798.110*）** • 須為**可驗證的消費者請求** • 頻率限制：1次/12個月	**知悉被販售、共享之資料、販售共享對象（*§1798.115*）** • 頻率限制：1次/12個月		
退出販售或分享權	• 無特殊限制（*§1798.120*）			
限制敏感個資使用權	• 無特殊限制（*§1798.121*）			
不因退出/行使權利受報復權	• 無特殊限制（*§1798.125*）			

國家發展委員會

31

美國相關規定（2/2）

無聯邦個資法，加州消費者隱私法（ CCPA）最近修正為 2018年，修正 CCPA 的新法 CPRA 將於 2023年實施，效力溯及 2022 年 1 月 1 日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），預計明年在各州提案。
CBPR成員國

UPDPA權利類型	個別權利限制規定	一般權利限制規定
請求複製本（知的權利）	• 頻率限制：12個月內免費提供一份複製本 • 費用限制：於超過一份的數量可收取合理行政費用（*UPDPA§5*）	• 不適用公開可得的資料 • 不適用符合保護人體受試者法規之人體試驗研究所處理或保有之資料 • 不適用法院令狀、命令或其他法律允許、要求處理或揭露之資料 • 依據政府資料公開法規須公開之資料 • 於資料當事人受雇或應徵期間處理或保有之資料*UPDPA§3(c)*
更正權	• 控管者有理由相信資料當事人的更正請求不精確、不合理或過度者，控管者有權不更正，並須向資料當事人說明（*UPDPA§5(a)(5), (6)*）	
不因行使權利受報復的權利	• 無特殊限制（*UPDPA§5 (c)*）	

國家發展委員會

日本相關規定（1/2）

32

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

權利類型	對象	限制事由
揭露權	非公務機關（§33II）	• 有損害於本人或第三人之生命、身體、財產或其他權益之虞者； • 對該個人資料處理事業業務之適當執行，有造成明顯妨礙之虞者； • 構成違反其他法令者。
	公務機關（§78I）	• 有損害於本人或第三人之生命、身體、財產或其他權益之虞者； • 有關法人及其團體，或是經營揭露請求權者以外事業之個人與所營事業相關之特定資料（但不包括保護人之生命、健康、財產必要之資料） • 可能損害國家安全、國際關係不利影響之資料； • 公務機關內部審議、檢討或協議資料，揭露可能不當損及意見交換或中立性； • 公務機關事務資料，揭露對執行事務造成妨礙之虞。
更正權	非公務機關（§34II）	當有其他法令對於更正另訂特別程序時。
	公務機關（§90I）	當有其他法令對於保有個人資料之更正另訂特別程序時。

國家發展委員會

日本相關規定（2/2）

33

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），預計於2022年4月正式施行。
CBPR成員國、GDPR適足性（2019）

權利類型	對象	限制事由
停止利用、刪除權	非公務機關（§35VI）	違反第18（利用目的之限制）、19（不當利用之禁止）、20（適當地蒐集）條 →本人得請求**停止利用或刪除**保有個人資料 個資處理事業認本人之請求**有理由**（第35條第2項） →除非停止利用或刪除成本過高或有困難之情況且已採取必要替代措施，原則上應停止利用或刪除該保有個人資料
	公務機關（§98I、100）	• 當有其他法令對於保有個人資料之停止利用、刪除或停止提供另訂特別程序時； • 因停止利用該保有個人資料，在該保有個人資料的利用目的相關之事務在性質上，可認為對於該當事務的適當執行造成顯著妨礙者。

國家發展委員會

34

韓國相關規定（1/2）

一、韓國PIPA賦予個資當事人的權利保障

- **當事人得行使之權利類型：**

1. PIPA第35條到第37條規定，個資當事人得向公務機關及非公務機關主張：
   1) 閱覽個人資料；
   2) 個人資料的刪除、更正；
   3) 停止處理個人資料。
2. PIPA於第38條權利行使的方法與程序中，規範得以代理的方式為之，又可以細分為「意定代理」及「法定代理」兩種樣態

意定代理	法定代理
得代理人行使PIPA第35條到第37條有關個資當事人權利，不必本人親自為之。	PIPA於第38條第2項明定14歲以下未成年人之法定代理人，可向資料處理者對該兒童之個資提出閱覽等要求。

35

韓國相關規定（2/2）

二、韓國PIPA有關「權利限制」的原則及例外

- 依照PIPA第五章個資當事人得行使權利之原則及例外整理如下：

當事人權利	原則	例外
閱覽個人資料（第35條）	1. 非公務機關：得向資料處理者要求閱覽其個人資料。 2. 公務機關：得直接或透過保護委員會要求閱覽。	1. 法律明文禁止或限制閱覽時； 2. 有危害其他人之生命、身體、財產及其他利之虞時； 3. 公務機關於執行法定職務時。
更正、刪除個人資料（第36條）	收到要求後，應立即調查後為更正或刪除。並將調查結果告知當事人，並應有使該資料不至於被回復或重製之措施。	若個資當事人為其他法令明定之蒐集對象時，則例外不得要求更正。
停止處理個人資料（第37條）	1. 非公務機關：資料處理者應立即依其要求，停止處理個人資料。 2. 公務機關：停止範圍僅限於PIPA第32條 所規定之資料。	符合法定要件得例外拒絕： 1. 法律規定或為法定義務； 2. 危害他人生命、身體、財產及其他利益之虞； 3. 公務機關執行法定職務； 4. 恐致債務不履行風險，當事人未表明解除契約之意思。

36

新加坡相關規定（1/3）

最近一次個資法修正：2020年
CBPR成員國

近用權（Access to personal data）
應個人要求，組織必須盡快向個人提供組織擁有或控制之有關個人之個人資料；以及在請求日期前一年內個人資料可能已被組織利用或揭露方式之資訊。（PDPA第21條）

例外限制－以下情形，組織得拒絕提供資料：
- 僅用於評估目的的意見資料；
- 由教育機構進行的任何考試、試卷以及在考試成績公佈前的考試成績；
- 私人信託受益人的個人資料，僅用於管理信託；
- 由仲裁機構或調解中心保存的個人資料，僅用於仲裁機構或調解中心管理的仲裁或調解程序；
- 司法檢調程序尚未完成之文件；
- 受法律特權約束的個人資料；
- 個人資料若揭露將洩露商業機密，且可能會損害組織的競爭地位；
- 依據PDPA附表1規定未經同意蒐集、利用或揭露的個人資料，用於調查目的，惟調查和相關訴訟程序尚未完成；
- 由調解員或仲裁員在進行調解或仲裁時所蒐集或建置；
- 由於請求的重複性或系統性將不合理地干擾組織的運作；提供存取相關負擔或費用對組織不合理或與個人利益不相稱；不存在或無法找到的資訊；無關緊要的資訊；或者輕率或不合理的請求。

（PDPA附表5）

37

新加坡相關規定（2/3）

最近一次個資法修正：2020年
CBPR成員國

更正權（Correction of personal data）
個人可要求組織更正組織擁有或控管的個人資料中的錯誤或遺漏，除非組織有合理理由認為不應進行更正，否則組織必須盡快更正個人資料。（PDPA第22條）

例外限制－以下情形，組織有合理理由拒絕進行更正：
- 僅用於評估目的的意見資料；
- 由教育機構進行的任何考試、試卷以及在考試成績公佈前的考試成績；
- 私人信託受益人的個人資料，僅用於管理信託；
- 由仲裁機構或調解中心保存的個人資料，僅用於仲裁機構或調解中心管理的仲裁或調解程序；
- 司法檢調程序尚未完成之文件；
- 組織在業務過程中，從該組織擁有或控制之個人或其他個人之其他個人資料中，得出有關該個人之個人資料（derived personal data）。

（PDPA附表6）

新加坡相關規定（3/3）

最近一次個資法修正：2020年
CBPR成員國

撤回同意（Withdrawal of consent）（PDPA第16條）

- 針對該組織基於任何目的所蒐集、利用或揭露有關個人資料，個人在向該組織發出合理通知後，得隨時撤回依本法所給予或被視為之同意。
- 組織接收第1款所述之通知後，該組織必須告知個人撤回其同意之可能後果。
- 組織不得禁止個人撤回對蒐集、利用或揭露個人資料之同意，但本條不影響因撤回同意而產生之任何法律後果。
- 依**本法第25條**，除本法或其他成文法要求或授權未經個人同意而蒐集、利用或揭露之資料外，若個人撤回對組織出於任何目的蒐集、利用或揭露個人資料之同意，該組織必須停止（並使其資料中介和代理人停止）搜集、利用或揭露個人資料。

個人資料之保留（Retention of personal data）（PDPA第25條）

- 若符合下列情形，組織必須停止保留包含個人資料之文件，或刪除該個人資料與特定個人相關聯的方式：蒐集個人資料之目的不再透過保留個人資料實現，且不再需要基於法律或商業目的保留。

「個人資料保護法相關議題」第 10 場產學專家學者諮詢會議—豁免情形、域外效力

議程

壹、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（資料可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「統一個人資料保護法」及「加州隱私權法」（CPRA）、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」、菲律賓「個人資料保護法」及瑞士「個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於豁免情形、域外效力之探討。

貳、議程

一、 主席致詞

二、 報告事項

豁免情形、域外效力之探討(國發會)

三、 討論事項

案由一、豁免情形之探討

說明：

一、 我國個資法規定及實務現況

我國個資法第 51 條第 1 項：「有下列情形之一者，不適用本法規定：一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。」。

其立法理由如下：依修正條文第二條第八款規定，本法所稱非公務機關包括自然人，惟有關自然人為單純個人（例如：社交活動等）或家庭活動（例如：建立親友通訊錄等）而蒐集、處理或利用個人資料，因係屬私生活目的所為，與其職業或業務職掌無關，如納入本法之適用，恐造成民眾之不便亦無必要，爰增訂第一項規定，予以排除。網際網路上張貼之影音個人資料，亦屬表現自由之一部分。為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意…其本身共同使用之合法目的亦相當清楚…不適用本法之規定，回歸民法適用。

而實務見解係根據該行為之目的進行判斷。舉例而言，民眾於公職人員選舉開票作業之公開活動中進行攝影，如僅為單純個人活動目的而蒐集自然人之資料，或僅攝影不特定自然人影像且未與其他個人資料結合時，尚無個資法之適用（法務部 104 年 11 月 5 日法律字第 10403514100 號函參照）。而消防人員於執行緊急救護勤務中所錄存之影音資料若涉及可直接或間接識別特定個人之資料，自有個資法之適用（法務部 106 年 2 月 15 日法律字第 10603502190 號函參照），故並未因可能係公開場所或公開活動之影音資料，而逕引為公務機關（消防機關）豁免適用個資法之依據。

二、 外國相關立法例

綜觀各國法制，可將常見的豁免類型概分政府行為、私人活動或其他私領域行為及基本權競合等三類；針對不同豁免類型可分為全域豁免（例如歐盟 GDPR 第 2 條第 2 項四種豁免情形之一者，整部 GDPR 皆不適用），以及細分為部分豁免之情形。說明如下：

(一) **「政府行為」**主要包含統治行為、公務機關執行公務、刑事案件機關程序、刑事案件或少年保護案件之程序、議會

訴訟程序等。目前許多國家（如歐盟、日本、韓國等）在刑事訴追過程等程序上，因有其他法律調和，故於個資法有豁免。

(二) 「**私人活動或其他私領域行為**」則主要為個人日常活動、單純個人或家庭活動、商業契約或商業活動、民法公開登記、受雇或應徵資料等。在個人家庭活動之部分，幾乎所有國家皆有豁免，較無爭議；受雇應徵資料、或企業內部管理為美國特別強調；商業契約則為新加坡特有規範。

(三) 「**基本權競合**」則有例如新聞媒體或出版自由、宗教自由、政治自由、學術自由、藝術自由等基本權利，該相關權利與隱私權競合。例如歐盟體系特別針對言論自由相關權利（如新聞目的及學術、藝術及或文學表意目的）有部分豁免規定；日、韓等國則有進一步針對宗教、政治等權利給予部分豁免；有關新聞、藝術、文學或研究目的，菲律賓為全域豁免。

(四) **附論：有關公開場所影音資料之管理**

1. 我國個資法第 51 條第 2 項「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」規定，未見於其他國家有相類似之豁免立法例，且條文因缺少規範主體，易滋生豁免主體範圍爭議。前開說明一已見函釋排除豁免基於職業或業務職掌之公開場所或公開活動影音資料蒐集、處理及利用。惟該條款僅係指豁免個資法適用，尚非監視設備之管理規定。

2. 以各國規範觀察之，目前德國、韓國針對監視器規範於個資法中，有訂定「得例外設置」之情形，並針對監視器之設置加強義務。其他國家，如英國規範於《自由保護法》、日本發布「監視器影像利用指引」、美國依判例等，多數國家未明文規範於個資法。

三、 小結

依我國個資法第 51 條立法理由觀之，我國個資法第 51 條第 1 項第 2 款，為我國獨有之張貼表現自由，其本質或可能與我國個資法第 51 條第 1 項第 1 款相似。而我國個資法排除自然人單純為個人活動目的，而各國相較我國，則有更多針對政府行為、

私法行為（如商業契約）、基本權（如言論自由）等之豁免情形。此外，我國個資法無類似公開場所或公開活動錄影監視錄影設備之管理規定。

根據以上觀察，請產學專家就以下議題提供建議：

(一) 現行我國個資法第 51 條第 1 項第 1、2 款之兩款事由是否須整併合一或調整？

(二) 我國是否參考他國模式，針對部分政府行為、私法行為（如調查、商業契約等）、基本權等類型（如言論自由），設立豁免規定？建議納入哪些行為類型？

(三) 我國雖有針對公開場所影音資料之豁免，然而尚未具體針對監視器規範，我國是否適合仿效德國、韓國，納入個資法規範？或於未另為規範前，發布指引？

案由二、域外效力之探討

說明：

一、 我國個資法法律適用效力範圍規範

常見之域外效力有二：(一)「蒐集主體在境外，對境內自然人個資之蒐集處理利用」、(二)「我國蒐集主體在境外，對境外之我國公民個資之蒐集處理利用」之情形。而我國尚未針對未在境內設有實體，但有蒐集、處理、利用我國境內人民個資之情形規範。

二、 我國個資法域外效力規定及實務現況

我國個資法「域外效力」則係規範於第 51 條第 2 項：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」。

本項之立法理由如下：「由於科技之進步與網際網路使用普遍，即使在我國領域外蒐集、處理或利用國人之個人資料，亦非常容易。為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任，爰增訂第二項，明定在我國領域外，亦有本法之適用。」。

實務見解認為個資法第 51 條第 2 項規定，在我國領域外蒐集、處理或利用個人資料行為，須合於下列要件，始有個資法之適用：(一)從事蒐集、處理或利用行為者為我國之公務機關及非公務機關；(二)所蒐集、處理或利用者為我國人民之個人資料(法務部 107 年 3 月 12 日法律字第 10703502240 號函參照)。將我國個資法之域外效力管轄範圍，特有規範境外我國人民，且蒐集主體必須為我國之公務機關或非公務機關之情形。

三、 外國相關立法例

(一) 域外效力

1. 歐盟 GDPR 體系國家(例如德國)、英國、日本、新加坡、瑞士等：

(1) 依據《競爭法》概念，若對市場有產生影響者，皆納入規範管制。故針對提供歐盟境內資料主體產品或服務；涉及監控歐盟境內資料主體之行為。

(2) 主體適用境內設立之控管者或處理者所為之個資處理活動，無論該處理是否發生於境內。

(3) 其對象針對歐盟境內之人，無論當事人國籍。

(4) 日本、新加坡、瑞士等國，其域外效力皆仿效歐盟模式。

2. 美國 CPRA：

(1) 要求營利事業有於加州展開業務，無論營利事業是否實體存在於加州。營利事業的定義延伸到「包括任何控制、或由營利事業控制的實體，並且與營利事業共用品牌名稱、服務標識或商標」，使位於加州境外的實體也可能受到規範。

(2) 對象針對加州居民。

(3) 若消費者資料的蒐集、販售和共享之商業行為皆未發生在加州境內，亦無任何個資為消費者位在加州時所蒐集，則 CPRA 規定將不適用於該資料。

3. 菲律賓

（1） 域外效力範圍較為寬泛，規範涉及菲律賓公民或居民之個人資料。

（2） 運用個人資料之自然人或法人於菲律賓境內，或於境外運用關於菲律賓個人或居民之個人資料，包含但不限於下列情況：在菲律賓簽訂契約；並未設立於菲律賓，但於菲律賓境內有管理和掌控之法人；法人於菲律賓境內有分公司、辦事處、辦公室或子公司，並可近用個人資料。

四、 小結

依據我國個資法第 51 條第 2 項法條結構觀之，僅針對保護我國公民，而我國域外效力管轄範圍，僅針對境外之我國蒐集主體對我國人民個資之蒐集、處理、利用行為。而我國個資法第 51 條第 2 項不宜解讀為類似歐盟 GDPR 第 3 條第 2 項之域外效力。

根據以上觀察，請產學專家就以下議題提供建議：

(一) 我國個資法並無類似歐盟 GDPR 第 3 條第 2 項針對境外實體域外效力規範，是否有納入我國個資法之必要？若採納，應有哪些適用條件？

(二) 現行有規範「針對境外法人或自然人對境內人民之行為」之國家，皆設有專責機關，而我國目前由各主管機關分別管理，若法條納入此類域外效力，是否有需其他配套措施？

豁免情形、域外效力

國家發展委員會
111 年 7 月 25日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	規範主體、行為區分與特定目的之解釋	資料可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6	111/5/20	111/6/20	111/7/25		

2

大綱

一 討論範圍

二 豁免情形之探討

三 域外效力之探討

四 附件

3

一、討論範圍（1/3）

■ 討論範圍

分別討論「豁免情形」、「域外效力」之要件，並以「個資法」為主要討論範疇，前幾場次已討論「學術研究」、「國際傳輸」、「當事人權利限制」等，不在此次討論範圍。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法	2020	歐盟前成員、GDPR適足性（2021）
美國	加州隱私權法（CPRA）	2020	CBPR成員 **統一個資保護法（UPDPA）非實定法律，為統一州法法律委員全國會議為協助統一各州規定而擬定
	統一個人資料保護法（UPDPA）	2021	
日本	個人資料保護法	2021	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員
菲律賓	個人資料保護法	2012	
瑞士	個人資料保護法	2020	GDPR適足性認定（指令時代取得）

一、討論範圍（2/3）

■ 經整理各國豁免情形主要分為：政府行為、私人活動或其他私領域行為、基本權競合等類型。

類型	具體樣態	代表國家
政府行為	統治行為：如外交、國安行為	歐盟GDPR
	刑事案件機關或程序	歐盟GDPR、日本
	特定領域政府活動	英國
	廣泛的政府活動	菲律賓
私人活動或其他私領域行為	私人行為、家庭或個人	我國、歐盟GDPR
	企業內部管理	美國CPRA
	商業契約、商業活動	新加坡
基本權競合	新聞或出版自由	日本、英國
	研究自由	日本、英國
	宗教自由	日本、韓國
	政治自由，如政黨活動	日本、韓國

一、討論範圍（3/3）

■ 所謂「域外效力」，屬於法律適用效力範圍之其中一種規範。
■ 我國個資法適用效力範圍，以下列2個樣態為例討論：

	具體樣態	有無規範
我國個資法適用效力範圍	蒐集主體在境外，對境內自然人個資之蒐集處理利用	×
	我國蒐集主體在境外，對境外之我國公民個資之蒐集處理利用	✓

討論議題將請專家學者依據豁免情形及域外效力之類型進行討論

6

大綱

一 討論範圍

二 豁免情形之探討

三 域外效力之探討

四 附件

7

二、豁免情形之探討
（一）我國個資法規定及實務現況（1/2）

■ **我國個資法豁免**

1. **單純個人或家庭活動之目的**，而蒐集、處理或利用個人資料。
2. 公開場所或公開活動中所蒐集、處理或利用之**未與其他個人資料結合**之影音資料。

個人資料保護法

第51條第1項

有下列情形之一者，不適用本法規定：

一、自然人為單純個人或家庭活動之目的，而蒐集、處理或利用個人資料。

二、於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料。

二、豁免情形之探討
（一）我國個資法規定及實務現況（2/2）

8

■ 立法理由

- 依修正條文第二條第八款規定，本法所稱非公務機關包括自然人，惟有關自然人為單純個人（例如：社交活動等）或家庭活動（例如：建立親友通訊錄等）而蒐集、處理或利用個人資料，因係屬私生活目的所為，與其職業或業務職掌無關，如納入本法之適用，恐造成民眾之不便亦無必要，爰增訂第一項規定，予以排除。
- 在網際網路上張貼之影音個人資料，亦屬表現自由之一部分。為解決合照或其他在合理範圍內之影音資料須經其他當事人書面同意...其本身共同使用之合法目的亦相當清楚...不適用本法之規定，回歸民法適用。（法務部立法說明參照）

■ 實務見解

- 民眾於公職人員選舉開票作業之公開活動中進行攝影，如僅為單純個人活動目的而蒐集自然人之資料，或僅攝影不特定自然人影像且未與其他個人資料結合時，尚無個資法之適用（法務部 104 年 11 月 05 日法律字第 10403514100 號函參照）
- 消防人員於執行緊急救護勤務中所錄存之影音資料若涉及可直接或間接識別特定個人之資料，自有個資法之適用。（法務部106 年 02 月 15 日法律字第10603502190號函參照）

- 而實務見解係根據該行為之目的進行判斷，並未因可能係公開場所或公開活動之影音資料，而逕引為公務機關（消防機關）豁免適用個資法之依據。
- 我國實務見解認為個資法第51條第1項第1款立法目的在私生活行為豁免，同項第2款立法目的在公開場所或公開活動之影音資料表現自由豁免，但未包含公開場所或公開活動監視錄影設備之管理或調和豁免。

國家發展委員會

二、豁免情形之探討
（二）外國相關立法例（1/5）

9

■ 國際立法例：豁免情形-1

主要分為政府行為、私人活動或其他私領域行為、基本權競合等類型。針對不同豁免類型可分為全域豁免（例如歐盟GDPR第2條第2項四種豁免情形之一者，整部GDPR皆不適用），以及細分為部分豁免之情形。

國家		豁免情形			
		政府行為	私人活動或其他私領域行為	基本權競合	其他
歐盟GDPR		• 刑事案件機關程序* • 外交安全政策	• 單純個人或家庭活動	• 表意自由與資訊自由，包括新聞目的及學術、藝術及或文學表意目的（部分豁免）	• 歐盟法領域外活動
德國					
英國		• 特定領域政府活動（執法行為、情報服務）			• 內閣大臣得以法律制定更多豁免規定
美國	CPRA	• 公務機關	• 企業內部管理（部分豁免） • 一般個人 • 受雇或應徵資料（部分豁免）		• 聯邦法律已規範 • 公開可得資料 • 特定類型豁免（部分豁免） • 特定責任豁免
	UPDPA	• 公務機關 • 法院令狀、命令或其他法律允許 • 政府資料公開	• 受雇或應徵資料		• 聯邦法律已規範 • 公開場所觀察所得資料 • 人體試驗研究

*另有歐盟第 2016/680號指令規範　※藍字為另有其他法律規範之情形。　※有關部分豁免範圍，可參閱簡報p.27-p.38附件說明。

二、豁免情形之探討（二）外國相關立法例（2/5）

10

■ 國際立法例：豁免情形-2

國家	豁免情形			
	政府行為	私人活動或其他私領域行為	基本權競合	其他
日本	• 刑事案件或少年保護案件之程序（部分豁免）		• 新聞或出版、宗教、政治、學術自由（部分豁免）	
韓國	• 公務機關執行公務（部分豁免） • 預防犯罪及搜查所必要（部分豁免）	• 個人日常活動（部分豁免）	• 媒體、宗教團體、政黨基於報導、傳教、推薦候選人等目的（部分豁免）	• 法令具體准許部分排除之情形 • 經合理評估，且使用其他資料也無法識別個資時得全部排除
新加坡	• 公務機關	• 單純個人或家庭活動 • 商業契約或商業活動（部分豁免）		• 專責機關得發布豁免名單
菲律賓	• 政府活動		• 新聞、藝術、文學或研究目的	• 外國法具備管轄權 • 公眾關注事項
瑞士	• 聯邦議會 • 政府訴訟程序	• 自然人個人使用 • 民法公開登記		• 紅十字會

※藍字為另有其他法律規範之情形。　※有關部分豁免範圍，可參閱簡報p.27-p.38附件說明。

二、豁免情形之探討（二）外國相關立法例（3/5）

11

■ 常見豁免情形

- 「政府行為」主要包含統治行為、公務機關執行公務、刑事案件機關程序、刑事案件或少年保護案件之程序、議會訴訟程序等。
  - 目前許多國家（如歐盟、日本、韓國等）在刑事訴追過程等程序上，因有其他法律調和，故於個資法有豁免。
- 「私人活動或其他私領域行為」則主要為個人日常活動、單純個人或家庭活動、商業契約或商業活動、民法公開登記、受雇或應徵資料等。
  - 在個人家庭活動之部分，幾乎所有國家皆有豁免，較無爭議；
  - 受雇應徵資料、或企業內部管理為美國特別強調；
  - 商業契約則為新加坡特有規範。
- 「基本權競合」則有例如新聞媒體或出版自由、宗教自由、政治自由、學術自由、藝術自由等基本權利，該相關權利與隱私權競合。
  - 歐盟體系特別針對言論自由相關權利（如新聞目的及學術、藝術及或文學表意目的）有部分豁免規定；
  - 日、韓等國則有進一步針對宗教、政治等權利給予部分豁免；
  - 有關新聞、藝術、文學或研究目的，菲律賓為全域豁免。

二、豁免情形之探討（二）外國相關立法例（4/5）

12

■ 附論：有關公開場所影音資料之管理-1

- 我國個資法第51條第2項「於公開場所或公開活動中所蒐集、處理或利用之未與其他個人資料結合之影音資料」規定，未見於其他國家有相類似之豁免立法例，且條文因缺少規範主體，易滋生豁免主體範圍爭議。
- 前開說明已見函釋排除豁免基於職業或業務職掌之公開場所或公開活動影音資料蒐集、處理及利用，惟該條款僅係指豁免個資法適用，尚非監視設備之管理規定。

◆ 德國：針對監視錄影設備設置例外允許規定

- 監視錄影設備屬於自動化之資料處理系統，監視錄影設備於公眾得進出之空間、場所架設，且該**監視畫面屬於可得辨識之個人資料時，應遵守BDSG對於蒐集、處理或利用行為之規範**。
- 依據德國個資法BDSG第4條第1項之規定，只有在必要時才例外允許監視錄影設備於公眾得出入之場所蒐集、處理或利用個人資料：
  (1)基於執行公務機關之任務
  (2)基於行使同意或拒絕他人進入所有物之權利
  (3)為特定目的行使合法利益者

BDSG第4條第3項規定，如對實現預期目的具必要性，且無跡象顯示資料當事人之合法性高於其餘利益，則應允許依據第一項進行資料之儲存或使用。僅必要時，得出於防止對**國家和公共安全**造成威脅及**起訴犯罪**之目的進一步處理資料。

- 德國法院審查「特定目的行使合法利益」時，其指明該目的須合法、明確且適當之特定目的，該目的須客觀可說明值得保護該利益之「合理的理由」，而非僅係權利人之主觀上利益而已；該手段須有助於設置目的之達成，且別無其他侵害較小亦能達成相同目的之手段可資運用時，始得為之。至於該**理由是否適當及手段是否必要，應由行政機關及法院根據個案具體事實予以判斷之**。

國家發展委員會

二、豁免情形之探討（二）外國相關立法例（5/5）

13

■ 附論：有關公開場所影音資料之管理-2

◆ 韓國：針對監視錄影設備設置例外允許規定

- 韓國PIPA依第25條第1項各款「得例外設置監視器」之情形：
  (1) 法令中有具體准許之情形；
  (2) 為預防犯罪及搜查所必要；
  (3) 設置係公共安全及防治火災所必要；
  (4) 交通管制所必須；
  (5) 交通資料之蒐集、分析所必要。

不適用個人資料的蒐集、處理利用的原則；取得資料當事人同意的方式；移轉個人資料予第三方之限制；個人資料外洩之通報義務；個人資料停止處理之要求之規定。（第15條、第22條、第27條第1項及第2項、第34條及第37條）

- 監視器設置應**依照細則規定程序舉辦公聽會或說明會**等，並聽取相關專家及利害關係人之意見；並**應設置公告說明**(1) 設置目的及場所；(2) 攝影範圍及時間；(3) 負責人之姓名及聯絡方式；(4) 其他依細則所定事項。（根據「軍事基地暨軍事設施保護法」第2條第2款之軍事設施及「防衛法」第2條第13款所定之國家重要設施或及其他依細則所定之設施不在此限。）
- 影像資料處理者應依第PIPA第29條規定設置**適當安全管理必要措施**；影像資料處理者應依細則所定之運作、管理規定操作，並得排除PIPA第30條「個人資料處理方針」之適用；影像資料處理者得將有關設置及運作事務委託第三方。惟公務機關委託第三方時，其程序及條件應**依細則**定之。

德國、韓國針對監視器規範於個資法中，有訂定「得例外設置」之情形，並針對監視器之設置加強義務。其他國家，如英國規範於《自由保護法》、日本發布「監視器影像利用指引」、美國依判例等，多數國家未明文規範於個資法。

國家發展委員會

二、豁免情形之探討（三）小結

14

1. 依我國個資法第51條立法理由觀之，我國個資法第51條第1項第2款，為我國獨有之張貼表現自由，其本質或可能與我國個資法第51條第1項第1款相似。
2. 我國個資法排除自然人單純為個人活動目的，而各國相較我國，則有更多針對政府行為、私法行為（如商業契約）、基本權（如言論自由）等之豁免情形。
3. 我國個資法無類似公開場所或公開活動錄影監視錄影設備之管理規定。

二、豁免情形之探討（四）討論議題

15

Q

1. 現行我國個資法第51條第1項第1、2款之兩款事由是否須整併合一或調整？
2. 我國是否參考他國模式，針對部分政府行為、私法行為（如調查、商業契約等）、基本權等類型（如言論自由），設立豁免規定？建議納入哪些行為類型？
3. 我國雖有針對公開場所影音資料之豁免，然而尚未具體針對監視器規範，我國是否適合仿效德國、韓國，納入個資法規範？或於未另為規範前，發布指引？

16

大綱

一 討論範圍

二 豁免情形之探討

三 域外效力之探討

四 附件

17

三、域外效力之探討
（一）我國個資法規定及實務現況（1/2）

■ 個資法管轄範圍為公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者。

個人資料保護法

第51條第2項

公務機關及非公務機關在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。

行為主體 \ 對象		蒐集、處理、利用對象	
		我國人民	外國人民
我國公務機關及非公務機關	於我國境內為之	適用	適用
外國公務機關及非公務機關			
我國公務機關及非公務機關	於我國境外為之	適用（個資法第51條第2項）	不適用
外國公務機關及非公務機關		不適用	不適用

三、域外效力之探討
（一）我國個資法規定及實務現況（2/2）

18

■ 立法理由

- 由於科技之進步與網際網路使用普遍，即使在我國領域外蒐集、處理或利用國人之個人資料，亦非常容易。為防範公務機關或非公務機關在我國領域外違法侵害國人個人資料之隱私權益，以規避法律責任，爰增訂第二項，明定在我國領域外，亦有本法之適用。

■ 實務見解

- 按個人資料保護法（下稱個資法）第51條第2項規定：「公務機關及非公務機關，在中華民國領域外對中華民國人民個人資料蒐集、處理或利用者，亦適用本法。」準此，在我國領域外蒐集、處理或利用個人資料行為，須合於下列要件，始有個資法之適用：（一）從事蒐集、處理或利用行為者為我國之公務機關及非公務機關；（二）所蒐集、處理或利用者為我國人民之個人資料。（法務部107年3月12日法律字第10703502240號函釋）

我國個資法之域外效力管轄範圍，特有規範境外我國人民，且蒐集主體必須為我國之公務機關或非公務機關之情形。

三、域外效力之探討
（二）法律適用效力討論範圍

19

- 蒐集主體在境外，對境內自然人個資之蒐集處理利用
- 我國蒐集主體在境外，對境外之我國公民個資之蒐集處理利用

域外效力

屬人主義：人之效力，我國人不問居住於國內外均以受我國法律拘束為原則。

保護我國公民：防範公務及非公務機關在我國領域外違法侵害我國國人個資。

（我國個資法第51條修正說明參照）

保護境內自然人：無論蒐集主體是否在境內，對境內自然人（不問國籍）處理個資。

（歐盟GDPR第3條第2項參照）

- 我國尚未針對未在境內設有實體，但有蒐集、處理、利用我國境內人民個資之情形規範。

三、域外效力之探討（三）外國相關立法例（1/3）

20

■ 國際立法例：域外效力

國家		受規範之蒐集主體	受規範行為	對象
歐盟GDPR 德國 英國		• 提供境內資料主體產品或服務（包括免費提供） • 涉及監控境內資料主體之行為 • 適用不在境內設立，但根據國際公法適用國內法之控管者	處理行為（適用境內設立之控管者或處理者所為之個資處理活動，不問該處理是否發生於境內）	境內之人（無論國籍）
美國	CPRA	• 特定標準之企業*	蒐集、購買、販售、分享行為	當地居民
	UPDPA	• 特定標準之企業	蒐集、購買、販售、分享行為	當地居民
日本		• 個資處理事業者對境內之人提供物品或勞務，而取得本人個資於境外處理或利用者	處理或利用行為	境內之人（無論國籍）
韓國		• 未明文規定域外範圍 • 公司對境內公民提供服務，或透過跨境提供商品或服務而產生收入	處理或利用行為 *韓國境內無地址或營業場所之ICT業者，若使用人數、營收達標準，須書面指定代理人。	未明文
新加坡		• 境內蒐集、利用或揭露個資之組織（無論境內是否設有實體營業據點）	蒐集、利用、揭露行為	境內之人（無論國籍）
菲律賓		• 境內運用個資者 • 境內簽約者 • 境內有控管之法人者 • 境內設有設備或分公司者	蒐集、處理、利用行為	境內之人（無論國籍） 境外公民
瑞士		• 在本國之違法行為者 • 有權懸掛聯邦國旗標誌的船舶或飛機	處理行為（對瑞士產生影響的情形）	境內之人（無論國籍）

國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

*美國CPRA：展開業務之外適須符合下列門檻(擇一)：1.年營業額達2500萬美金或年度購買/販售/分享超過10萬消費者之個資；2.公司有50%以上之年營業額來自販售/分享消費者個資

三、域外效力之探討（三）外國相關立法例（2/3）

21

■ 域外效力之範圍 - 1

◆ 歐盟GDPR體系（如德國）、英國、日本、新加坡、瑞士等

- 歐盟GDPR依據《競爭法》概念，若對**市場有產生影響**者，皆納入規範管制。故針對提供歐盟境內資料主體產品或服務；涉及監控歐盟境內資料主體之行為。主體適用境內設立之控管者或處理者所為之個資處理活動，**無論該處理是否發生於境內**。
- 對象針對境內之人，無論當事人國籍。
- 日本、新加坡、瑞士等國，其域外效力皆仿效歐盟模式。

◆ 美國CPRA

- 要求營利事業有於加州展開業務，無論營利事業是否實體存在於加州。營利事業的定義延伸到「包括任何控制、或由營利事業控制的實體，並且與營利事業共用品牌名稱、服務標識或商標」，使**位於加州境外的實體也可能受到規範**。
- 對象針對加州居民。
- 若消費者資料的**蒐集、販售和共享**之商業行為皆未發生在**加州境內**，亦無任何個資為消費者位在加州時所蒐集，則CPRA規定將不適用於該資料。

國家發展委員會 NATIONAL DEVELOPMENT COUNCIL

三、域外效力之探討
（三）外國相關立法例（3/3）

22

■ 域外效力之範圍 - 2

◆ 菲律賓域外效力範圍較為寬泛

- 規範涉及菲律賓公民或居民之個人資料。
- 運用個人資料之自然人或法人於菲律賓境內，或於境外運用關於菲律賓個人或居民之個人資料，包含但不限於下列情況：（1）在菲律賓簽訂契約；（2）並未設立於菲律賓，但於菲律賓境內有管理和掌控之法人；（3）法人於菲律賓境內有分公司、辦事處、辦公室或子公司，並可近用個人資料。

1. 歐盟GDPR規範任何有意圖在境內提供產品或服務者（含免費提供）；美國CPRA限定在對當地居民展開業務之營利事業，並須符合一定程度之業務標準（營業額、資料量）。
2. 多數國家不要求須實體存在境內，未直接針對行為發生地規範，故規範可涵蓋網路上所進行之處理行為。
3. 菲律賓為少數規範對象包含境內人民及境外公民之國家；而多數國家僅規範境內人民個資。
4. 亦有不以明文規定域外效力之國家，如韓國。

三、域外效力之探討
（四）小結

23

1. 依據我國個資法第51條第2項法條結構觀之，僅針對保護我國公民，而我國域外效力管轄範圍，僅針對境外之我國蒐集主體對我國人民個資之蒐集、處理、利用行為。

2. 我國個資法第51條第2項不宜解讀為類似歐盟GDPR第3條第2項之域外效力。

三、域外效力之探討
（五）討論議題

24

Q

1. 我國個資法並無類似歐盟GDPR第3條第2項針對境外實體域外效力規範，是否有納入我國個資法之必要？若採納，應有哪些適用條件？
2. 現行有規範「針對域外法人或自然人對境內之人行為」之國家，皆設有專責機關，而我國目前由各主管機關分別管理，若法條納入此類域外效力，是否有需其他配套措施？

討論議題

25

案由一、豁免情形之探討

- 現行我國個資法第51條第1項第1、2款之兩款事由是否須整併合一或調整？
- 我國是否參考他國模式，針對部分政府行為、私法行為（如調查、商業契約等）、基本權等類型（如言論自由），設立豁免規定？建議納入哪些行為類型？
- 我國雖有針對公開場所影音資料之豁免，然而尚未具體針對監視器規範，我國是否適合仿效德國、韓國，納入個資法規範？或於未另為規範前，發布指引？

案由二、域外效力之探討

- 我國個資法並無類似歐盟GDPR第3條第2項針對境外實體域外效力規範，是否有納入我國個資法之必要？若採納，應有哪些適用條件？
- 現行有規範「針對域外法人或自然人對境內之人行為」之國家，皆設有專責機關，而我國目前由各主管機關分別管理，若法條納入此類域外效力，是否有需其他配套措施？

26

大綱

一 討論範圍

二 豁免情形之探討

三 域外效力之探討

四 附件

27

歐盟相關規定（1/2）

最近一次個資法修正：2016年（2018年施行）

GDPR不適用主體	
亡者（前言第27點）	法人（前言第14點）
豁免情形	
全域豁免（第2條第2項）	**部分豁免（第85條）**

1. 歐盟法領域外的活動	• 與言論自由相關之資料處理。
	• 當資料控管者因新聞目的、學術藝術或文學目的處理資料時，成員國得對部分GDPR條文給予豁免，包含：
	  • 第二章 資料處理原則
	  • 第三章 資料主體權利
	  • 第四章 資料控管者與受託處理者義務
	  • 第五章 國際傳輸
	  • 第六章 獨立專責機關
	  • 第七章 專責機關合作與一致性
	  • 第九章 特定資料處理情形
	• 但是，部分豁免必須是因為要平衡言論自由與個資保護而必要。

2. 外交安全政策綱領規範之活動	
3. 自然人之個人或私人活動 與個人私生活或是家庭生活相關之活動	
4. 辦理刑事案件之機關	

歐盟相關規定（2/2）

最近一次個資法修正：2016年（2018年施行）

域外效力（第3條第2項）	
提供歐盟境內資料主體產品或服務	涉及監控歐盟境內資料主體之行為
• 判斷依據並非是以國籍或是居住地，而是資料主體是否處於歐盟境內 • 時間點：提供產品或服務之當下 • 適用性：意圖提供 • 免費提供亦適用	三個要件： 1. 資料主體應於歐盟境內 2. 監控之行為應於歐盟境內 3. 監控行為是指對自然人進行決策或對其個人喜好、行為及態度進行分析或預測
* 適用GDPR規定，但不享有一站式機制（第56條）	

英國相關規定（1/2）

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

豁免情形 GDPR § 2(2)	
個人與家庭生活	➢ 個人在單純的個人或家庭活動過程中對個人資料之處理
特定主管機關	➢ 主管機關出於任何執法目的處理個人資料（需參見DPA 2018第3部分） (a)主管機關完全或部分透過自動化方式處理個人資料 (b)由主管機關以自動方式以外的方式，處理構成歸檔系統的一部分或旨在構成歸檔系統的一部分的個人資料 ➢ 主管機關（competent authority）：DPA 2018附件7列舉之56個政府機關，EX：倫敦市警察局長、英國稅務海關總署專員，
情報單位服務	➢ 情報單位之個人資料處理（需參見DPA 2018第4部分） (a)情報單位完全或部分透過自動化方式處理個人資料 (b)由情報單位以自動方式以外的方式，處理構成歸檔系統的一部分或旨在構成歸檔系統的一部分的個人資料 ➢ 情報單位： ● 英國安全局（Security Service） ● 英國祕密情報局（Secret Intelligence Service） ● 政府通信總部（Government Communications Headquarters）

30

英國相關規定（2/2）

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

DPA 2018 §207(1)：
處理屬於DPA 2018 Part 2 *，則其域外效力適用UK GDPR §3之規定（紅色表格）
處理不屬於DPA 2018 Part 2，則依§207(2)之規定（綠色表格）

域外效力 GDPR §3	
英國內設有機構之控管者處理者	處理行為無論境內或境外都適用UK GDPR
英國外之控管者、處理者	1.對英國境內之資料主體提供商品或服務（不問是否付費） 2.監視英國境內資料當事人之行為 3.根據國際公法適用英國國內法之控制者，其對於個人資料的處理

域外效力 DPA 2018 §207(2)	
在英國設有機構之控管者處理者	處理行為無論境內或境外都適用DPA 2018

在英國設有機構之意義：
1) 通常居住在英國的個人
2) 根據英國或英國一部分法律成立的機構、合夥企業或其他非法人協會
3) 非前述情形，但在英國有穩定之辦事處、分支機構或代理機構並有開展活動者。

* 註：DPA 2018 Part 2 之內容係在補充UK GDPR規定

31

德國相關規定

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

豁免情形 BDSG § 1(1)、GDPR § 2(2)	
BDSG	➢ 資料當事人所為之單純個人或家庭活動，不適用本法之規定。
GDPR	➢ 歐盟法領域外的活動（outside the scope of Union law），例如國安相關； ➢ 外交安全政策綱領規範之活動（common foreign and security policy），例如與政黨、人權侵犯相關之活動； ➢ 自然人之個人或私人活動（purely personal or household activity）； ➢ 辦理刑事案件之機關。 →以上皆為豁免情形，不適用本法之規定。

域外效力 BDSG § 1(4)、GDPR § 3		
於德國境內運用、處理個人資料抑或於歐盟成員國或歐洲經濟共同體之締約國境內設立登記者。	➢ BDSG第1條第4項第1款及第2款之規定，有德國BDSG之適用。
未於德國境內運用、處理個人資料抑或未於歐盟成員國或歐洲經濟共同體之締約國境內設立登記者。	➢ 提供商品或服務之資料主體，（不問資料主體付款與否）非於歐盟境內。 →無德國BDSG之適用。
	➢ 提供商品或服務之資料主體，（不問資料主體付款與否）位於歐盟境內。 →依據GDPR第3條規定有適用，則有BDSG第1條第4項第3款之適用。

美國相關規定（1/2）

32

無聯邦個資法，加州消費者隱私法（ CCPA）最近修正為 2018年，修正 CCPA 的新法 CPRA 將於 2023 年實施，效力溯及 2022 年 1 月 1 日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），目前已陸續有州提案。

CBPR成員國

豁免類型	CCPA&CPRA 豁免規定	例外
已受其他法規規範	• **醫療資料、主體**：適用**CMIA / HIPAA**的資料和主體、**符合人體受試者保護規範**的研究、臨床試驗蒐集資個資（*CPRA§1798.145 (c)*）	
	• **信用資料處理活動**：受**《公平信用報告法》**規範者（*§1798.145(d)*）	不豁免 §1798.150 的資安侵害責任
	• **金融資料**：受**《金融服務法現代化法》**、**《加州財務資訊隱私法》**、**《農業信用法》**規範者（*§1798.145(e)*）	不豁免 §1798.150 的資安侵害責任
	• **駕駛人資料**：受**《駕駛人隱私保護法》**規範者（*§1798.145(f)*）	不豁免 §1798.150 的資安侵害責任
公開可得資料	• 直接排除於個人資料定義之外（*§1798.104 (v)*）	
特定資料類型豁免	• **勞雇關係資料**（*§1798.145(m)(1)*）	不豁免§ 1798.100 (a) 蒐集個資告知義務、§1798.150 資安侵害責任
	• **自然人作為工作單位機關手足、提供、接收產品服務或善盡相關責任時**與營利事業書面、口頭溝通之個資（*§1798.145(n)(1)*）	
特定主體情境豁免	• **商業信用報告機構就業務負責人資料**：如僅用於消費者作為事業所有人、主管、經理人之角色用以聯繫消費者、識別消費者與其所擁有事業的關係，不適用刪除權、退出個資販售分享權規定。（*§1798.145(o)*）	
特定責任豁免	• 營利事業**無實際知悉（actual knowledge）、無理由相信（no reason to believe）下列違法意圖不須負責** • 服務提供者、承包商違反CCPA、CPRA之意圖，但營利事業向前二者揭露個資係遵守規定 • 第三方違法使用個資之意圖，但營利事業經簽訂書面契約要求相同權利保護程度 • 營利事業違反義務，服務提供商、承包商亦不負責，僅對自己違法行為負責（*§1798.145(i)*）	

美國相關規定（2/2）

33

無聯邦個資法，加州消費者隱私法（ CCPA）最近修正為 2018年，修正 CCPA 的新法 CPRA 將於 2023 年實施，效力溯及 2022 年 1 月 1 日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），目前已陸續有州提案。

CBPR成員國

豁免類型	UPDPA豁免規定	例外
主體類型	• 排除公務機關（*UPDPA§3(b)*）	
資料類型	• 已公開可得資料 • 符合人體受試者法規之研究資料 • 司法令狀、命令 • 政府資料公開法規要求公開之資料 • 勞雇關係資料（*UPDPA§3(c)(2)*）	
已受其他聯邦法律規範	• 受 **HIPAA** 規範之主體（*UPDPA§5 (c)*） • 受**《公平信用報告法》**（FCRA）規範的資料處理態樣 • 由 FCRA 所稱之消費者報告機構、資訊提供者、使用或取得消費者報告者用於生成消費者報告（consumer report） • 資料處理受下列**聯邦法律**規範並符合規定：**《金融服務法現代化法》**（Gramm-Leach-Bliley Act）、**《駕駛人隱私保護法》**（Drivers Privacy Act of 1994）、**《家庭教育權利及隱私法》**（Family Education Rights and Privacy Act of 1974）、**《兒童線上隱私保護法》**（Children's Online Privacy Protection Act of 1998）（*UPDPA§11(b)*）	• 未受聯邦法律約束的資料處理，**仍受UPDPA約束**。 • 企業遵守其他相類個人資料保護法時（須經該州總檢察長認定），**可替代**UPDPA合規性。（*UPDPA§11*）
法規/草案	**域外效力**	
CCPA、CPRA	• 未限制營利事業須實體存在於加州，**具域外（州外）效力** • 營利事業定義延伸至「包括任何控制、或由營利事業控制的實體，並且與營利事業共用品牌名稱、服務標識或商標」，位於加州境外的實體也可能受到CCPA、CPRA規範（*§1798.140(d)*）	
UPDPA	• 未限制控管者、處理者須實體存在於州內，**具域外（州外）效力**（*UPDPA§3(a)*）	

日本相關規定

34

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

豁免情形	• 非公務機關依第57條共有四種情形： （1）廣播機關、新聞社，通訊社及其他報導媒體（包含以報導為業之個人）供報導之用，所稱「報道」係指將客觀事實告知非特定且多數人（包括基於此陳述意見或見解）；（2）以著述為業者，供著述之目的利用；（3）宗教團體為供宗教活動（包含其附隨活動）目的之利用；（4）政治團體為政治活動（包含其附隨活動）之目的之利用。
	• 公務機關依第124條： 在刑事案件或者少年保護案件相關之裁判、檢察官、檢察事務官或者司法警察所為之處分，刑罰或者保護處分的執行、更生緊急保護或者恩赦有關之保有個人資料，不適用本章公務機關之義務第4節「開示、更正及停止利用」部分。
域外效力	• 依第171條規定，個人資料處理事業者對於日本境內之人提供物品或勞務，而取得本人之個人資料，並於日本境外處理該當個人資料或利用該當個人資料所作成之假名化資料處理事業、匿名化資料處理事業者，亦適用本法之相關規定

國家發展委員會

韓國相關規定

35

最近一次個資法修正：2020年（2020年8月5日正式生效）
CBPR成員國

- 一、豁免規定：
  - 1. 部分排除：

排除條文	類型	具體樣態
排除第三章到第七章適用	政府行為	公務機關為執行公務而蒐集之個人資料，如：統計、國家安全、公共衛生及人民福祉、交通管制、公共安全及防災等事由
	基本權競合	政治自由、宗教自由、言論自由；為報導、傳教、推薦候選人等目的而蒐集、處理及利用之個人資料
公開設置並使用之影像資料處理器：排除§15、§22、§27 I及II、§34及§37條	法令規定	法令中有具體准許之情形
	刑事追訴	為預防犯罪及搜查所必要
	政府行為	設置係公共安全及防治火災所必要；交通管制所必須，以及交通資料之蒐集、分析所必要
排除§15、§30、§31	私人行為	個人日常活動，如：聯誼、社團（我國亦將私人行為排除個資法適用）

  - 2. 排除適用：
    以合理之時間、費用、技術予以評估，當使用其他資料也無法識別個人資料時，即不適用本法。
- 二、域外效力：
  PIPA並未明文規定域外範圍，然而自細則觀之，應如GDPR，需考量是否提供對韓國境內公民提供服務，或是透過提供商品或服務以產生收入，而適用PIPA。

國家發展委員會

新加坡相關規定

36

最近一次個資法修正：2020年
CBPR成員國

豁免情形

- 不適用於個人家庭活動、組織員工以及任何公務機關。（PDPA第4條）
- 不適用於基於商業契約簽訂所載之個人資料*、存在超過100年以上紀錄中相關個人資料、死亡時間超過10年以上者之個人資料，以及出於商業目的所提供之商務聯繫資訊*。（PDPA第4條）

★ 經部長（Minister）批准後，個人資料保護委員會（PDPC）可於公報（Gazette）發布命令，豁免任何個人或組織或任何類別之個人或組織，不受本法的全部或任何條款約束，但須遵守其指定之條款或條件。（PDPA第62條）

*排除適用第 3、4、5、6 和 6A 部分（個資保護責任之一般規定；個人資料蒐集、利用和揭露；近用和更正個資；個資保管；資料外洩通知）

域外效力

- 適用於所有在其境內進行個人資料之蒐集、利用或揭露個人資料的所有組織，**無論**該組織是否依據新加坡法律設立，或在境內是否設有實體營業據點。（PDPA第2條）

國家發展委員會

菲律賓相關規定

37

最近一次個資法修正：2012年（2017年、2019年分別提出修正案，尚未完成立法程序）

豁免情形	根據DPA 2012第4條規定，不適用本法之情形包括： 1. 任何現職或曾任職於政府機關之個人，與其職位和職能相關之資料，包含：該個人現職或曾為政府機關之官員或職員之事實；該個人之頭銜、工作地址及辦公室電話號碼；該個人之職位、薪資範圍及職責；該個人任職於政府機關時，工作過程中於文件填寫的名字。 2. 任何過去與現在，個人為政府機關提供服務所訂之契約，包含契約條款以及於提供服務過程中所提供之個人姓名。 3. 任何與社會福利相關之個人資料，如包含個人姓名及福利類型之許可證。 4. 為新聞、藝術、文學或研究目的而運用之個人資料。 5. 政府機關為執行其職務所需之個人資料。 6. 《反洗錢法》及其相關法律所需之個人資料。 7. 外國法具備管轄權之個人資料，包含最初自外國蒐集與目前於菲律賓運用之個人資料。
域外效力	根據DPA 2012第6條規定，本法適用於下列情形： 1. 涉及菲律賓公民或居民之個人資料； 2. 運用個人資料之自然人或法人於菲律賓境內，或於境外運用關於菲律賓個人或居民之個人資料，包含但不限於下列情況：（1）在菲律賓簽訂契約；（2）並未設立於菲律賓，但於菲律賓境內有管理和掌控之法人；（3）法人於菲律賓境內有分公司、辦事處、辦公室或子公司，並可近用個人資料。 3. 於菲律賓境內經營事業，或自菲律賓境內蒐集或持有相關個人資料。

國家發展委員會

瑞士相關規定

最近一次個資法修正：2020年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

豁免情形	• 根據DSG 2020第2條第2項規定，不適用本法之情形包括： 1. 自然人基於個人使用所處理的個人資料； 2. 聯邦議會及議會委員會在審議期間處理的個人資料； 3. 未決之民事訴訟程序、刑事訴訟程序、國際互助程序、憲法程序以及除一審程序外的行政訴訟程序； 4. 基於民法的公開登記； 5. 國際紅十字會所為的資料處理。 • 依同條第4項規定民法的公開登記，當聯邦法律有特別規定者，將受其拘束，若無規定者，始適用本法規定。
域外效力	• 根據DSG 2020第3條第1項規定，本法適用於對瑞士產生影響的情形，即使該些情形係發生於國外。 • 同條第2項規定，適用刑法（Strafgesetzbuch, StGB）有關地域效力之規定： 1. 依刑法第3條規定，本法適用於在本國之違法行為； 2. 及同法第4條規定，無論行為地的法律如何，本國刑法均適用於在有權懸掛聯邦國旗標誌的船舶或飛機上實施的犯罪。

「個人資料保護法相關議題」第 11 場產學專家學者諮詢會議—獨立專責機關監督權限行使方式議程

壹、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（資料可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較「歐盟一般資料保護規則」、「英國一般資料保護規則」、德國「聯邦資料保護法」、美國「加州隱私權法」（CPRA）、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及瑞士「個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，此次討論會議聚焦於獨立專責機關監督權限行使方式。

有關獨立監督機關之職權、首長產生方式、任期保障、預算及人力規模等，不在此次討論範圍。本次會議將就有關「監督」職權中之「調查權」、「處分權」等 2 項進行討論。

貳、議程

一、 主席致詞

二、 報告事項

獨立專責機關監督權限行使方式（國發會）

三、 討論事項

案由一、調查權之行使方式

說明：

一、 我國個資法之調查權規定

我國個人資料保護法之調查權如下：依個資法第 22 條規定，中央目的事業主管機關或直轄市、縣(市)政府得實施行政檢查；個資法第 23 條規定有關扣留物或複製物之適當處置或保管；而個資法第 24 條就對於要求、強制、扣留或複製行為不服者，有得向中央目的事業主管機關或直轄市、縣（市）政府聲明異議之規定，並規範中央目的事業主管機關等機關，其受理聲明異議後，有理由者應停止或變更，無理由者應繼續執行；而不得對該案件聲明不服者，得單獨提起行政訴訟。

而依據個資法第 26 條，中央目的事業主管機關或直轄市、縣（市）政府依第 22 條規定檢查後，未發現違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果；另外，依個資法第 52 條規定，中央目的事業主管機關或直轄市、縣(市)政府執行之權限，得委任所屬機關、委託其他機關或公益團體辦理。

二、 外國相關立法例

綜觀各國法制，可見以下情形：

(一) 各國獨立專責機關之調查權限大致相似

1. 皆類似於歐盟 GDPR 賦予獨立專責機關之調查權，多包含命提供資訊、進行調查、通知違法情況、獲取資訊，以及實地調查等權限。

2. 針對調查權之執行，依各國行政程序差異，規範略有不同，例如德國有要求機關在一定之期限內作出回應；英國則強調命提供資訊應先為資訊通知（information notice)、進行

調查應先為評估通知（assessment notice）；新加坡則分為持法院搜索令進入場所檢查，或在必要時透過發出通知後直接進入場所檢查。

(二) 除歐盟外，多數國家未規範怠於行政處理之救濟程序

1. 在歐盟體系，若獨立專責機關未處理當事人之申訴或是未於三個月內通知調查進度或結果，當事人有權向成員國國內法院訴求司法救濟。

2. 其他國家則多未規範怠於行政處理之救濟程序。

(三) 日本、韓國可委由其他單位協助進行調查

1. 日本有「權限委任」規定，委員會為確保個人資料適當處理必要及其他政令所訂事項，關於第 146 條報告及進入檢查之權限得委任由事業所管大臣、金融廳、證券交易監視委員會等行使；而前述機關應向委員會報告前項權限行使結果。（日本個資法第 150 條）

2. 韓國資料處理者於處理個資，而有侵害資料當事人權益時，受侵害之人得將被侵害事實向保護委員會通報，保護委員會得依施行細則指定專門機關 KISA 之隱私申訴中心受理，調查與個資爭議有關申訴案。（PIPA 第 62 條）

3. 瑞士得在調查範圍內召集其他聯邦機關與地方政府警察機關執行。（DSG 2020 第 50 條）

4. 多數國家由專責機構獨立完成調查。

三、 小結

我國個資法第 22 條有關行政檢查之規範，包含進入檢查、命說明提供文件、扣留等，已有與國際立法例相似之調查權規範，此外，日本、韓國、瑞士有與外部單位合作執行調查程序；我國亦有委外調查之規定，惟係主要由各主管機關執法。多數國家於調查程序中，司法不會介入調查，惟美國得由檢察總長隨時介入調查程序，歐盟體系則僅在獨立專責機關三個月內未回覆調查進度或結果時，始得進入司法救濟。

根據以上觀察，請產學專家就以下議題提供建議：

(一) 觀察我國目前目的事業主管機關之調查權與國外獨立專責機關之調查權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些調查權？

(二) 未來若設置獨立個資專責機關，為避免其調查權之行使，與目的事業主管機關權限行使產生不一致，是否訂定相關衡平之規定(例如：日本個資法規定對於金融事業之調查權委託金融廳行使)？

案由二、處分權之行使方式

說明：

一、 我國個資法之處分權規定

依個資法第 25、47、48 條規定，中央目的事業主管機關或直轄市、縣（市）政府對於違法者得分別處以各種裁罰性或非裁罰性之不利益處分。

二、 外國相關立法例

(一) 各國對於獨立專責機關之處分權內容相似

各國之處分權包括發布警告、發布訓誡、命令遵循當事人要求、命令符合法規規範、命令通知侵害、課予限制、命令更正刪除、行政罰鍰、命令停止國際傳輸、執行通知（限期改正）等權限。

(二)受處分之救濟程序，多數國家採直接進入司法救濟程序

1. 多數國家直接進入司法救濟程序，有關救濟程序之細節，亦因各國行政程序體系而略有差異，例如美國加州檢察長雖有權優先接手案件移轉，加州隱私保護機關(California Privacy Protection Agency, CPPA)不得限制州檢察長執行本法之權力。惟若 CPPA 處分已作成，則受處分企業應依據處分結果，直接進行司法救濟。

2. 新加坡則針對替代性紛爭解決、違規指示、自願承諾或依審查權等作出之任何指示或決定，可依書面申請由 PDPC 重新再議（reconsideration）；若不服再議結果，則可在規定

期間內向再申訴小組主席（the Chairperson of the Appeal Panel）提出再申訴。（但無論是否進行再議程序，皆可提出再申訴）

(三)僅瑞士針對公務機關並無裁罰相關規範

除美國、新加坡之個資法本身即未規範公務機關之外，僅瑞士與我國類似，針對公務機關均無裁罰相關規範，其他多數國家之獨立專責機關可針對公務機關進行裁罰。（有關公務或非公務機關之具體裁罰標準，將於「罰則」場次進行討論）

(四) 日本可將處分權限委任其他單位

日本具有「權限委任」規定，委員會為確保個人資料適當處理必要及其他政令所訂事項，關於第 148 條勸告及命令之權限得委任由事業所管大臣、金融廳長官、證券交易監視委員會等行使；而前述機關應向委員會報告前項權限行使結果。（日本個資法第 150 條）

三、 小結

我國個資法第 25、47、48 條已有規定，中央目的事業主管機關或直轄市、縣（市）政府對於違法者得處以不利益處分。其類型包含禁止蒐集、處理或利用個人資料；命令刪除經處理之個人資料檔案；沒入或命銷燬違法蒐集之個人資料；公布非公務機關之違法情形，及其姓名或名稱與負責人等。而我國相較於國際，已有類似於國際之處分權規範，惟尚由各主管機關進行執法。多數國家之獨立專責機關可針對公務機關進行處分，除美國、新加坡本身未規範公務機關之外，僅我國、瑞士之個資法並無針對公務機關之裁罰權限。另外，多數國家之獨立專責機關所作處分結果不受上級管轄，若受處分者不服獨立專責機關之處分，新加坡有採另組委員會進行審議，而其他國家則採以直接進行司法程序救濟。

根據以上觀察，請產學專家就以下議題提供建議：

(一) 觀察我國目前目的事業主管機關之處分權與國外獨立專責機關之處分權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些裁罰性或非裁罰性之不利益處分？

(二) 觀察其他國家之個資法規定，對於不利益處分，訂有相關緩和作法，例如於不利益處分作成前，日本個資法規定有作成「勸告」之規定、GDPR 有作成「建議」之規定，若勸告或建議之對象已為相關改善，則無後續之不利益處分；又例如日本規定個資保護委員會得授權主管機關為處分等規定，均屬個資法對於不利益處分作成之緩和措施，是否值得我國參考？

(三) 未來若設置獨立個資專責機關，須否納入對公務機關之裁罰權限？

獨立專責機關監督權限行使方式

國家發展委員會
111 年 8 月 24 日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	規範主體、行為區分與特定目的之解釋	資料可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6	111/5/20	111/6/20	111/7/25	111/8/24	

大綱

2

一 討論範圍

二 調查權之行使方式

三 處分權之行使方式

四 附件

一、討論範圍（1/2）

3

■ 討論範圍

討論「獨立專責機關監督權限行使方式」，討論調查權、處分權之行使及救濟，有關罰則置於其他場次討論，並以「個資法」為主要討論範疇。

■ 比較國家

國別	規範名稱	修正時間	特性	專責機關
我國	個人資料保護法	2015	CBPR成員，GDPR適足性諮商中	無
歐盟	一般資料保護規則（GDPR）	2016		歐盟資料保護委員會（European Data Protection Board, EDPB），歐盟成員國應成立至少一間獨立專責機關
德國	聯邦資料保護法	2021	歐盟成員	聯邦個人資料保護暨資訊自由監察官（Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, BfDI） 各邦設置之資料保護監察官（Der Landesbeauftragte für den Datenschutz, LfD）
英國	資料保護法（DPA	2020	歐盟前成員，GDPR適足性（2021）	英國資訊委員辦公室（Information Commissioner's Office, ICO）
美國	加州隱私權法（CPRA）	2020	CBPR成員	加州隱私保護機關（California Privacy Protection Agency, CPPA）
日本	個人資料保護法	2021	CBPR成員，GDPR適足性（2019）	日本個人資料保護委員會（個人情報保護委員会）
韓國	個人資料保護法	2020	CBPR成員，GDPR適足性（2021）	個人資料保護委員會（개인정보보호위원회, PIPC）
新加坡	個人資料保護法	2020	CBPR成員	個人資料保護委員會（Personal Data Protection Commission）
瑞士	個人資料保護法	2020	GDPR適足性認定（指令時代取得）	聯邦資料保護及資訊委員會(Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, EDÖB)

一、討論範圍（2/2）

4

- 有關獨立監督機關之職權、首長產生方式、任期保障、預算及人力規模等，不在此次討論範圍。本次會議將就有關「**監督**」職權中之「**調查權**」、「**處分權**」等2項進行討論。
- 有關罰則規範之細節，如裁罰之標準、金額、刑度等，將於「罰則」場次再行討論。

大綱

5

一 討論範圍
二 調查權之行使方式
三 處分權之行使方式
四 附件

二、調查權之行使方式

6

■ （一）我國個人資料保護法之調查權-1

1. 依個資法第22條規定，中央目的事業主管機關或直轄市、縣（市）政府得實施**行政檢查**。
2. 依個資法第52條規定，中央目的事業主管機關或直轄市、縣（市）政府執行之權限，得**委任所屬機關、委託其他機關**或**公益團體**辦理。

個人資料保護法	
第22條	1. 中央目的事業主管機關或直轄市、縣（市）政府為執行資料檔案安全維護、業務終止資料處理方法、國際傳輸限制或其他例行性業務檢查而認有必要或有違反本法規定之虞時，得**派員攜帶執行職務證明文件，進入檢查，並得命相關人員為必要之說明、配合措施或提供相關證明資料**。 2. 中央目的事業主管機關或直轄市、縣（市）政府為前項檢查時，**對於得沒入或可為證據之個人資料或其檔案，得扣留或複製之**。對於應扣留或複製之物，得要求其所有人、持有人或保管人提出或交付；無正當理由拒絕提出、交付或抗拒扣留或複製者，得採取對該非公務機關權益損害最少之方法強制為之。 3. 中央目的事業主管機關或直轄市、縣（市）政府為第一項檢查時，得率同資訊、電信或法律等專業人員共同為之。 4. 對於第一項及第二項之進入、檢查或處分，非公務機關及其相關人員不得規避、妨礙或拒絕。 5. 參與檢查之人員，因檢查而知悉他人資料者，負保密義務。
第52條	1. 第二十二條至第二十六條規定由中央目的事業主管機關或直轄市、縣（市）政府執行之權限，**得委任所屬機關、委託其他機關或公益團體辦理**；其成員因執行委任或委託事務所知悉之資訊，負保密義務。 2. 前項之公益團體，不得依第三十四條第一項規定接受當事人授與訴訟實施權，以自己之名義提起損害賠償訴訟。

我國目前並無獨立之個資專責機關，係由中央目的事業主管機關或直轄市、縣（市）政府管轄，而因資源預算差異等因素，對各產業個資保護法遵循之監督與管理程度並不相同。

國家發展委員會

二、調查權之行使方式

7

■ （一）我國個人資料保護法之調查權-2

1. 依個資法第23條，有規範中央目的事業主管機關或直轄市、縣（市）政府之**扣留物或複製物之適當處置**。
2. 依個資法第24條規定，針對前兩條之要求、強制、扣留或複製行為**不服者**，得向中央目的事業主管機關或直轄市、縣（市）政府**聲明異議**。
3. 依個資法第26條規定，未發現有違反本法規定之情事者，經該非公務機關同意後，得公布檢查結果。

個人資料保護法	
第23條	1. 對於前條第二項扣留物或複製物，**應加封緘或其他標識，並為適當之處置**；其不便搬運或保管者，得命人看守或交由所有人或其他適當之人保管。 2. 扣留物或複製物**已無留存之必要**，或決定不予處罰或未為沒入之裁處者，應發還之。但應沒入或為調查他案應留存者，不在此限。
第24條	1. 非公務機關、物之所有人、持有人、保管人或利害關係人對前二條之要求、強制、扣留或複製行為不服者，得向中央目的事業主管機關或直轄市、縣（市）政府**聲明異議**。 2. 前項聲明異議，中央目的事業主管機關或直轄市、縣（市）政府認為有理由者，應立即停止或變更其行為；認為無理由者，得繼續執行。經該聲明異議之人請求時，應**將聲明異議之理由製作紀錄交付**之。 3. 對於中央目的事業主管機關或直轄市、縣（市）政府前項決定不服者，僅得於對該案件之實體決定聲明不服時一併聲明之。但第一項之人依法不得對該案件之實體決定聲明不服時，得單獨對第一項之行為經行提起**行政訴訟**。
第26條	中央目的事業主管機關或直轄市、縣（市）政府依第二十二條規定檢查後，未發現有違反本法規定之情事者經該非公務機關同意後，**得公布檢查結果**。

國家發展委員會

二、調查權之行使方式

8

■ （二）國際立法例比較

相似　涉及強制力

權限 / 國別	命提供資訊	進行調查	實地調查	通知違法情況	獲取資訊	稽核評估	受理申訴	提供建議	扣留或複製	傳喚取證	委外調查	其他
我國	○	○	○	○	○	○	○	○	○	X	○	
歐盟	○	○	○	○	○	○	○	○	-	-	-	
英國	○	○	○	○	○	○	○	○	○	X	X	
德國	○	○	○	○	○	○	○	○	X	X	X	
美國	○	○	○	○	○	○	○	○	○	○	X	聽證通知
日本	○	○	○	○	○	X	○	○	X	X	○	
韓國	○	○	○	○	○	○	○	○	○	X	○	申訴中心
新加坡	○	○	○	○	○	○	○	○	○	○	X	
瑞士	○	○	○	○	○	X	○	○	X	○	X	專家評估

二、調查權之行使方式

9

■ （三）國際立法例：調查權之限制與救濟-1

國家	調查權之程序及限制	調查權之救濟
歐盟 GDPR	GDPR §58 (1) 調查權，其程序及限制由各國專責機關自行訂定	• GDPR §78 (2) 若獨立專責機關未處理當事人之申訴或是未於三個月內通知調查進度或結果，當事人有權向成員國國內法院訴求司法救濟
英國	• 命提供資訊應先行「資訊通知」；進行調查應先行「評估通知」 • 獲取資訊、實地調查應先進行「評估通知」，並遵守DPA附錄15之程序性規定（例如通知之內容、複製本、執行時限等規範）	• 受通知對象28日內可向行政法院提出救濟（appeal to the Tribunal）（DPA §162），若不服可上訴至上級行政法院。 • 英國行政司法體系下的法庭系統（Tribunal System），以類似於法院的方式來裁決爭議，但有不同的規則和程序，並且只在專業領域內運作。以個人資料為例，會交由總監管分庭的法庭（tribunal in the General Regulatory Chamber）處理。
德國	• GDPR §58 (1) 調查權 • 除所涉及的問題微不足道或在此期間已得到補救外，監察官應向BfDI傳達投訴，並要求BfDI在一定之期限內作出回應。 • 除有立即危險或為了公共利益而有必要即刻作出決定，且提供建議將與公共利益相衝突之外，應給予BfDI在合理期限內對資料控管者提供建議的機會。	BDSG §60自然人或法人可對監察官(Federal Commissioner)提出投訴 (complaint)。
美國 CPRA	• 違規案件執法（行政）： 合理依據認定需通知，提供證據，告知可親自出席或委任律師 認定企業違規，須依加州行政程序法舉辦聽證，舉行聽證前並以書面通知（§1798.199.50） • 州檢察長（民）要求接手案件須移轉（§1798.199.90 (c)） • 當確定沒有發生任何違規行為時，CPPA應發佈聲明。	• 無（待專責機關之處分作成後，可由司法審查救濟）

二、調查權之行使方式

10

■ （三）國際立法例：調查權之限制與救濟- 2

國家	調查權之程序及限制	調查權之救濟
日本	• 進入檢查之職員應攜帶身分證明書，如關係人請求時並應提示之 • 當行政機關首長依豁免規定提供個資，不得行使監督權限。 • 應不得妨礙表現自由、學問自由、信仰自由及政治活動自由；對豁免規定所列人員不得行使監督權限。	無（待專責機關之處分作成後，可由司法審查救濟）
韓國	• PIPA第63條更賦予保護委員會，在資料處理者有第1項各款情形之一時，於資料處理者符合下列各款情形之一者，保護委員會得發動調查權，要求資料處理者提出相關資料： 1. 有違反本法所定之事項或得知有嫌疑。 2. 接獲通報或申訴時。 3. 為保護資料當事人所必要的事項由施行細則定之。 • 應注意執行上述調查應確保相關文件及證據有相關安全保護措施不會被流出，並應遵守相關保密義務。	• 除了個人資料保護委員會（PIPC）外，在韓國訊息安全局（KISA）轄下，另設有「個人資料紛爭調解委員會」負責調解與個人資料相關爭議。 • 若不適用調解，調解不成或一方當事人提出訴訟，則應中止調解，並對該調解終止事實，另行訴訟程序 • 若為PIPC發動調查，應賦予被調查者補正與說明機會。
新加坡	• 可透過向組織發出書面通知，要求該出示特定文件或特定資訊 • 持法院搜索令進入場所檢查；或2日前發出通知，並表明調查主題目的後，得不持搜索令進入檢查。	無（專責機關之處分得對個資保護委員會提起申訴，如不服可由司法審查救濟）
瑞士	• 若違反資料保護之情形輕微得避免展開調查 • 若經申訴，應告知採行措施及調查結果。	無（專責機關之處分得對個資保護委員會提起申訴，如不服可由司法審查救濟）

二、調查權之行使方式

11

■ （四）小結-1

◆ 各國獨立專責機關之調查權限大致相似

- 皆類似於歐盟GDPR賦予專責機關之調查權，多包含命提供資訊、進行調查、審查驗證、通知違法情況、獲取資訊，以及實地調查等調查權。
- 針對調查權之執行，依各國行政程序差異其規範略有不同，例如**德國**有要求機關在一定之期限內作出回應；**英國**則強調命提供資訊應先資訊通知；進行調查應先評估通知、獲取資訊、實地調查應先評估通知；**新加坡**則分為持法院搜索令進入場所檢查、或在必要時透過發出通知後直接進入場所檢查。

◆ 除歐盟外，多數國家未規範怠於行政處理之救濟程序

- 歐盟若獨立專責機關未處理當事人之申訴或是**未於三個月內通知調查進度或結果**，當事人有權向成員國**國內法院訴求司法救濟**。
- 其他國家多未規範怠於行政處理之救濟程序。

二、調查權之行使方式

12

■ （四）小結-2

◆ 日本、韓國可委由其他單位協助進行調查

- 日本有「**權限委任**」規定，委員會為確保個人資料適當處理必要及其他政令所訂事項，關於第146條**報告及進入檢查**之權限**得委任由事業所管大臣、金融廳、證券交易監視委員會等行使**。而前述機關應向委員會報告前項權限行使結果。（日本個資法第150條）
- **韓國**資料處理者於處理個資，而有侵害資料當事人權益時，受侵害之人得將被侵害事實向保護委員會通報，保護委員會得依施行細則**指定專門機關訊息安全局（Korea Internet & Security Agency, KISA）之隱私申訴中心**受理，調查與個資爭議有關申訴案。（PIPA第62條）
- **瑞士**得在調查範圍內**召集其他聯邦機關與地方政府警察機關執行**。（DSG 2020第50條）
- 多數國家由專責機構獨立完成調查。

二、調查權之行使方式

13

■ （四）小結-3

1. 我國個資法第22條有關行政檢查之規範，包含進入檢查、命說明提供文件、扣留等，**已有類似國際之調查權規範**，惟尚由各主管機關進行執法。
2. 我國亦可委外進行調查，日本、韓國及瑞士與外部單位合作執行調查程序；多數於調查程序中，司法不會介入調查。
3. 惟美國檢察總長隨時可介入調查程序，歐盟體系則僅在專責機關三個月未回覆調查進度或結果才可進入**司法救濟**。

二、調查權之行使方式

14

■ （五）討論議題

Q

1. 觀察我國目前目的事業主管機關之調查權與國外獨立專責機關之調查權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些調查權？
2. 未來若設置獨立個資專責機關，為避免其調查權之行使，與目的事業主管機關權限行使產生不一致，是否訂定相關衡平之規定(例如：日本個資法規定對於金融事業之調查權委託金融廳行使)？

大綱

15

一 討論範圍
二 調查權之行使方式
三 處分權之行使方式
四 附件

三、處分權之行使方式

16

■ （一）我國個人資料保護法之處分權

依個資法第25、47、48條規定，中央目的事業主管機關或直轄市、縣（市）政府對於違法者得分別處以各種裁罰性或非裁罰性之不利益處分。

個人資料保護法	
第25條	1. 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分： 一、禁止蒐集、處理或利用個人資料。 二、命令刪除經處理之個人資料檔案。 三、沒入或命銷燬違法蒐集之個人資料。 四、公布非公務機關之違法情形，及其姓名或名稱與負責人。 2. 中央目的事業主管機關或直轄市、縣（市）政府為前項處分時，應於防制違反本法規定情事之必要範圍內，採取對該非公務機關權益損害最少之方法為之。
第47條	非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之： 一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。
第48條	非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

二、處分權之行使方式

17

■ （二）國際立法例比較

權限 / 國別	相似											
	（可能違規）發布警告	（已違規）發布訓誡	命令遵循當事人要求	命令符合法規規範	命令通知侵害	課予限制	命令更正刪除	行政罰鍰	命令停止國際傳輸	執行通知（限期改正）	裁罰公務機關	其他
我國	○	○	○	○	○	○	○	○	○	○	X	
歐盟	○	○	○	○	○	○	○	○	○	○	○	
英國	○	○	○	○	○	○	○	○	○	○	○	
德國	○	○	○	○	○	○	○	○	○	○	○	
美國	X	X	○	○	○	○	○	○	X	○	X	*CPRA無國際傳輸規定
日本	○	○	○	○	○	○	○	○	○	○	○	
韓國	○	○	○	○	○	○	○	○	○	○	○	
新加坡	○	○	○	○	○	○	○	○	○	X	X	得依自願承諾書裁罰
瑞士	○	○	○	○	○	○	○	○	○	○	X	

18

三、處分權之行使方式

■（三）國際立法例- 1

國家		處分權行使要件及程序	處分權之救濟
歐盟GDPR		• GDPR §58(2)、§58(3) 糾正、授權及建議，其程序及限制由各國專責機關自行訂定	• GDPR §78 (1) 任何自然人及法人皆可對獨立專責機關具約束力之處分提起司法救濟
英國		• 依DPA 2018 §115，(c)命令控管者或處理者遵循當事人行使權利的要求、(d)處理個人資料符合規定、(e)通知個人資料之侵害、(f)課予暫時或終局之限制，包括對資料處理之禁令、(g)命令對個人資料之更正或刪除，或對資料處理之限制等、(h)撤銷或命令驗證機構撤銷所為之驗證，或命令驗證機構不得核發驗證、(j)命令對位於第三國之接收者或國際組織停止資料流通，應發出強制執行通知。 • 處以行政罰鍰前，應先發出處罰通知。	• 受通知對象28日內可向行政法院提出救濟（appeal to the Tribunal）（DPA §162），若不服可上訴至上級行政法院。
德國		• GDPR §58(2)、§58(3) 糾正、授權及建議 • 程序另依其他法令規範	專責機關之處分可由司法審查救濟
美國	CPRA	• 如經州檢察長為民事裁罰，CPPA不得再為行政裁罰，州檢察長（民事）可優先接手案件。（CPRA §1798.199.90 (c).）	• 專責機關之處分可由司法審查救濟 • 美國為司法一元制，刑事、行政訴訟皆由普通法院管轄，不另設行政法院。 • CPPA 依據 CPRA § 1798.199.50要求，向被指控違反CPRA的組織送達其舉行聽證會的合理依據時，應構成行政處分的開端。（§ 1798.199.70 (a)）

19

三、處分權之行使方式

■（三）國際立法例-2

國家	處分權行使要件及程序	處分權之救濟
日本	程序另依其他法令規範	專責機關之處分可由司法審查救濟
韓國	程序另依其他法令規範	• 若不服個資保護委員會之處分或裁罰，可由司法程序救濟。
新加坡	• 可指示當事人依循訴訟外紛爭解決機制。 • 違規指示、經濟處罰必須透過書面通知，內容包含相關作為或指示及其原因。	• 設有資料保護再申訴小組（Data Protection Appeal Panel）及資料保護再申訴委員會（Data Protection Appeal Committees）再申訴委員會擁有地區法院在審理訴訟時賦予之權力、權利和特權（強制證人出席或訊問、強制出示文件判支付費用） • 最終決定後，如不服可由司法審查救濟
瑞士	程序另依其他法令規範	專責機關之處分得對個資保護委員會提起申訴，如不服可由司法審查救濟

三、處分權之行使方式

20

■ （四）小結-1

◆ 國際各國對於專責機關之處分權內容相似

■國際各國之處分權包括發布警告、發布訓誡、命令遵循當事人要求、命令符合法規規範、命令通知侵害、課予限制、命令更正刪除、行政罰鍰、命令停止國際傳輸、執行通知（限期改正）等權限。

◆ 受到處分之救濟程序，多數國家直接進入司法救濟程序

■多數國家直接進入司法救濟程序，救濟程序之細節，亦因各國行政程序體系而略有差異，例如**美國**州檢察長雖有權優先接手案件移轉，CPPA不得限制州檢察長執行本法之權力。 CPRA §1798.199.90 (c). 但若CPPA處分已作成，則受處分企業應依據處分結果，直接進行**司法救濟**。

■**新加坡**則針對替代性紛爭解決、違規指示或自願承諾或依審查權等作出之任何指示或決定，可依書面申請由PDPC**重新再議（reconsideration）**。（PDPA第48N條）可在規定期間內向**再申訴小組主席（ the Chairperson of the Appeal Panel ）提出再申訴**。（但無論是否進行再議程序，皆可提出再申訴）（PDPA第48Q條1、2項； PDPA第65條；PDPA上訴條例）

三、處分權之行使方式

21

■ （四）小結-2

◆ 僅瑞士針對公務機關無裁罰相關規範

■除美國、新加坡之個資法本身即未規範公務機關之外，僅瑞士與我國類似，針對公務機關均無裁罰相關規範，其他多數國家之獨立專責機關可針對公務機關進行裁罰。（有關公務或非公務機關之具體裁罰標準，將於「罰則」場次進行討論）

◆ 日本可將處分權限委任其他單位

■日本有**「權限委任」**規定，委員會為確保個人資料適當處理必要及其他政令所訂事項，關於第148條**勸告及命令**之權限**得委任由事業所管大臣、金融廳、證券交易監視委員會等行使**。而前述機關應向委員會報告前項權限行使結果。（日本個資法第150條）

多數國家獨立專責機關設立皆有處分權之規範，相關權限均相似，包含命改善停止、行政罰鍰等權限。而處分之救濟，除新加坡會先經過再申訴委員會審理外，其他國家皆直接採司法程序進行救濟。而針對公務機關之裁罰，則僅我國及瑞士無類似權限。

三、處分權之行使方式

■ （四）小結-3

1. 我國個資法依個資法第25、47、48條已有規定，中央目的事業主管機關或直轄市、縣（市）政府對於違法者得處以不利益處分。包含禁止蒐集、處理或利用個人資料；命令刪除經處理之個人資料檔案；沒入或命銷燬違法蒐集之個人資料；公布非公務機關之違法情形，及其姓名或名稱與負責人等。我國相較於國際，**已有類似於國際之處分權規範**，惟尚由各主管機關進行執法。

2. **多數國家**專責機關**可針對公務機關進行處分**，除美國、新加坡本身不規範公務機關外，僅我國及瑞士之個資法並無針對公務機關之裁罰權限。

3. 多數專責機關處分結果不受上級管轄，若不服專責機關處分，新加坡另組再申訴委員會審議，其他國家則直接採司法程序救濟。

三、處分權之行使方式

■ （五）討論議題

Q

1. 觀察我國目前目的事業主管機關之處分權與國外獨立專責機關之處分權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些裁罰性或非裁罰性之不利益處分？
2. 觀察其他國家之個資法規定，對於不利益處分，訂有相關緩和作法，例如於不利益處分作成前，日本個資法規定有作成「勸告」之規定、GDPR有作成「建議」之規定，若勸告或建議之對象已為相關改善，則無後續之不利益處分；又例如日本規定個資保護委員會得授權主管機關為處分等規定，均屬個資法對於不利益處分作成之緩和措施，是否值得我國參考？
3. 未來若設置獨立個資專責機關，須否納入對公務機關之裁罰權限？

討論議題

24

案由一、調查權之行使方式

1. 觀察我國目前目的事業主管機關之調查權與國外獨立專責機關之調查權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些調查權？
2. 未來若設置獨立個資專責機關，為避免其調查權之行使，與目的事業主管機關權限行使產生不一致，是否訂定相關衡平之規定(例如：日本個資法規定對於金融事業之調查權委託金融廳行使)？

案由二、處分權之行使方式

1. 觀察我國目前目的事業主管機關之處分權與國外獨立專責機關之處分權，是否有不足之處？未來若設置獨立個資專責機關，建議增加哪些裁罰性或非裁罰性之不利益處分？
2. 觀察其他國家之個資法規定，對於不利益處分，訂有相關緩和作法，例如於不利益處分作成前，日本個資法規定有作成「勸告」之規定、GDPR有作成「建議」之規定，若勸告或建議之對象已為相關改善，則無後續之不利益處分；又例如日本規定個資保護委員會得授權主管機關為處分等規定，均屬個資法對於不利益處分作成之緩和措施，是否值得我國參考？
3. 未來若設置獨立個資專責機關，須否納入對公務機關之裁罰權限？

大綱

25

一 討論範圍
二 調查權之行使方式
三 處分權之行使方式
四 附件

歐盟相關規定

26

最近一次個資法修正：2016年（2018年施行）

獨立專責機關監督權限行使方式	
工作（第57條）	權限（第58條）
• 監督GDPR之實施、執法 • 推廣公眾對GDPR的認知 • 提倡GDPR義務 • 履行當事人之權利 • 對成員國採取個資保護措施提出建議 • 處理調查爭訟 • 與其他專責機關合作 • 主動調查 • 認可標準契約條款、行為守則、驗證制度、企業自我拘束規則 • 建立並維持資料保護影響評估清單等	• **調查權**：命令提供資訊、稽核、審查受證單位、通知違法事項、進入實體場域調查 • **糾正權**：祭出警告、公眾譴責、命令履行當事人權利、命令於期限內改善、命令進行個資事故通知、撤回驗證、祭出行政罰鍰、命令停止國際傳輸 • **授權及建議權**：諮詢及建議資料保護影響評估結果為高風險者，及核准符合公共利益之資料處理行為、發布個人資料保護意見書、核准行為守則、審核驗證機構及規則、認可標準契約條款、自行制定的契約條款、行政條款、企業自我拘束規則。

* 每一個成員國必須成立至少一間獨立專責機關 （第51條）
* 獨立專責機關不受上級審查，得向成員國國內法院提起司法救濟 （第78條）
* 當組織於多個成員國境內設有據點並互相傳輸資料時，採一站式（one stop shop）制度
* 驗證機制部分，獨立專責機關受歐盟個資保護委員會及歐盟執委會監督（第70條、第42條）

國家發展委員會

英國相關規定（1/2）

27

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

獨立專責機關【英國資訊專員辦公室】（Information Commissioner’s Office，簡稱ICO）		
職權	**內容**	**限制**
調查權	UK GPDR §58 I (a)命提供資訊 (b)進行調查：以資料保護審核（data protection audit）之形式 (c)審查驗證：對根據UK GDPR§42Ⅶ頒發的驗證進行審查 (d)通知違法情況：將涉嫌違反UK GDPR的行為通知控管者或處理者 (e)獲取資訊：自控管者或處理者處獲得 (f)實地調查：得進入控管者或處理者之任何辦公處所	➢ DPA 2018 §115 • (a)應先發出資訊通知 • (b)應先發出評估通知 • (e)(f)應先發出評估通知&遵守附錄15之程序性規定 ➢ **通知的意義：受通知對象可向法院提出救濟**（DPA 2018 §162）
裁罰權	➢ **糾正權**（UK GPDR §58Ⅱ） (a)可能違反UK GPDR時，發布警告 (b)已違反UK GPDR時，發布訓誡 (c)命令控管者或處理者遵循當事人行使權利的要求 (d)命令控管者或處理者處理個人資料符合UK GPDR之規定 (e)命令控管者向當事人通知個人資料之侵害 (f)**課予暫時或終局之限制，包括對資料處理之禁令** (g)命令對個人資料之更正或刪除，或對資料處理之限制等 (h)撤銷或命令驗證機構撤銷所為之驗證，或命令驗證機構不得核發驗證 (i) **額外或不以本項所提及之其他方式而依第83條處以行政罰鍰** (j)命令停止國際傳輸	➢ DPA 2018 §115 • (c)~(h)、(j)須先發出強制執行通知 • (i)應先發出處罰通知 ➢ **通知的意義：受通知對象可向法院提出救濟**（DPA 2018 §162）

國家發展委員會

英國相關規定（2/2）

28

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

獨立專責機關【英國資訊專員辦公室】（Information Commissioner’s Office，簡稱ICO）		
職權	**內容**	**限制**
（續）裁罰權	➢ **行政罰鍰**（UK GPDR §83） • 應確保於個案中有效、適當且具有懲戒性 • 應該要考慮違規性質、故意過失、影響個人資料情況等事項 • 最高限額為1750萬英鎊	➢ DPA 2018 §115 • 應依第155條發出處罰通知 • 得向法院提出救濟 • 可不爭論處罰之事實僅就**罰款的金額**提出救濟
其他職權	➢ **授權及建議之權力**（UK GPDR §58Ⅲ） 發布指導和授權，並使用標準契約條款來滿足資料處理和海外傳輸的要求	無限制規定
	➢ **驗證及認證相關職權**（UK GDPR §42、§43） • 驗證機構本身應有專員或國家級認證組織之認證 • 驗證機構核發及更新認證時，應先通知專員 • 專員應整理並公開資料保護驗證機制與資料保護標章及標誌	

國家發展委員會

德國相關規定（1/2）

29

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

調查權 公務機關BDSG § 2(1) (2)、§ 7-§ 16 非公務機關BDSG § 37-§ 38		
公務機關	聯邦個人資料保護暨資訊自由監察官	責任義務§ 7 ➢ 告知並提供建議。 ➢ 監督及管理。 ➢ 與監督機關共同合作。
	各邦設置之資料保護監察官	職務權責§ 8-§ 16 ➢ 組織設立、監察官之獨立性、監察官之任用及任期、權利及義務以及相關職務權限。 ➢ 非公務機關或個人違反個資法：通知主管機關+給予主管機關在合理期限內對資料控管者提供建議的機會。 ➢ 聯邦公務機關違反個資法：向聯邦最高主管機關提出投訴+要求該機關在一定之期限內作出回應。
非公務機關		§ 37-§ 38 ➢ 資料控管者及受託處理者經常性雇用至少二十名雇員，則應指定一名資料保護長。

國家發展委員會

德國相關規定（2/2）

30

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

裁罰權BDSG § 41-§ 43
GDPR § 83(4)-(6)

BDSG	➢ §42(1)將未公開之個人資料，基於商業之目的予以傳輸第三方或使其取用，將處以3年以下有期徒刑或罰金。 ➢ (2)將未公開之個人資料，基於對價或基於滿足自己或侵害他人之意圖，最高得處以2年有期徒刑或罰金。 ➢ §43未能妥適地處理資訊的請求、未通知消費者、行為不正確、不完整或延遲者最高得處以5萬歐元之行政罰鍰。
GDPR	➢ §83(4)最高1,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之。 ➢ (5)最高2,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之4%。 ➢ (6)最高2,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之4%。 ->以上皆以數額高為優先。

認證BDSG § 39
GDPR § 43(1)

➢ 允許具有適當專業知識水準的認證機構於必要時行使權力，頒發和更新認證。
➢ 認證機構之權力來源應由聯邦或各州的監管機構授予。

美國相關規定

31

無聯邦個資法，加州消費者隱私法（CCPA）最近修正為 2018 年，修正 CCPA 的新法 CPRA 將於 2023 年實施，效力溯及 2022 年 1 月 1 日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於 2021 年訂定統一個資保護法（UPDPA），目前已陸續有州提案。
CBPR成員國

獨立專責機關		組織型態及規定	權責
CPRA	加州隱私保護機關（California Privacy Protection Agency, CPPA）	5人委員會，其中1主席及1名委員由州長任命，另3名分別由州檢察長、州參議院規則委員會、州眾議院議長任命（*§1798.199.10-30*） **委員獨立性**，委員應免於外部直接、間接之影響，且不得尋求或接受他人之指示。（*§1798.199.15(c)*）	CPRA之行政執法主管機關 • 更新現有規範 • 訂立施行規範、解釋規範 • 受理申訴 • **受理申訴調查或主動調查** ➢ 可決定不查、給予改正期 ➢ 書面回覆申訴人（如有） • 違規案件執法（行政） ➢ 聽證通知（加州行政程序法） ➢ 命令停止、中止行為 ➢ 可處行政罰鍰（*§1798.199.55*） ➢ 可司法審查救濟（*§1798.199.85*） • 提供立法機關諮詢意見（*§1798.199.10 (a) - (l)；1798.199.45-65*）
		委員資格 • 加州人，具隱私和科技領域資格、經驗、能力（*§1798.199.15*）	
		特殊規定 • 委員會應於主席外另任命1執行委員 • 委員任期不得超過連續8年 • 卸任後1年內，不得接受其任內或就任前五年期間曾受CCPA、CPRA執行或民事訴訟之企業之罷課 • 卸任後2年內，不得以影響CPPA之行為為目的任CPPA機關待決案件之相關人的有酬代理人或律師（*§1798.199.15-20*）	
		委員薪酬 • 薪酬：100 USD / 執行公務日，每兩年依物價調整（*§1798.199.25*）	
UPDPA	N/A	UPDPA 旨在提供靈活性、泛州適用，執法和規則制定事宜，安排留給**現有州法、州檢察長**處理 • 違反UPDPA之執法機關、救濟、處罰依**該州消費者保護法**規定 • 另**州檢察長**可依該州行政程序法實施UPDPA，司規則訂定權力（*UPDPA §16*）	N/A

日本相關規定

32

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

監督對象	監督權限行使方式
非公務機關	• **報告及進入檢查**（§146）：得要求個人資料處理事業者就個人資料之處理提出必要之報告或資料，或得使其職員進入該當個人資料處理事業等之事務所、其他必要場所，命其說明有關個資處理或檢查其他相關文件。 • **指導及建議**（§147）：得對個人資料處理事業者提供關於個人資料處理之必要指導及建議（無法律拘束力）。 • **勸告及命令**（§148）：得勸告個人資料處理事業者將違反行為中止或為改正所應採取之其他必要措施 • **委員會權限行使之限制**（§149）：應不得妨礙表現自由、學問自由、信仰自由及政治活動自由；對豁免規定（§57）所列人員不得行使監督權限。
公務機關	• **要求提出資料及實地調查**（§156）：為確保行政機關等的義務之規定順利運用而認為有必要時，得要求行政機關首長對行政機關就個人資料處理之相關事務的實施狀況，提出資料並且進行說明，或得使其職員進行實地調查。 • **指導及建議**（§157）：同§156得進行必要之指導或給予建議。 • **勸告**（§158）：同§156得進行勸告。 • **基於建議所採取措施之報告要求**（§159）：得要求該行政機關首長報告其根據該勸告所採取的措施。 • **委員會權限行使之限制**（§160）：同§149當行政機關首長依豁免規定提供個資，不得行使監督權限。
認定個人資料保護團體	• **報告之提出**（§153）：於施行第4章第5節「民間團體推動個人資料保護」之必要範圍內，對於認定個人資料保護團體得使其為有關認定業務之報告。 • **命令**（§154）：於施行第4章第5節「民間團體推動個人資料保護」之必要範圍內，對於認定個人資料保護團體得命其為認定業務施行方法之改善、變更個人資料保護指引及其他應採取之必要措施。 • **認定之撤銷**（§155）：於確認認定個人資料保護團體有該當失格、違反前條命令、不正當手段受認定等情形時得撤銷其認定，且委員會依同條第2項規定應將撤銷認定公告之。

國家發展委員會

韓國相關規定（1/2）

33

最近一次個資法修正：2020年（ 2021年9月28日提出「個人資料保護法修正草案」在國會審議中）
CBPR成員國、GDPR適足性（2021）

- 一、為符合GDPR適足性要求，針對個資委員會規定之修法重點：
  - 整合過去隸屬行政安全部之職權，修正為保護委員會執掌，以集中管理
  - 強化委員會功能，增訂委員專業性、獨立性、任期及身分保證的規定
  - 個人資料保護委員會的層級提升為中央行政機關
  - 除了舊法既有之勸導改善功能外，修法後賦予其行政罰鍰之裁處權
- 二、保護委員會職權（ PIPA第7條之8參照）：

現行保護委員會執權	
檢視個人資料保護相關法令	與國際機構關於個人資料保護之交流與合作
建立並執行個人資料保護政策、制度及計畫	調查、研究與教育、宣傳個資法令、政策、制度與實務
對資料當事人之權利侵害調查其處分事宜	支持個人資料保護技術發展及專門人才培育
個人資料權利救濟及相關爭議之調解	依本法及其他法定所訂之規定

  - 上述保護委員會職權，大致可歸納為（1）調查資料當事人權利侵害及裁處事項、（2）制定、執行、改善個資保護政策與制度、（3）國際參與及制度推廣（包含認證標章之推行）。

國家發展委員會

韓國相關規定（2/2）

- 三、調查權之行使與限制（ 63條賦予委員會資料請求權及實地稽查之權利）：
  - 於符合下列各款情形之一者，保護委員會得發動調查權：
  (1)有違反本法所定之事項或得知有嫌疑
  (2)接獲通報或申訴時
  (3)為保護資料當事人所必要的事項由施行細則定之
  (4)稽核與行政檢查
  - 另應注意執行上述調查應確保相關文件及證據有相關安全保護措施不會被流出，並應遵守相關保密義務。

- 四、裁罰權之行使與限制：

違反義務	裁罰之行使與限制之規定
假名資料處理義務之違反（第28條之6）	資料控管者若違反處理假名資料之禁止義務（第28條之5第1項），保護委員會得課以整體銷售總額百分之三以下之行政罰鍰；但無整體銷售總額或計算顯有困難時，得施行細則規定，以4億韓圜或資本額百分之三取高者課與罰鍰
資料控管者若違反處理假名資料之禁止義務（第28條之5）	保護委員會應評估(a)履行第24條第3項必要安全管理措施之努力程度、(b)受侵害及毀損程度、(c)積極防止侵害擴散。
資通訊業者處理個資義務之違反（第39條之15）	保護委員會得依違反行為對其課徵銷售額百分之三以下之罰鍰

  - 滯納金、怠金：依照PIPA第75條規定，由保護委員會與相關中央行政機關首長課徵。

新加坡相關規定

最近一次個資法修正：2020年；CBPR成員國

類型	權限	權限內容
調查權	審查權限	針對機關團體拒絕提供或拒絕更正申訴人之個資、超過合理時間仍未提供或更正等情事，個人資料保護委員會得確認或推翻該等拒絕提供或拒絕更正之決定；另針對機關團體向申訴人就取得或更正個資收取之費用，個人資料保護委員會亦得進行審核，並得確認、減少或禁止該等費用，或要求該等機關團體退費予申訴人（PDPA第48H條）
	調查權限	PDPC及其內部調查員，得依據申訴案或主動調查組織是否確實遵守該法規定，接受組織的書面自願承諾書 ，以糾正違規行為並防止其再次發生，亦得裁量申訴案是否為惡意申訴或濫訴，以決定是否受理、暫停或終止調查（PDPA第48L條、第50條、附表9）
裁罰權	接收自願承諾、提出指令及裁罰權限	組織得向PDPC提出書面自願承諾書（Voluntary undertakings），如組織未遵守PDPA有關個資保護之一般性規範、個資之蒐集、利用、揭露、取得、更正及維護等規定，PDPC得對該等機關團體提出要求，強制其停止相關個資蒐集、利用或揭露等行為、銷毀違法蒐集之個資，或對其裁罰等；（PDPA 第48I條）且該等要求可由新加坡法院強制執行；如未經他人授權不當更正其個人資料，PDPC得對該自然人或組織處以5,000新幣以下的罰鍰，或12個月以下的有期徒刑（PDPA第48J條）
其他職權	發布法規與解釋權限	經部會首長同意下，得於達成該法目的之必要範圍內，發布相關授權命令或制定適當之規範 。提供與資料保護相關之諮詢、建議及技術管理或其他專門人員之服務 ；得隨時發布相關法規解釋建議之書面準則，並隨時修正或廢止之。（PDPA第65條、第6條b項、第49條）
	訴訟外紛爭解決	PDPC認為個人（申訴人）對某個組織之任何申訴，以調解方式解決更恰當，得在未經申訴人與該組織同意情況下，根據紛爭解決機制將該事宜提交調解（PDPA第48G條）
	監督「拒絕來電」制度運作	維運拒絕來電登記處（Do-Not-Call Registry），資料當事人可以在拒絕來電登記處註冊其位置在新加坡之電話號碼，以防止私人機關為了商業行銷之理由而進行電話行銷，假設資料當事人已完成相關登記卻持續收到行銷電話時，可以向PDPC進行申訴。（PDPA第39條）

瑞士相關規定

最近一次個資法修正：2020年（尚未施行，施行日期由行政機關決定）
GDPR適足性認定（指令時代取得）

依據DSG 2020第7節設有「聯邦資料保護及資訊專員（Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte, EDÖB）之相關規定。

調查權之相關規定	• EDÖB得依第49條對於資料處理可能違反資料保護之聯邦機構或個人進行調查，並命其提供調查所需資料及相關文件，且應告知其所採取之措施及調查之結果。 • EDÖB得依第50條對於聯邦機構或個人未履行合作義務所採行之措施包括：（1）近用調查所需相關資訊、文件、處理活動列表及個人資料；（2）進入處所及設施；（3）詢人訊問；（4）專家評估。
裁罰權之相關規定	• EDÖB得依第51條命令有違反本法之資料處理為全部或部分調整、終止或中斷，並全部或部分刪除、銷毀；違反國際傳輸規定者得命其推遲或禁止。 • EDÖB得依第60條對於故意提供虛假或不完整資訊、未履行通知義務、未履行知情權義務等；第61條違反注意義務、第62條違反職業機密、第63條無視命令、第64條業務違規等規定得對個人處以最高25萬瑞士法郎之罰款。
其他相關職權	• EDÖB得依第56條登記之規定，EDÖB負責對聯邦機構的資料處理活動進行登記並公佈。 • EDÖB依第57條規定應每年向聯邦議會報告其活動情形；另依第58條第1項EDÖB之任務尚包括：（1）向聯邦機構及個人提供資料保護方面之資訊、培訓及建議；（2）協助地方機構並與負責資料保護之外國政府合作；（3）提升民眾對資料保護之重視；（4）向當事人提供有關如何行使其權利的資訊；（5）針對資料處理之法令草案及聯邦措施表示意見；（6）執行《公共資料法》或其他聯邦法律分配之任務；（7）開發工具以提供良好作法之建議。

「個人資料保護法相關議題」第 12 場產學專家學者諮詢會議—罰則

議程

壹、背景說明

我國電腦處理個人資料保護法自 84 年公布施行後，雖曾於 99 年全盤修正並更名為個人資料保護法（下稱個資法），並嗣經 104 年部分修正。然隨著數位經濟與資訊科技之迅速發展，個人資料已成為大數據分析之重要來源，故各國對於如何促進資料流通並兼顧個資保護，多已進行相關修法與檢討，為使我國個資法與時俱進並與國際接軌，本會規劃就個資法重要議題：豁免情形、域外效力、國際傳輸、蒐集處理利用之合法要件探討（不含「當事人同意」要件）、受託處理者義務、產業應用（含科學研究、假名化、匿名化）、當事人權利（資料可攜權、被遺忘權、權利限制規定）、獨立專責機關監督權限行使方式、罰則等議題，參考國際立法例並規劃依議題別陸續邀請專家學者召開會議，廣泛徵集修法意見。

本次諮詢會議藉由比較歐盟「一般資料保護規則」(GDPR)、英國「一般資料保護規則」、德國「聯邦資料保護法」、美國「加州隱私權法」（CPRA）、日本「個人資料保護法」、韓國「個人資料保護法」、新加坡「個人資料保護法」及菲律賓「個人資料保護法」規範內容，借鏡並擬定我國「個人資料保護法」的法制調適取向，就「罰則」之裁罰之標準、金額、刑度等進行討論，並以「個資法」為主要討論範疇。裁罰性不利益處分已於前場次討論，爰不在本次會議討論之列。

貳、議程

一、 主席致詞

二、 報告事項

罰則（國發會）

三、 討論事項

案由一、行政罰

說明：

一、 我國個資法之行政罰規定

我國個資法之行政罰規定於第 47 條至第 50 條，依據個資法第 47 條，非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之：一、違反第六條第一項規定。二、違反第十九條規定。三、違反第二十條第一項規定。四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。

而依據個資法第 48 條，非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰：一、違反第八條或第九條規定。二、違反第十條、第十一條、第十二條或第十三條規定。三、違反第二十條第二項或第三項規定。四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。

此外，依據個資法第 49 條，非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。依據個資法第 50 條，非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

二、 外國相關立法例

綜觀各國法制，可見以下情形：

(一) 多數國家針對個資法設有行政罰

除菲律賓未制定行政罰外，歐盟體系、英國、美國、日本、韓國、新加坡皆有行政罰相關規定。

(二) 罰鍰係固定額度上限或依受處分對象規模調整，各國規範不同

1. 歐盟 GDPR、德國、英國、新加坡、韓國係依據受處分對象規模計算比例，調整裁罰金額。

(1) 歐盟 GDPR、德國處最高 2,000 萬歐元或 4%全球營業額。（依較高者）

(2) 英國最高 1750 萬英鎊或前一會計年度全球年營業額之 4%。（依較高者）

(3) 新加坡原為固定額度上限，2020 年修法後大幅加重罰款額度及增加依比例計算之規定，一般中小企業仍維持固定額度，上限最高 100 萬新幣；新加坡年營業額 1000 萬新幣以上之組織，最高處新加坡年營業額 10%。

(4) 韓國則為 4 億韓圜或資本額 3%。（依較高者）

2. 美國、日本罰鍰係固定額度上限

(1) 美國 CPRA 在規範對象的規定已排除小規模企業，故 CPRA 罰鍰額度雖可調整，其考量因素不包括處分對象規模，而係企業的善意合作作為。罰鍰最高為 2,500 美元，或於每項故意違規行為、每項涉及未成年消費者個人資料的違規行為處以最高 7,500 美元行政罰鍰。

(2) 日本為固定罰鍰額度上限，最高為 10 萬日幣以下罰鍰。

(三) 各國並未要求須先命其改正才可處罰

歐盟體系、英國、美國、日本、韓國、新加坡皆未要求專責機關須先命令其改正後，未改正再進行行政裁罰。

(四) 多數國際立法例於法人處罰時，未同時於個資法規範處罰其負責人或其他有監督管理責任者

1. 多數國家皆針對法人有行政罰。

2. 但除新加坡外，多數國家未處罰其負責人或其他有監督管理責任者。

3. 新加坡處罰組織高層或參與管理且可影響違法之個人。若同意或縱容或與他人共謀實施違反本法行為；或以任何其他方式（不論作為或不作為），明知其涉及或參與組織違反本法行為；或明知或可得而知或可預期組織違反本法，而未採取一切合理步驟防止或制止者，一經確定，應受到相應的懲罰。

4. 韓國雖無針對負責人之行政罰，但在刑事部分，尚得對該法人之代表人、代理人、使用人及其他從業員課處對應條文之罰金刑。

(五) 除美國、新加坡未規範公務機關外，多數國際立法例皆有針對公務機關處罰。

三、 小結

(一) 相較於國際立法例未要求須先命其改正才可處罰，我國則在個資法第 47 條至第 50 條針對行政罰規定中，分別有不同規範。針對第 47 條為同時命改正及處罰；第 48 條則須先命改正，未依命令改正者再為行政罰鍰；第 49 條則無命改正相關規定。

(二) 多數國際立法例有裁罰公務機關，我國則未針對公務機關有裁罰機制。在非公務機關部分，我國另針對非公務機關受罰鍰處罰時，其代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。新加坡亦有處罰負責人之規定，但要件限縮於明知違反個資法等情形。

(三) 歐盟體系、英國、新加坡、韓國罰鍰係依據受處分對象規模調整，以針對不同規模的對象達成懲罰效果，而我國罰鍰係採固定額度上限。

(四) 綜觀各國行政罰，主要係針對違反資料運用之合法要件、控管者義務、當事人權利、目的外利用、國際傳輸、妨礙調查等情形規範，且針對特種個資之處理有較重的罰則。較具特

色的規範模式，如美國僅有行政罰，菲律賓則無行政罰之規範。

四、 討論議題

根據以上觀察，請產學專家就以下議題提供建議：

(一) 各國未要求須先命其改正才可處罰，我國個資法第 48 條則需先命改正後未改善，才得處罰(例如：非公務機關違反第 27 條第 1 項規定，未採行適當之安全措施，發生個資外洩)，是否需調整？

(二) 未來我國設置個資保護獨立監督機制後，須否納入對公務機關之裁罰權限？若納入，考量公務機關類型多元(包含中央五院及所屬機關、地方自治機關、各級法院等)，是否須與非公務機關之裁罰有差異？或有其他可行方案？

(三) 歐盟體系、英國、新加坡、韓國罰鍰係依據受處分對象規模調整，以針對不同規模的對象達成懲罰效果，而我國罰鍰目前係採固定額度上限之作法，若我國欲依據受處分對象規模調整，建議採何標準（如資本額、當地營業額、全球營業額之比例）？

(四) 我國針對非公務機關之代表人、管理人或其他有代表權人，有受同一額度罰鍰之處罰，但多數國家未於個資法訂有相關規範，我國是否仍維持特殊規範或回歸行政罰法第 15 條規定適用即可？

案由二、刑事罰

說明：

一、 我國個資法之刑事罰規定

個資法第 41、42、44、45、46 條規定刑事罰之罰則，我國刑事罰依其意圖限縮處罰範圍，限定於意圖為自己或第三人不法之利益或損害他人之利益之情形。

又依據個資法第 41 條，意圖為自己或第三人不法之利益或損害他人之利益，而違反第六條第一項、第十五條、第十六條、第

十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。而依據個資法第 42 條則規定，意圖為自己或第三人不法之利益或損害他人之利益，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。

其中，第 41 條修正說明如下：行為人非意圖為自己或第三人不法之利益或損害他人之利益，而違反本法相關規定者，因其可受非難性之程度較低，原則以民事損害賠償、處以行政罰為已足。惟行為人如有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定，因其可受非難性之程度較高，仍有以刑罰處罰之必要，爰為本條之修正。

另個資法第 44 條規定公務人員之加重條款，針對公務員假借職務上之權力、機會或方法，犯本章之罪者，加重其刑至二分之一。第 45 條規定本章之罪，須告訴乃論，但犯第 41 條之罪者，或對公務機關犯第 42 條之罪者，不在此限。第 46 條規定犯本章之罪，其他法律有較重處罰規定者，從其規定。

二、 外國相關立法例

(一) 除美國 CPRA 無刑事罰，及歐盟 GDPR 未統一規範刑事罰，其他國家皆有刑事罰

1. 歐盟 GDPR 將刑事罰的訂定權限給予各成員國，惟各成員國制定後應向歐盟報備。

2. 美國 CPRA 並未規定刑事罰則；英國、德國、日本、韓國、新加坡、菲律賓皆有刑事罰相關規定。主要針對明知、違反委員會命令、偽證等情形有以刑事罰規範。並對故意、有意圖營利、不當手段的有較重罰則。

(二) 多數國家之財產刑係固定額度上限

1. 美國 CPRA 無刑事罰、歐盟 GDPR 無統一規範刑事罰。

2. 英國、日本、韓國、新加坡、菲律賓皆針對財產刑採固定額度上限。

(1) 英國最高為 5000 英鎊以下罰金；

(2) 日本最高為 100 萬日幣以下罰金；

(3) 韓國最高為 1 億韓圜以下罰金；

(4) 新加坡最高為 1 萬新幣以下罰金；

(5) 菲律賓最高為 400 萬比索以下罰金。

3. 德國刑事罰依犯罪行為人之收入、財產及其他量處每日額罰金額之基礎，最高為 360 日整日額。（德國刑事法特殊計算方式）

(三)各國自由刑之額度多為 1~3 年，韓國最高至 10 年有期徒刑

1. 美國 CPRA 無刑事罰、歐盟 GDPR 無統一規範刑事罰；英國刑事罰未包含自由刑。

2. 德國、日本、韓國、新加坡、菲律賓有以自由刑作為刑事罰懲罰手段。德國最高為 3 年以下有期徒刑；日本最高為 2 年以下有期徒刑；韓國最高為 10 年以下有期徒刑；新加坡最高為 3 年以下有期徒刑；菲律賓為 1 年以上、5 年以下有期徒刑。

(四)有刑事罰則之國家，皆有處罰過失：英國、德國、日本、韓國、新加坡、菲律賓皆有處罰過失。

(五)是否依據其意圖限縮刑事罰範圍

多數國家未依據其意圖限縮刑事罰範圍，但韓國針對「以妨害個資處理業務為目的」及「以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供、教唆或幫助者」另有較重之刑事罰則。

(六)日本、韓國、菲律賓針對身分有特別規定

1. 日本、菲律賓皆針對公務員身分有加重處罰之規定。

2. 韓國則針對資通訊業者，設有資通信業者專章特別義務規定。

(七)僅有菲律賓於個資法規範違反個資法規範之數個犯罪行為樣

態有結合或接續之狀態，加重刑事處罰。

(八)各國刑事罰客觀要件不同，除各國刑事體系差異外，有部分特別以刑事罰處罰的項目。例如，日本有將違反委員會命令等行為納入刑事罰規範，新加坡亦有將未經同意行使當事人權利、更改、偽造、隱藏或銷毀，或教唆者拒絕提供委員會資料或偽證等納入刑事法規範。

三、 小結

(一) 我國個資法第 41、42、44、45、46 條針對刑事罰之規定，皆處罰故意犯，未處罰過失犯。最高為五年以下有期徒刑，得併科新臺幣一百萬元以下罰金，另針對公務人員有加重規定。

(二) 雖部分國家在行政罰會依據受處分對象規模調整，但在刑事罰之罰金部分，皆似我國罰金係採固定額度上限之作法。綜觀罰金金額大約為 20 萬臺幣至 200 萬臺幣區間，我國為 100 萬臺幣以下，罰金之金額居中。

(三) 目前國際立法例僅韓國有特別針對意圖部分有加重刑責規定，多數國家未針對意圖限縮刑事罰範圍。我國原則以民事損害賠償、行政罰，將刑事罰限縮在行為人有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定之情形。

四、 討論議題

根據以上觀察，請產學專家就以下議題提供建議：

(一) 多數國際立法例未根據「意圖」限縮刑事罰範圍，且有處罰過失情形，處罰範圍較大，韓國特別針對意圖部分有加重刑責規定，我國目前僅針對「意圖為自己或第三人不法之利益或損害他人之利益」之情形懲罰，是否增加過失犯之刑事罰？是否增加其他犯罪行為樣態之刑事罰，如韓國「以妨害個資處理業務為目的」及「以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供、教唆或幫助者」？

(二) 日本有針對違反主管機關命令、偽證等情形以刑事罰規範；新加坡亦有針對偽證情形有以刑事罰規範；未來我國設置個資保護獨立監督機制後，是否增加相關刑事罰則？

(三) 因個資法規範之行為特性，可能涉及在同一個資法規範數個犯罪行為樣態有結合或接續之狀態，參考菲律賓針對此有結合犯或接續犯之規定，並加重刑事處罰，我國是否參考菲律賓模式增訂相關規範？

罰則

國家發展委員會
111 年 10 月 3 日

背景說明

1

隨著數位經濟與資訊科技的蓬勃發展，人工智慧、巨量分析、演算法或物聯網等新興科技的應用，涉及大量個人資料的蒐集、處理和利用，在國際上法制與實務均快速發展的情況下，我國為**保障當事人個資安全及隱私保護**，並同時**促進資料流通及資料經濟**，爰有重新檢視個資隱私相關重要性議題之必要，俾利精進及調和我國個資法制與時俱進接軌國際。

場次	1	2	3	4	5	6	7	8	9	10	11	12
主題	蒐集、處理、利用之合法要件探討（一般個資）	蒐集、處理、利用之合法要件探討（特種個資）	產業應用（科學研究）	產業應用（匿名化、假名化）	受託處理者義務	國際傳輸	規範主體、行為區分與特定目的之解釋	資料可攜權、被遺忘權	權利限制規定	豁免情形、域外效力	獨立專責機關監督權限行使方式	罰則
日期	110/10/6	110/11/3	110/12/6	111/1/13	111/2/25	111/3/2	111/4/6	111/5/20	111/6/20	111/7/25	111/8/24	111/10/3

國家發展委員會

大綱

2

一 討論範圍

二 行政罰

三 刑事罰

四 附件

一、討論範圍（1/2）

3

■ 討論範圍

討論「罰則」之裁罰之標準、金額、刑度等，並以「個資法」為主要討論範疇。裁罰性不利益處分已於前場次討論。

■ 比較國家

國別	規範名稱	修正時間	特性
我國	個人資料保護法	2015	CBPR成員、GDPR適足性諮商中
歐盟	一般資料保護規則（GDPR）	2016	
德國	聯邦資料保護法	2021	歐盟成員
英國	資料保護法（DPA）	2020	歐盟前成員、GDPR適足性（2021）
美國	加州隱私權法（CPRA）	2020	CBPR成員
日本	個人資料保護法	2022	CBPR成員、GDPR適足性（2019）
韓國	個人資料保護法	2020	CBPR成員、GDPR適足性（2021）
新加坡	個人資料保護法	2020	CBPR成員
菲律賓	個人資料保護法	2012	

一、討論範圍（2/2）

■ 經整理各國罰則主要分為：

類型	分析架構
行政罰	有無行政罰
	罰鍰係固定額度上限，或得依據受處分對象規模調整
	是否須先命其改正
	是否針對法人處罰
	是否處罰其負責人或其他有監督管理責任者
	是否處罰公務機關
刑事罰	有無刑事罰
	財產刑係固定額度上限，或得依據受處分對象規模調整
	自由刑之額度
	是否處罰過失
	是否依據其意圖限縮刑事處罰範圍
	是否依其身分有特別規定（如公務員）
	是否針對法人處罰

大綱

一 討論範圍
二 行政罰
三 刑事罰
四 附件

二、行政罰

6

■（一）我國個人資料保護法之罰則

依個資法第47條至第50條規定，有關行政罰之罰則。

個人資料保護法	
第47條	非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣五萬元以上五十萬元以下罰鍰，並令限期改正，屆期未改正者，按次處罰之： 一、違反第六條第一項規定。 二、違反第十九條規定。 三、違反第二十條第一項規定。 四、違反中央目的事業主管機關依第二十一條規定限制國際傳輸之命令或處分。
第48條	非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府限期改正，屆期未改正者，按次處新臺幣二萬元以上二十萬元以下罰鍰： 一、違反第八條或第九條規定。 二、違反第十條、第十一條、第十二條或第十三條規定。 三、違反第二十條第二項或第三項規定。 四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。
第49條	非公務機關無正當理由違反第二十二條第四項規定者，由中央目的事業主管機關或直轄市、縣（市）政府處新臺幣二萬元以上二十萬元以下罰鍰。
第50條	非公務機關之代表人、管理人或其他有代表權人，因該非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。

二、行政罰

7

■（二）國際立法例比較-1

國別	有無行政罰	罰鍰係固定額度上限，或得依據受處分對象規模調整	是否以命令改正為前提	是否針對法人處罰	是否處罰其負責人或其他有監督管理責任者	裁罰公務機關
我國	○	固定額度	§47併行；§48先命改正；§49無命改正規定	○	原則併罰；已盡防止義務者不罰	X
歐盟	○	併行	X	○	X	○
英國	○	併行	X	○	X	○
德國	○	併行	X	○	X	○
美國	○	固定額度	X	○	X	—
日本	○	固定額度	X	○	X	X(另有刑事罰)
韓國	○	併行	X	○	X	○
新加坡	○	併行	X	○	§52同意知情或未盡防止義務者	—
菲律賓	X	—	—	—	—	— (另有刑事罰)

註：本表格僅以個資法為討論範圍

二、行政罰

（二）國際立法例比較-2

8

紫色：各國特有規定

重：處罰較嚴格之項目

國別	條號	對象	要件	效果
我國	§47	非公務機關	違反特種個資、蒐集、處理或利用之合法要件(下稱合法要件)、目的外利用、國際傳輸	重 處罰鍰並限期改正；未改正，按次罰之新臺幣五5萬元以上50萬元以下
	§48		違反告知義務、當事人權利、行銷、適當安全措施、訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法	先限期改正；未改正，再處罰鍰，按次罰之新臺幣2萬元以上20萬元以下
	§49		規避、妨礙或拒絕進入、檢查或處分	處罰鍰 新臺幣2萬元以上20萬元以下
	§50	非公務機關代表	非公務機關依前三條規定受罰鍰處罰時，除能證明已盡防止義務者外	受同一額度罰鍰之處罰
歐盟	§83	資料控管者或資料處理者	違反控管處理者義務、驗證機構義務、行為守則監管機構義務	處罰鍰，最高1,000萬歐元或2%全球營業額
			違反處理原則、當事人權利、特種個資處理、國際傳輸、監管機關限制資料傳輸之命令、監管機關之調查權及糾正權	重 處罰鍰，處最高2,000萬歐元或4%全球營業額
英國	UK GDPR §83	資料控管者或資料處理者	違反控管處理者義務、驗證機構義務、行為守則監管機構義務	最高處以870萬英鎊，或2%全球營業額
			違反處理原則、當事人權利、特種個資處理、國際傳輸、監管機關限制資料傳輸之命令、監管機關之調查權及糾正權	重 最高處以1750萬英鎊，或4%全球營業額

各國的行政罰，主要係針對違反合法要件、控管者義務、當事人權利、目的外利用、國際傳輸、妨礙調查等情形規範。並針對特種個資之處理有較重的罰則。

國家發展委員會

二、行政罰

（二）國際立法例比較-3

9

紫色：各國有規定

重：處罰較嚴格之項目

國別	條號	對象	要件	效果
德國	§41	資料控管者或資料處理者	違反控管處理者義務、驗證機構義務、行為守則監管機構義務	處罰鍰，最高1,000萬歐元或2%全球營業額
			違反基本處理原則規定、權利規定、國際傳輸規定、特殊資料處理情形規定、監管機關限制資料傳輸之命令、監管機關之調查權及糾正權	重 處罰鍰， 處最高2,000萬歐元或4%全球營業額
	§43	任何機構	故意或過失違反其他歐盟境內借貸方(Darlehensgeber)關於評估消費者信譽之資訊請求(§30 I)、故意或過失未正確、未完全或未及時告知消費者，借貸方據以不予簽訂消費借貸契約或有償經濟援助契約之資訊(§30 II S. 1)	5萬歐元；公務機關金額不在此限
美國 CPRA	§179 8.199 .55	營利事業	(美國無刑事罰，所有違規行為皆為民事或行政罰) 所有違反CPRA之行為	有合理依據，舉辦聽證確定違規發布命令要求停止；及/或罰鍰 每項2,500 美元；最高每項7,500 美元
日本	§185	非公務機關	違法向第三方提供個資、冒用認定個資保護團體名稱、未申報或不實申報個資保護團體、以詐欺或其他不當方法取得行政機關揭露保有個資之決定	10萬日幣以下罰鍰
韓國	§39-15	資通訊業者	違反合法要件、受託者義務、安全管理措施、國際傳輸	原則銷售總額3% 例外4億韓圓
	§75	資料控管者或資料處理者	違反合法要件、當事人權利、告知義務、安維措施、個資外洩通知設置及運作影像處理器義務、虛偽認證、指定國內代理人、指定個資保護員、設置流動性風控必要措施*、委託規定、文件紀錄保存管理、行政檢查	怠金 5千萬、3千萬、2千萬及1千萬韓圓
	§28-6		以識別特定個人為目的而處理假名資料	原則資本額3% 例外4億韓圓或資本額3%孰高
新加坡	§48J	組織	故意或過失違反一般規則、當事人同意、當事人權利、資料保存、外洩通知	書面通知、罰鍰 當地年營業額10%或100萬新幣罰較
		個人	故意或過失違反或使用字典式攻擊或地址蒐集軟體規定	

國家發展委員會　註：菲律賓未規定行政罰，故不列入表格　*設置流動性風控必要措施：未有保險或加入公債、提撥準備金等必要措施者

10

二、行政罰

■ （三）小結-1

1. 多數國家針對個資法設有行政罰

除**菲律賓**未制定行政罰外，**歐盟體系、英國、美國、日本、韓國、新加坡**皆有行政罰相關規定。

2. 罰鍰係固定額度上限或依受處分對象規模調整，各國規範不同

1) 歐盟GDPR、德國、英國、新加坡、韓國係依據受處分對象規模計算比例，調整裁罰金額。

① **歐盟GDPR、德國**處最高2,000萬歐元或**4%全球營業額**。（依較高者）

② **英國**最高1750萬英鎊或前一會計年度**全球年營業額之4%**。（依較高者）

③ **新加坡**原為固定額度上限，2020年修法後大幅加重罰款額度及增加依比例計算之規定，一般中小企業仍維持固定額度，上限最高100萬新幣，新加坡年營業額1000萬新幣以上之組織，最高處**新加坡年營業額10%**。

④ **韓國**則為4億韓圜或**資本額3%**。（依較高者）

2) 美國、日本罰鍰係固定額度上限

① **美國**CPRA在規範對象的規定已排除小規模企業，故CPRA罰鍰額度雖可調整，其考量因素不包括處分對象規模，而係企業的善意合作作為。罰鍰最高為2,500美元，或於每項故意違規行為、每項涉及未成年消費者個人資料的違規行為處以最高7,500 美元行政罰鍰。

② **日本**為固定罰鍰額度上限，最高為10萬日幣以下罰鍰。

11

二、行政罰

■ （三）小結-2

3. 各國並未要求須先命其改正才可處罰

歐盟、德國、英國、美國、日本、韓國、新加坡皆未要求專責機關須先命令其改正後，未改正再進行行政裁罰。

4. 多數國際立法例於處罰法人時，未同時於個資法規範處罰其負責人或其他有監督管理責任者

1) 多數國家皆有針對法人有行政罰。

2) 但除新加坡外，多數國家未處罰其負責人或其他有監督管理責任者。

3) **新加坡**處罰組織高層或參與管理且可影響違法之個人。若**同意**或**縱容**或**與他人共謀**實施違反本法行為；或以任何其他方式（不論作為或不作為），**明知**其涉及或**參與**組織違反本法行為；或**明知或可得而知**或**可預期**組織違反本法，而**未採取一切合理步驟防止或制止者**，一經確定，應受到相應的懲罰。

4) **韓國**雖無針對負責人之行政罰，但在刑事部分，尚得對該法人之代表人、代理人、使用人及其他從業員課處對應條文之罰金刑。

5. 除美國、新加坡未規範公務機關；多數國際立法例皆有針對公務機關處罰

二、行政罰

12

■ （三）小結-3

1. 相較於國際立法例未要求須先命其改正才可處罰，我國則在個資法第47條至第50條針對行政罰規定中，分別有不同規範，針對第47條為同時命改正及罰鍰；第48條則須先命改正，未依命令改正者再為行政罰鍰；第49條則無命改正之規定。

2. 多數立法例有裁罰公務機關，我國則未針對公務機關有裁罰機制，在非公務機關部分，我國另針對非公務機關受罰鍰處罰時，其代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，應並受同一額度罰鍰之處罰。新加坡亦有處罰負責人之規定，但要件限縮於明知違反個資法之情形。

3. 歐盟體系、英國、新加坡、韓國罰鍰係依據受處分對象規模調整，以針對不同規模的對象達成懲罰效果，而我國罰鍰係採固定額度上限。

4. 綜觀各國行政罰，主要係針對違反資料運用之合法要件、控管者義務、當事人權利、目的外利用、國際傳輸、妨礙調查等情形規範，且針對特種個資之處理有較重的罰則，較具特色的規範模式，如美國僅有行政罰，菲律賓則無行政罰之規範。

國家發展委員會

三、行政罰

13

■ （四）討論議題

Q

1. 各國未要求須先命其改正才可處罰，我國個資法第48條則需先命改正後未改善，才得處罰(例如：非公務機關違反第27條第1項規定，未採行適當之安全措施，發生個資外洩)，是否需調整？
2. 未來我國設置個資保護獨立監督機制後，須否納入對公務機關之裁罰權限？若納入，考量公務機關類型多元(包含中央五院及所屬機關、地方自治機關、各級法院等)，是否須與非公務機關之裁罰有差異？或有其他可行方案？
3. 歐盟體系、英國、新加坡、韓國罰鍰係依據受處分對象規模調整，以針對不同規模的對象達成懲罰效果，而我國罰鍰目前係採固定額度上限之作法，若我國欲依據受處分對象規模調整，建議採何標準（如資本額、當地營業額、全球營業額之比例）？
4. 我國針對非公務機關之代表人、管理人或其他有代表權人，有受同一額度罰鍰之處罰，但多數國家未於個資法訂有相關規範，我國是否仍維持特殊規範或回歸行政罰法第15條規定適用即可？

國家發展委員會

大綱

14

一 討論範圍

二 行政罰

三 刑事罰

四 附件

國家發展委員會

三、刑事罰

15

■ （一）我國個人資料保護法之罰則

依個資法第41、42、44、45、46條規定，有關刑事罰之罰則。

個人資料保護法	
第41條	**意圖為自己或第三人不法之利益或損害他人之利益**，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處**五年以下有期徒刑，得併科新臺幣一百萬元以下罰金**。
第42條	**意圖為自己或第三人不法之利益或損害他人之利益**，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，**處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金**。
第44條	**公務員假借職務**上之權力、機會或方法，犯本章之罪者，**加重**其刑至二分之一。
第45條	本章之罪，須告訴乃論。但犯第四十一條之罪者，或對公務機關犯第四十二條之罪者，不在此限。
第46條	犯本章之罪，其他法律有較重處罰規定者，從其規定。

第41條修正說明：行為人非意圖為自己或第三人不法之利益或損害他人之利益，而違反本法相關規定者，因其可受非難性之程度較低，**原則以民事損害賠償、處以行政罰為已足**。惟行為人如有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定，因其可受非難性之程度較高，仍有以刑罰處罰之必要，爰為本條之修正。

我國刑事罰依其意圖限縮處罰範圍，限定於意圖為自己或第三人不法之利益或損害他人之利益之情形。

國家發展委員會

三、刑事罰

16

■（二）國際立法例比較-1

國別	有無刑事罰	財產刑額度	自由刑之額度	是否處罰過失	是否依據意圖限縮刑事	身分特別規定	是否針對法人處罰
我國	O	固定額度	5年以下	X	意圖為自己或第三人不法之利益或損害他人之利益	公務員加重（為無過失責任）	X
歐盟	各國自行訂定	–	–	–	–	–	–
英國	O	固定額度	–	O	X	X	O
德國	O	–	3年以下	O	X	X	O
美國	X	–	–	–	–	–	–
日本	O	固定額度	2年以下	O	意圖為自己或第三人不當利益，將業務所處理資料庫提供或盜用	公務員加重	O
韓國	O	固定額度	10年以下	O	針對十年刑責有主觀意圖要件	違反資通信業者專章規定	O
新加坡	O	固定額度	3年以下	O	X	X	O
菲律賓	O	固定額度	5年以下	O	出於惡意揭露所取得之個人資料	公務員加重	O

國家發展委員會

註：本表格僅以個資法為討論範圍

二、刑事罰

17

紫色：各國特有規定

重：處罰較嚴格之項目

■（二）國際立法例比較-2

國別	條號	對象	主觀要件	客觀要件	效果
我國	§41	自然人	意圖為自己或第三人不法之利益或損害他人之利益	違反特種及一般個資之蒐集處理利用之合法要件、目的外利用、限制國際傳輸之命令或處分，足生損害於他人者	有期徒刑得併科罰金
	§42			對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者	
	重 §44	公務員		公務員假借職務上之權力、機會或方法，犯本章之罪者	有期徒刑得併科罰金（加重二分之一）
英國	DPA §196	自然人	故意或重大過失	未經控管者同意獲取、揭露、保留個人資料，以及再進一步為買賣行為、對已去識別化之個人資料再識別	罰金（簡易定罪）
	DPA §198	法人*	故意或重大過失	未經控管者同意獲取、揭露、保留個人資料，以及再進一步為買賣行為對已去識別化之個人資料再識別	罰金（董事、經理、秘書、或類似人員可被起訴並受相應處罰）
德國	重 §42 I	任何人	明知無權而基於商業目的	將個人資料傳輸給第三方或以其他方式使其近用	有期徒刑或罰金
	§42 II	任何人	基於對價或意圖為自己或第三人不法利益或加損他人	未經授權，處理或經由提供不實訊息而獲得個人資料	

各國的刑事罰，主要針對明知、違反委員會命令、偽證情形規範，並對故意、有意圖營利、不當手段的有較重罰則。

國家發展委員會

*包含法人的董事、經理、秘書或類似人員，或聲稱以此身分行事者　註：歐盟、美國未規定刑事罰，故不列入表格

二、刑事罰
（二）國際立法例比較-3

18

紫色：各國特有規定

重：處罰較嚴格之項目

國別	條號	對象	主觀要件	客觀要件	效果
日本	§178	自然人	故意或過失	違反委員會命令	有期徒刑或罰金
	§179		意圖為自己或第三人不當利益	將業務所處理個人資訊資料庫提供或盜用	
	§182		故意或過失	拒絕或虛偽報告、提出資料、答辯，或妨礙、迴避檢查	罰金
重	§184	法人	故意或過失	違反委員會命令	罰金
			意圖為自己或第三人不當利益	將業務所處理個人資訊資料庫提供或盜用	
			故意或過失	拒絕或虛偽報告、提出資料、答辯，或妨礙、迴避檢查	
重	§176	公務員	故意或過失	無正當理由提供個人資料檔案	有期徒刑或罰金
	§177			委員會成員或事務局職員違反保密義務而洩露秘密或盜用	
	§180		意圖為自己或第三人之不當利益	將業務上知悉之保有個人資料提供或盜用	
	§181		意圖為供自己職務以外用途	濫用職權而蒐集屬於個人秘密事項之文書、圖畫或電磁紀錄	
韓國	§70	資料控制者或處理者	故意	致公務機關執行業務有中斷或嚴癈等重大障礙者	有期徒刑併科罰金
重			意圖為自己或第三人不當利益	以虛偽或其他不正手段或方法取得他人個資，並以不正方法向第三方提供	
	§71		故意或過失	違反當事人同意向第三方提供、違反處理機敏及假名資料、當事人權利、洩漏業務上知悉或未經授權個資等規定	
			意圖為自己或第三人不當利益	明知取自業務上洩漏之個資，卻仍意圖以營利或不正方法而接收該個資者	
	§72		故意或過失	違反設置操作影像資料處理器合法要件、不正方法取得處理個資同意	
			意圖為自己或第三人不當利益	明知係不正方法取得處理個資同意，仍意圖以營利或不正方法接收該個資者	
	§73		故意或過失	無安維措施致個資事故；未設置更正刪除措施並持續向外提供；未停止處理個資而持續利用或向第三方提供者	

二、刑事罰
（二）國際立法例比較-4

19

紫色：各國特有規定

重：處罰較嚴格之項目

國別	條號	對象	主觀要件	客觀要件	效果
新加坡	§51	組織或個人	故意或過失	未經同意行使當事人權利，資料可擅處置、更改、偽造、隱藏或銷毀，或教唆者 拒絕提供委員會資料或偽證	罰金或自由刑
菲律賓	§26	自然人	過失	違反近用一般個資、敏感個資規定	有期徒刑及罰金
	§25		故意或過失	違法運用一般個資、敏感個資	
重	§32			違法向第三方揭露一般個資、敏感個資	
	§33			有數個構成§25～32結合犯或接續犯之行為*	
	§27			不當處理一般個資、敏感個資	
	§28			違法目的外運用一般個資、敏感個資	
	§29		故意	違法揭害資料機密與安全資料制度	
	§30			明知安全漏洞而隱瞞事實	
	§31		惡意	揭露所保有一般個資、敏感個資有關之無根據或虛假資料	
	§34	法人	故意或過失	有§25－32違法行為	對負責人處有期徒刑及罰金；對法人為中止或撤銷權利

國家發展委員會

註：美國、歐盟未規定刑事罰，故不列入表格

三、刑事罰

■ （三）小結-1

1. 除美國CPRA無刑事罰，及歐盟GDPR未統一規範刑事罰，其他國家皆有刑事罰
   1) 歐盟GDPR將刑事罰的訂定權限給予各成員國，惟各成員國制定後應向歐盟報備。
   2) 美國CPRA並未規定刑事罰則；英國、德國、日本、韓國、新加坡、菲律賓皆有刑事罰相關規定，主要針對明知、違反委員會命令、偽證等情形有以刑事罰規範，並對故意、有意圖營利、不當手段的有較重罰則。
2. 多數國家之財產刑係固定額度上限
   1) 美國CPRA無刑事罰、歐盟GDPR無統一規範刑事罰。
   2) 英國、日本、韓國、新加坡、菲律賓皆針對財產刑採固定額度上限。
      ① 英國最高為5000英鎊以下罰金；
      ② 日本最高為100萬日幣以下罰金；
      ③ 韓國最高為1億韓圜以下罰金；
      ④ 新加坡最高為1萬新幣以下罰金；
      ⑤ 菲律賓最高為400萬比索以下罰金。
   3) 德國刑事罰依犯罪行為人之收入、財產及其他量處每日額罰金額之基礎，最高為360日整日額。（德國刑事法特殊計算方式）

三、刑事罰

■ （三）小結-2

3. 各國自由刑之額度多為1~3年，韓國最高至10年有期徒刑
   1) 美國CPRA無刑事罰、歐盟GDPR無統一規範刑事罰；英國刑事罰未包含自由刑。
   2) 德國、日本、韓國、新加坡、菲律賓有以自由刑作為刑事罰懲罰手段。
      ✓ 德國最高為3年以下有期徒刑；日本最高為2年以下有期徒刑；韓國最高為10年以下有期徒刑；新加坡最高為3年以下有期徒刑；菲律賓為1年以上、5年以下有期徒刑。
4. 有刑事罰則之國家，皆有處罰過失

   英國、德國、日本、韓國、新加坡、菲律賓皆有處罰過失。
5. 是否依據其意圖限縮刑事罰範圍

   多數國家未依據其意圖限縮刑事罰範圍，但韓國針對「以妨害個資處理業務為目的」及「以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供、教唆或幫助者」另有較重之刑事罰則。
6. 日本、韓國、菲律賓針對身分有特別規定
   1) 日本、菲律賓皆針對公務員身分有加重處罰之規定。
   2) 韓國則針對資通訊業者，設有資通信業者專章特別義務規定。
7. 僅有菲律賓於個資法規範違反個資法規範之數個犯罪行為樣態有結合或接續之狀態，加重刑事處罰。
8. 各國刑事罰客觀要件不同，除各國刑事體系差異外，有部分特別以刑事罰處罰的項目。

   日本有將違反委員會命令等行為納入刑事罰規範，新加坡亦有將未經同意行使當事人權利、更改、偽造、隱藏或銷毀，或教唆者拒絕提供委員會資料或偽證等納入刑事法規範。

三、刑事罰

■ （三）小結-3

1. 我國個資法第41、42、44、45、46條針對刑事罰之規定，皆處罰故意犯，未處罰過失犯。最高為五年以下有期徒刑，得併科新臺幣一百萬元以下罰金，另針對公務人員有加重規定。

2. 雖部分國家在行政罰會依據受處分對象規模調整，但在刑事罰之罰金部分，皆似我國罰金係採固定額度上限之作法。綜觀罰金金額大約為20萬臺幣至200萬臺幣區間，我國為100萬臺幣以下，罰金之金額居中。

3. 目前國際立法例僅韓國有特別針對意圖部分有加重刑責規定，多數國家未針對意圖限縮刑事罰範圍。我國原則以民事損害賠償、行政罰，將刑事罰限縮在行為人有意圖為自己或第三人不法之利益或損害他人之利益而違反本法相關規定之情形。

三、刑事罰

■ （四）討論議題

Q

1. 多數國際立法例未根據「意圖」限縮刑事罰範圍，且有處罰過失情形，處罰範圍較大，韓國特別針對意圖部分有加重刑責規定，我國目前僅針對「意圖為自己或第三人不法之利益或損害他人之利益」之情形懲罰，是否增加過失犯之刑事罰？是否增加其他犯罪行為樣態之刑事罰，如韓國「以妨害個資處理業務為目的」及「以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供、教唆或幫助者」？
2. 日本有針對違反主管機關命令、偽證等情形以刑事罰規範；新加坡亦有針對偽證情形有以刑事罰規範；未來我國設置個資保護獨立監督機制後，是否增加相關刑事罰則？
3. 因個資法規範之行為特性，可能涉及在同一個資法規範數個犯罪行為樣態有結合或接續之狀態，參考菲律賓針對此有結合犯或接續犯之規定，並加重刑事處罰，我國是否參考菲律賓模式增訂相關規範？

大綱

24

一 討論範圍

二 行政罰

三 刑事罰

四 附件

歐盟相關規定（1/2）

25

最近一次個資法修正：2016年（2018年施行）	
行政罰	
1.處罰資料控管者或受託處理者意圖或過失之行為 （第83(3)條）	
2.兩類：	• 最高1,000萬歐元或2%全球營業額，擇高者 （第83(4)條） • 最高2,000萬歐元或4%全球營業額，擇高者 （第83(5)、(6)條）
3.評估具體違法的事項、違法的嚴重程度、違法時間長短，考量資料傳輸之情形、資料傳輸之範圍、資料傳輸之目的、資料主體之數量、實際所受傷害；資料之種類； 違反規定之行為是意圖或過失（第83(2)(a)、(b)、(g)條）	
4.判斷有無GDPR第83條其他事項（第83(2)(c)-(f)、(h)-(k)條）：	• 減免行為 • 負責任之程度 • 違反GDPR之前科 • 與監管機關之配合度 • 監管機關是如何得知違反GDPR之事件 • 是否遵守監管機關糾正命令 • 行為守則及驗證之遵守程度 • 其他事項（不當得利、疫情）
5.行政罰則應有效、合比例性、具遏制力 （第83(1)條）	
* 處罰法人格，不處罰各別自然人，如企業負責人或其他監督管理責任者。但是當自然人之行為完全是私人行為或自然人完全為第三人所為時，即處罰各別自然人	

歐盟相關規定（2/2）

26

最近一次個資法修正：2016年（2018年施行）

刑事罰
刑事罰之權力交予歐盟成員國 （第84(1)條） • 針對GDPR行政罰鍰裁罰以外的事項，歐盟成員國可立法制定刑事罰
刑事罰則應有效、合比例性、具遏制力（第84(1)條）
告知歐盟執委會 （第84(2)條）

英國相關規定

27

最近一次個資法修正：2020年，但2021年公開徵詢修法建議（因應將GDPR改為 UK GDPR）
歐盟前成員國、GDPR適足性認定（2021）

	行政罰（UK GDPR §83 ）	刑事罰（DPA §§196-200）
對象	資料控管者、處理者、驗證機構、監管機構	董事、經理、秘書、個人，以及法人團體
事由	• 資料的控管者&處理者：違反第8、11、25至39、42及43條的義務 • 驗證機構：違反相關義務（ex未獲得認證） • 監管機構：對於資料控管者及處理者違反行為守則事件未採取適當行動。	• 因故意或重大過失未經控管者同意，獲取或揭露個人資料 • 在取得個人資料後，未經控管者同意而保留該資料 • 對上述資料，為資料買賣行為 • 在未得資料控管者同意的情況下，對於已去識別之個人資料進行再識別等
程序	• 附加或取代UK GDPR§58Ⅱ(a)~(h)&(j)所定措施 • 依DPA 155條發出處罰通知，載明受罰者的姓名、住址、處罰原因……等（參DPA附件16）	• 需要獲得專員或檢察署長同意 • 且在犯罪事實發生3年之後不能再追訴
處罰額度	依違反條文不同有不同處罰： • 870萬英鎊OR前一會計年度全球年營業額之2%（企業），並以較高者為準 ➢ 第8、11、25~39、41~43條 • 1750萬英鎊OR前一會計年度全球年營業額之4%（企業），並以較高者為準 ➢ 第5、6、7、9、12~22、44~49條 ➢ 違反主管機關第58Ⅱ之命令	• 個資相關犯罪均屬簡易定罪（summary conviction） • 依照英國2020年量刑法（Sentencing Act 2020）第122條，最高額不超過5000英鎊

德國相關規定

28

最近一次個資法（BDSG）修正：2021年6月23日
歐盟成員國

裁罰權BDSG § 41-§ 43 GDPR § 83(4)-(6)		
BDSG	刑事罰	➢ §42(1)將未公開之個人資料，明知無權基於商業之目的予以傳輸第三方或使其近用，將處以3年以下有期徒刑或罰金(最高360日整日額)。 (2)將未公開之個人資料，基於對價或滿足自己或他人之不法利益或侵害他人之意圖，處以2年以下有期徒刑或罰金。
	行政罰	➢ §43未能妥適地處理資訊的請求、未正確、未完全或未及時告知消費者，最高得處以5萬歐元之行政罰。
		➢ §41處理GDPR與本法處罰之競合規定 除本法另有規定外，應適用 GDPR§ 83(4)最高1,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之4%， (5)最高2,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之4%， (6)最高2,000萬歐元罰鍰or最高處以前一個會計年度全球年營業額之4%， ->以上皆以數額高為優先。

美國

29

無聯邦個資法，加州消費者隱私法（CCPA）最近修正為2018年，修正CCPA的新法CPRA將於2023年實施，效力溯及2022年1月1日；為協助統一各州法律規定，統一州法律委員全國會議（ULC）於2021年訂定統一個資保護法（UPDPA），目前已陸續有州提案。
CBPR成員國

	罰則規定				其他規定
CCPA CPRA	民/行/刑	民事	行政	刑事	1. 同一CCPA、CPRA違規行為：民事、行政不二罰 (§1798.199.90 (d); 100) 2. **州檢察長有權介入並接手案件**。州檢察長為了進行調查或民事訴訟，可向CPPA請求暫停行政行為或行政調查，CPPA應停止，直到州檢察長後續決定不進行調查或民事訴訟。 3. CPPA不得限制州檢察長執行本法之權力 (§1798.199.90)
	罰則內容	違反CCPA、CPRA • 可處最高2,500美元民事懲罰金，或於每項故意違規行為、每項涉及未成年消費者個人資料的違規行為處以最高7,500美元民事懲罰金 • 訴訟所得之懲罰金或和解所得，均應歸入**消費者隱私基金** (§1798.199.90)	經確認加州隱私保護機關確認存在違規行為，應命令 • 停止、中止違規行為 • 可處最高2,500美元行政罰鍰，或於每項故意違規行為、每項涉及未成年消費者個人資料的違規行為處以最高7,500美元**行政罰鍰** • 罰鍰均歸入**消費者隱私基金** (§1798.199.55) • 可受司法審查救濟 (§1798.199.85)	N/A	
	罰則權限	由**州檢察長** 以加州公民的名義於法院提起訴訟	由**加州隱私保護機關**處分		
		機關、法院在決定行政、民事金額時，可考量營利事業、服務提供者、承包商或其他人之善意合作 (§1798.199.100)			
UPDPA	UPDPA旨在提供靈活性、泛州適用，安排留給州檢察長依現有**州法**處理 • 違反UPDPA之執法機關、救濟、處罰依**該州消費者保護法**規定 • 州檢察長可依該州行政程序法實施本法、訂定規則 (UPDPA §16)				N/A

日本相關規定（1/2）

30

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

類型	處罰對象	規定
刑事罰	非公務機關	• 違反委員會命令者，處1年以下有期徒刑或100萬日幣以下罰金（§178） • 個人資料處理事業者（法人情形包括其董監事、代表人或管理人）或其從業人員或上開等人，意圖為自己或第三人之不當利益，而將其業務所處理之個人資訊資料庫提供或盜用，處1年以下之有期徒刑或50萬日幣以下罰金（§179） • 有下列情形之一得處50萬日幣以下罰金：（1）未提出依第146條第1項之報告或資料，或為虛偽報告、提出虛偽資料，或對職員質詢不為答辯，或為虛偽之答辯、拒絕、妨礙、迴避檢查者；（2）未依第153條為報告，或為虛偽報告者（§182） • 法人之罰金刑：違反第178、179條者，處1億日幣以下之罰金；違反第182條者，處同條之罰金刑（§184）
	公務機關	• 行政機關職員無正當理由而提供個人資料檔案，處2年以下有期徒刑或100萬日幣以下罰金（§176） • 委員會成員或事務局職員違反保密義務而洩漏秘密或盜用者，處2年以下有期徒刑或100萬日幣以下罰金（§177） • 行政機關職員意圖為自己或第三人之不當利益，將在業務上知悉之保有個人資料提供或為盜用者，處1年以下有期徒刑或50萬日幣以下罰金（§180） • 行政機關職員濫用職權，意圖為供其專門之職務使用以外之用途，而蒐集關於個人秘密事項之文書、圖畫或電磁記錄者，處1年以下有期徒刑或50萬日幣以下罰金（§181）

國家發展委員會

日本相關規定（2/2）

31

最近一次個資法修正：2021年，依《數位社會形成整備法》第50條修正個資法（令和3年改正個人情報保護法），分別於2022年4月及2023年施行。
CBPR成員國、GDPR適足性（2019）

類型	處罰對象	規定
行政罰	非公務機關	有下列情形之一得處10萬日幣以下罰鍰（§185）： （1）違反第30條第2項提供個資予第三方（包括準用第31條第3項提供個人關聯資料予第三方之情形）或有第56條冒用認定個人資料保護團體名稱者； （2）未依第51條第1項規定提出申報或為不實申報者； （3）以詐欺或其他之不當手段，基於第85條第3項規定因而受有以公開決定等為依據所公開之保有個人資料者。

國家發展委員會

韓國相關規定（1/2）

32

最近一次個資法修正：2020年（ 2021年9月28日提出「個人資料保護法修正草案」在國會審議中）
CBPR成員國、GDPR適足性（2021）

- 一、罰則規定於第10章（第70條至第76條）。保護委員會職權除原有的調查權，新增行政罰權限，一改過去僅有勸誘效果，提升其威嚇強制力。

- 二、 行政罰
  - 罰鍰（과징금）

違反義務	罰則
處理假名資料之規定（§28-6）	• 以識別特定個人為目的而處理資料時，處以銷售總額百分之三以下之行政罰鍰；若無銷售總額或計算顯有困難者，得依施行細則規定，以4億韓圜或資本額3%孰高者，處以行政罰鍰。
資通訊業者違反處理個人資料之規定（§39-15）	資通信業者若符合下列各款之事項，保護委員會得處以銷售總額百分之三以下之行政罰鍰： • 違反個資蒐集、個資特定目的內蒐集、向第三方提供個資； • 違法蒐集兒童個資； • 未有必要安全管理、監督、教育訓練等必要措施，致使受託者違反義務； • 未設置必要安全管理措施，致使資個資有遺失、竊取、洩漏、偽造、變造及毀損之虞； • 未取得使用者同意，蒐集個人資料； • 未取得使用者同意向國外提供其個資者。

  - 怠金（과태료）
    - 被裁罰之公務及非公務機關，怠於履行PIPA之義務而課與之金錢上處罰。PIPA於第75條依照違反作為義務之內容，而定有5千萬、3千萬、2千萬及1千萬以下韓圜裁罰。

韓國相關規定（2/2）

33

- 三、 刑事罰
  - PIPA針對刑事罰的規定除設有刑責及罰金的規定外，尚設有沒收或追徵的規定。
  - 除對該法人處罰外，尚得對該法人之代表人、代理人、使用人及其他從業員，課處罰金刑。
  - 另有團體訴訟機制，採取調解先行模式，受侵害之資料當事人得像個資保護委員會提出調解申請，若拒為調解或調解不成立，得由民間消費者保護團體 ，代表被侵權者提起團體訴訟。

違反義務	刑責與罰金	罰則
§70	10年以下有期徒刑，併科1億韓圜以下罰金。	• 以妨害個資處理業務為目的，而向公務機關變更或刪除處理中的個人資料，而致公務機關執行業務有中斷或難以等重大障礙者。 • 以虛偽或其他不正手段或方法取得他人處理中之個人資料，意圖營利並以不正方法向第三方提供，教唆或幫助者。
§71	5年以下有期徒刑，併科5千萬韓圜以下罰金。	• 未取得資料當事人同意，即將其個資向第三方提供者，以及明知該事由仍接收該個人資料； • 意圖以營利或不正方法而得到該個人資； • 違反PIPA規定處理敏感個資、固有識別資料、假名資料； • 資通訊業者未有更正、刪除而利用資料或向第三方提供，未取得使用者同意卻仍蒐集個人資料，未取得法定代理人同意，或未確認法定代理人是否曾經同意而蒐集14歲以下兒童之個人資料者 • 違反第59條第2款，洩漏業務上知悉之個人資料，未經授權即提供給他人利用、明知前揭事由卻仍以營利或不正方法取得個人資料及明知該事由，仍意圖以營利或不正方法而得到該個人資料，或有毀損、滅失、變更、偽造或洩漏他人之個人資料者。
§72	3年以下有期徒刑，併科3千萬韓圜以下罰金。	• 違法設置影像資料處理器，並以特定目的外操作影像處理器，或拍攝他處及使用錄音功能； • 以虛假、負面手段方法取得同意，意圖以營利或不正方法而得到該個人資料； • 違反第60條，洩漏因職務上明知或可得而知之機密，或將該資料利用於職務目的外。
§73	2年以下有期徒刑，併科2千萬韓圜以下罰金。	• 未設置安全維護必要措施致個人資料遺失、竊取、洩漏、偽造、變造及毀損； • 未依法銷毀個人資料之資通信業者； • 未設有更正、刪除等必要安全維護措施，而持續利用個人資料或向第三方提供； • 未停止處理個人資料而持續利用或向第三方提供者。

新加坡相關規定

34

最近一次個資法修正：2020年；CBPR成員國

	行政罰	刑事罰
對象	個人、組織	
事由	• 故意或過失違反PDPA第3、4、5、6、6A或6B章；或者任何組織或個人故意或過失違反第9章任何條文或第48B條第1項，PDPC應以書面通知要求該組織或個人支付罰款。	• 依第21條第1項提出請求，在未經另一人授權之情況下獲取有關另一人的個人資料 • 未經他人授權，根據第22條第1項提出更改有關該人的個人資料的請求 • 在符合第51條第1A項之規定下，根據第26H條第1項向轉移組織提出資料轉移請求，以在未經另一個人授權的情況下將有關另一個人的個人資料傳送給接收組織。
處罰額度	不得超過規定的最高金額100萬新幣；而對個人所處以的罰款不得超過規定的最高數額20萬新幣。可針對違反本法不同規定的行為規定不同的最高金額。	• 違反第51條第3項a款可處以5,000新幣之罰款，或12個月以下之監禁 • 違第51條第3項b款或第3項c款10,000新幣之罰款或12個月以下的監禁 • 違反第51條第3項ba款或bb款，可處以5,000新幣以下罰款或6個月以下監禁 • 犯有本法規定的罪行且未明確規定處罰的人，一經定罪，將被處以10,000新幣罰款或3年以下監禁，或兩者兼施，如繼續罪行，定罪後繼續犯罪的每日處1,000新幣以下罰款。

註：2020年修法後預計於2022年實行大幅加重罰款額度，處以最高為該組織在新加坡年營業額的10%或100萬新幣罰款，取金額高者計算。

國家發展委員會

菲律賓相關規定

35

最近一次個資法修正：2012年（2017年、2019年分別提出修正案，尚未完成立法程序）

- 針對違反行為態樣、資料類型處以不同額度、身分效果之刑罰：

1. **未經授權運用個人資料及敏感性個人資料之行為**→一般個資處1~3年有期徒刑及50~200萬比索罰金／敏感個資處3~6年有期徒刑及50~400萬比索罰金
2. **過失近用個人資料及敏感性個人資料之行為**→一般個資處1~3年有期徒刑及50~200萬比索罰金／敏感個資處3~6年有期徒刑及50~400萬比索罰金
3. **不當處理個人資料及敏感性個人資料之行為**→一般個資處6個月~2年有期徒刑及10~50萬比索罰金／敏感個資處1~3年有期徒刑及10~100萬比索罰金
4. **未經授權目的運用個人資料及敏感性個人資料之行為**→一般個資處1年6個月~5年有期徒刑及50~100萬比索罰金／敏感個資處2~7年有期徒刑及50~200萬比索罰金
5. **未經授權近用或故意違反之行為**→處1~3年有期徒刑及50~200萬比索罰金
6. **隱瞞涉及敏感性個人資料的安全漏洞之行為**→處1年6個月~5年有期徒刑及50~100萬比索罰金
7. **惡意揭露之行為**→處1年6個月~5年有期徒刑及50~100萬比索罰金
8. **未經授權揭露之行為**→一般個資處1~3年有期徒刑及50~100萬比索罰金／敏感個資處3~5年有期徒刑及50~200萬比索罰金

- 針對上述行為有**結合犯或接續犯**，將處3~6年有期徒刑及100~500萬罰金
- 行為人為**公司、合夥或任何法人**，應根據具體情形對參與犯罪或因重大過失允許犯罪的負責人處以刑罰；若行為人為法人，法院得根據本法暫停或撤銷其享有本法之權利
- 當涉及**超過100人以上個資違法之行為**，構成大規範犯罪，將處以對應行為之最高刑
- 針對**公務人員**應適用從刑規定，包括褫奪公權

國家發展委員會

「個人資料保護法相關議題研析」委外服務案/顧振豪研究
主持. -- 初版. –
臺北市 : 國發會, 民 111.10
面: 表，公分
編號: (111)014.0905
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會
資料保護法
584.111

「個人資料保護法相關議題研析」委外服務案
委託單位：國家發展委員會
受託單位：財團法人資訊工業策進會
研究主持人：顧振豪
出版機關：國家發展委員會
電話：02-23165300
地址：臺北市寶慶路 3 號
網址：http://www.ndc.gov.tw/
出版年月：中華民國 111 年 10 月
版次：初版
刷次：第 1 刷
編號：(111)014.0905　(平裝)