標案案號 W1050224

# 法務部
# 「歐盟及日本個人資料保護立法最新發展之分析報告」委託研究案
# 成果報告

受託單位：東海大學

研究主持人：范姜真媺教授

協同主持人：劉定基副教授

協同主持人：李寧修副教授

中 華 民 國 一 ○ 五 年 十 二 月 三 十 日

# 摘　要

我國於 1995 年 7 月完成立法施行之「電腦處理個人資料保護法」及之後 2010 年 5 月修正通過之「個人資料保護法」，其中若干條文均係參考歐盟 1995 年之資料保護指令(95/46/EC)。

然因 90 年代後期資訊科技發展一日千里，電腦網路日益普及，加上各種電子終端裝置及感應設施大量設置、使用，得隨處大量、快速蒐集個人購物、上網履歷、行動位置等各種資料，儲存於各處電腦上或雲端中，並透過網路輕易將各資料庫作連結，形成個資共有化及巨量化(big-data)。如此個資之蒐集、利用，常係在當事人未查知下利用於其未預知之目的上。從而個人對自己資料存於網路上之何處？由何人？如何被利用難以掌握，資料自主權面臨新的挑戰難以貫徹。故如何確保個資被安全、合法蒐集、處理及利用，發揮其有用性以提升行政效率、創新產業，成為各國及國際間共同、重要之課題。因此歐盟及日本近年均開始著手修正有關個資保護規範。

歐盟之理事會已於 2015 年 6 月協議達成修正規則案之一般方向(general approach) ，在同年 12 月 15 日完成與歐洲議會之交涉，公布一般資料保護規則(General Data Protection Regulation)，並預計在 2016 年由歐洲議會及理事會通過，兩年後生效適用。另外日本內閣在歷經兩年之研究、檢討後，於 2015 年 3 月向國會提出「有關個人情報保護法及行政程序中為識別特定個人之編號利用等法部分修正案」，後於同年 9 月 3 日經國會審議通過，完成修法。

在國際電子商務蓬勃發展，資訊產業全球化浪潮中，我國自不能置身事外，有必要再檢視現行個資法制是否同有不足之處。另事實上，近年判例實務上已有現行個資法適用上出現爭議之案例出現，彰顯出我現行個資法解釋適用上之問題及規範不足之處。

為讓我國個資法能修補規範不足之處，符合資訊社會高度發展之所需，本研究計畫將詳細研究歐盟最新個資保護規則與日本新修正之個人情報保護法，深入分析其有關個人資料之定義與保護範圍、合法蒐集、處理及利用個資之要件、個資當事人之權利、跨國傳遞個資之規範、個資之安全維護及個資法施行之監督機制等議題；並比較法制上特色及優缺點，從中探討出我國將來修法可以擷取參考之部分。

關鍵字：個人資料保護；日本情報公開保護法；歐盟個人資料保護指令；歐盟一般性個人資料保護規則

# Abstract

The 1995 EU Data Protection Directive (95/46/EC) has influenced both Taiwan's Computer-processed Personal Data Protection Act of 1995 and Personal Data Protection Act of 2010.

However, since the late 1990s, information technology has developed rapidly. The Internet becomes more pervasive. Different electronic devices and sensors collect and store a massive amount of personal data (e.g., shopping habits, browsing histories, locational data) in computerized databases or even in the clouds. With the help of the Internet, these databases are easily linked together. The concept of "big data" has emerged. At the same time, individuals have gradually lost control over their personal information. The collection and use of personal data are without the knowledge of individuals. The longstanding principle of "information self-determination" has faced great challenges and often times cannot be fully realized. As a result, it becomes an important issue to ensure that personal data is lawfully collected, processed, and used, while at the same time to allow reasonable and proper use of such data in order to enhance administrative efficiency and promote business innovation. Under these circumstances, in recent years, both the European Union and Japan have tried to reform their personal data protection laws.

In June 2015, the European Council has reached a general approach regarding the reform of the EU Data Protection Directive, and based on the consensus with the European Parliament, a draft General Data Protection Regulation was released on December 15, 2015. The new law is scheduled to complete the legislative process in 2016 and become effective in two years. Meanwhile, after two years of research, the Japanese Cabinet had proposed a bill to amend Japan's Personal Data Protection Act and the Act on Use of Numbers to Identify Specific Individuals in Administrative Procedures in March 2015. The bill was enacted into law by the Japanese Congress on September 3, 2015.

With the booming development of e-commerce and globalization of ICT, Taiwan must also carefully review the existing Personal Data Protection Act. In fact, some recent court judgments have already indicated the problems of the current law.

This research project aims to study the newly enacted EU General Data Protection Regulation and the Japanese Personal Data Protection Act. The project will analyze important issues, such as the definition of personal data, legal grounds to process personal data, data subjects' rights, international data transfer, data security, and the supervisory mechanism. By comparing the advantages and disadvantages among the data protection laws in EU, japan and Taiwan, this research hopes to provide some guidance on how to amend Taiwan's Personal Data Protection Act in the future.

Keywords: Personal Data Protection, The Act on the Protection of Personal Information, EU Personal Data Protection Directive, EU General Data Protection Regulation

# 目錄

# 第一章　研究背景及研究方法

## 第一節　研究背景

我國於 1995 年 7 月完成立法施行之「電腦處理個人資料保護法」，及之後 2010 年 5 月修正通過之「個人資料保護法」，其中若干條文均係參考歐盟 1995 年之資料保護指令(95/46/EC)[1]。

查上開歐盟指令訂立時，係尚未有搜尋引擎(search engineer)、社群網站( social networking service)、智慧型手機(Smart phone)問世使用，亦未發展出雲端運算、GPS 定位技術之背景下，所定立之個資保護規範；而於 90 年代後期資訊科技發展一日千里，電腦網路日益普及，加上各種電子終端裝置及感應設施大量設置、使用，得隨處大量、快速蒐集個人購物、上網履歷、行動位置等各種資料，儲存於各處電腦上或雲端中，而透過網路輕易將各資料庫作連結，形成個資共有化及巨量化(big-data)；如再依自動化處理系統加以比對或進行分析，即得以預測商品流行趨勢、顧客消費傾向，用於開發新產品、提升產業競爭力；亦得用於流行疾病之預測或交通流量之管制。然如此之個資蒐集、利用，常係在當事人未查知下利用於其未預知之目的上。另一方面，因數位化資料留存於電腦網路，具無時間、空間限制之特性，常使與當事人現況已不符、或與蒐集特定目的無關連、過剩之資料，仍存於網路上，隨時得供人利用，造成當事人現在生活或形象遭受破壞，個人對自己資料存於網路上之何處？由何人？如何被利用難以掌握，資料自主權面臨新的挑戰難以貫徹。而國際上有關個資保護之規約，包括 OECD 八大原則[2]及前述之歐盟指令等，顯然已不足應對現今新形態之個資蒐集、處理或利用，資料當事人權利處於被侵害之高風險下。故如何確保個資被安全、合法蒐集、處理及利用，發揮其有用性以提升行政效率、創新產業，成為各國及國際間

[1] Directive 95/46/EC of 24 October 1995on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[2] OECD Guidelines on the Protection. of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/sti/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

共同、重要之課題。因此歐盟、OECD、歐洲評議會(Council of Europe,CoE)[3]及日本近年均開始著手修正有關個資保護規範，並有志一同集中於 2012 年左右公佈草案，而有日本學者稱該年為「隱私權年(プライバシー・イヤー2012)」[4]。且歐盟之理事會已於 2015 年 6 月協議達成修正規則案之一般方向(general approach) ，在同年 12 月 15 日完成與歐洲議會之交涉，公布一般資料保護規則(General Data Protection Regulation)（以下簡稱歐盟個資規則），並預計在 2016 年由歐洲議會及理事會通過，兩年後生效適用。另外日本內閣在歷經兩年之研究、檢討後，於 2015 年 3 月向國會提出「有關個人情報保護法及行政程序中為識別特定個人之編號利用等法部分修正案」[5]，後於同年 9 月 3 日經國會審議通過，完成修法。

如上之發展趨勢下，我國現行個資法雖修正後施行未久，原為立法重要參考之歐盟指令，已然為因應社會之需而進行修正，則在國際電子商務蓬勃發展，資訊產業全球化浪潮中，我國自不能置身事外，有必要再檢視現行個資法制是否同有不足之處。事實上，近年判例實務上已有現行個資法適用上出現爭議之案例出現，如電話號碼及電信服務提供業者別，是否具有特定個人識別性而應保護之個資[6]。衛福部健保署蒐集被保險人就診資料，建置資料庫後供研究機構利用，而被當事人起訴要求停止提供[7]，以及原告要求 Google 搜尋引擎刪除網頁上有關自

[3]歐洲評議會(Council of Europe)於 1981 年 1 月 28 日簽署、1985 年 10 月 1 日生效之「個人資料自動化處理之個人保護條約( Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data)」第 108 号(Convention 108)，至 2014 年 2 月已有包含 EU 加盟國在內之 46 國批准。自 2011 後歐洲評議會亦進行條約第 108 号現代化(modernization)修正檢討，而於 2012 年 11 月第 29 屆總會通過現代化提案，參見 Coe, The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data；Propositions of Modernisation,27-30,Novermber 2012(29 th Plenary meeting)。之後評議會之閣僚會議(Committee of Ministers)於 2013 年 7 月 10 日設置資料保護特別委員會(Ad hoc Committee on Data Protection，CAHDATA) 進行提案檢討，至 2014 年 3 月 25 日公布作業文書。http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Terms%20of%20reference%20-%20Ad%20hoc%20committee%20on%20data%20protection%202013.pdf（最後瀏覽日:2016 年 12 月 26 日）。

[4]宮下紘、プレイバシーイヤー2012、NEXT COM,vol.2012 winter，頁 32

[5] 個人情報の保護に関する法律及び行政手續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の一部を改正する法律。

[6] 台北地方法院，103 年度北小字第 1360 號判決。

[7] 台北高等行政法院，102 年度訴字第 36 號判決；最高行政法院 103 年判字第 600 號判決。

己過去涉及打假球新聞報導資料之記載之訴訟[8]等。上述案件涉及個資範圍之認定、資料庫匿名資料之提供利用、當事人被遺忘權利之主張及對 Google 搜尋引擎我國有無司法管轄權之重要爭議問題，亦彰顯出我現行個資法解釋適用上之問題及規範不足之處。

為讓我國個資法能修補規範不足之處，符合資訊社會高度發展之所需，實有必要詳細研究歐盟最新個資保護規則與日本新修正之個人情報保護法，深入分析其有關個人資料之定義與保護範圍、合法蒐集、處理及利用個資之要件、個資當事人之權利、跨國傳遞個資之規範、個資之安全維護及個資法施行之監督機制等議題；並比較法制上特色及優缺點，從中探討出我國將來修法可以擷取參考之部分。

## 第二節　研究方法

### 一、文獻(判決)回顧及歸納

本研究首先將回顧國內外有關「歐盟 1995 年個人資料保護指令」、「歐盟個資規則」及日本「有關個人情報保護法及行政程序中為識別特定個人之編號利用等法部分修正」之政府出版品、法院判決、專家學者論著、網路資訊等文獻，以充分了解上述規定之內涵及其適用上所可能產生的爭議。

### 二、政策評估

在對歐盟及日本最新之個人資料保護規範有深入之瞭解後，本研究將比較兩國法制的差異、分析其優缺點，並將其與我國之個人資料保護法加以對照研析，藉以評估現行個資法之缺漏與不足之處，最後並依據歐盟與日本之新規範，研提符合我國國情之修法建議或實務上可採行之解釋方案。

[8] 台灣高等法院，104 年抗字第 491 號裁定。

## 第二章　歐盟個人資料保護法制介紹與分析

### 第一節　法制沿革

歐盟於 1995 年頒布個人資料保護指令(95/46/EC)，對於歐洲各國乃至全世界個人資料保護法制之發展，均有極重要影響。但 1995 年以來，資通訊技術發展變化迅速，網際網路與各項應用興起、近年來又有「巨量資料」與「物聯網（internet of things）」概念之提出，既有歐盟個人資料保護指令面對這些變化已經難以為繼；另一方面，1995 年個人資料保護指令在規範形式上僅係「指令（directive）」，必須透過各國立法轉化，因而產生各國個人資料保護規範不一致之情形，除增加資料管理者遵法成本外，更影響歐盟資料跨境流通之目標，歐盟因此欲藉由具有直接規範效力之「規則（regulation）」之訂定，[1]進一步統合各會員國間之個人資料保護標準，故自 2010 年 11 月初即將修正內容對外公開，凝聚各方共識。

觀察歐盟本次之修法工程，一開始即極具野心，不但在修正幅度上全盤檢討既有規範內容，在修法時程上也希望儘量壓縮，原先歐盟執委會於 2012 年初提出草案後，[2]希望能於 2014 年完成立法，2016 年正式施行。然而因為草案內容爭議頗大，各方意見紛歧，直至 2013 年底，歐洲議會公民自由、司法與內政委員會（European Parliament Committee on Civil Liberties, Justice and Home Affairs）方才通過對於執委會版草案之修正意見；[3]其後，歐盟執委會、議會與理事會（European Council）持續進行三方協商討論，於 2015 年末終於獲致共識，提出歐盟個資規則之三方協議版草案，[4]並於 2016 年 4 月 27 日通過，同年 5 月 4 日正式公布。依據歐盟個資保護規則第 99 條第 1 項，其將於公布後 20 天生效（即

---

[1] *See* Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies*, 28 Santa Clara Computer & High Tech. L. J. 815, 823-26 (2012).

[2] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (last visited: Dec. 26, 2016).

[3] http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf. (last visited: Dec. 26, 2016).

[4] https://www.huntonregulationtracker.com/files/Uploads/Documents/EU%20Data%20Protection%20Reg%20Tracker/GDPR-consolidated-text-outcome-of-trilogue-15.12.2015.pdf (last visited: Dec. 26, 2016).

2016 年 5 月 25 日），但考量為達到歐盟個資保護規則所要求之保護水準，不論是公務機關或是非公務機關，都需要時間因應此一轉變，故於同條第 2 項中，將其生效日期再延後 2 年，故其於 2018 年 5 月 25 日方生效，屆時亦將正式取代 1995 年個人資料保護指令。[5]另外，值得一提者，隨著歐盟個資規則同時通過及公布的，還有「刑事司法個資保護指令（Datenschutzrichtlinie für Strafjustiz）」，其主要在於規範各有權機關基於預防、偵查、揭露或追訴犯罪行為之目的，或為執行刑罰之目的，處理個人資料之行為。

2016 年歐盟個資規則之通過，具有里程碑之意義，對於當代個人資料保護藍圖之描繪，亦有引領的功能，因選擇「規則」之形式，故其得普遍、直接拘束各會員國，且其所規範之內容毋須經立法轉換，即得適用於各會員國之內國法體系；[6]但被稱為個資保護基本規則（Datenschutz-Grundverordnung）之歐盟個資規則，事實上卻無法、亦不願將歐盟內所有關於個資處理之事項皆完整地納入其規範範疇，而僅是以提供一個資保護最低、基本的個人資料保護框架，並取得歐盟境內個人資料保護水準一致性為目標，也因此在其條文中，得見大量不確定法律概念及概括條款之運用，並將具體化之任務，進一步委託各會員國之立法者。因此，對於歐盟個資規則所發揮之具體影響，建議應得持續關注歐盟各會員國個人資料保護法制之發展，另再為相應之研究分析。

## 第二節　法制修正之背景與課題

相較於 1995 年個人資料保護指令，歐盟個資規則呈現了以下值得關注的發展：

1. 擴張規則之適用範圍，強化執法措施

任何以歐盟會員國消費者為對象之服務(services that target EU customers)，即便提供服務之公司或相關設備位於歐盟領域外，均將納入指令之適用範圍；此外，

[5] 歐盟個資規則第 94 條第 1 項。

[6] 歐洲聯盟運作條約（Treaty on the Functioning of the European Union, TFEU）第 288 條第 2 項參照。

歐盟也正嚴肅考慮對境外資料管理者(data controllers)提起相關法律程序、甚至就設於境外之伺服器進行必要檢查之可能性。

2. 強化個人資料當事人之權利

在當事人權利之強化方面，主要以請求移除之權利（或稱「被遺忘權」）與「資料可攜權（data portability）」為代表。前者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紀錄，並永久保存、無法抹滅之具體機制，亦即賦予資料當事人得以在資料管理者無正當理由保存相關資料之情形下，請求移除/刪除(delete)使個人感到不堪、困窘或其他不欲再為人知之資訊，並被社會所遺忘之權利。後者則是賦予當事人要求資料管理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資料管理者間移動(例如：從某一社群網站搬遷到另一社群網站)。

3. 強化資料當事人之同意

就此部分而言，主要著重於兩方面。首先是同意定義之釐清，包括增加：「明確（explicit）」的要件，此外也要求同意之方式必須為「聲明（statement）」或「清楚的積極行為(clear affirmative action)」。其次則是新增「同意條件（Conditions for Consent）」，包括當事人是否同意，應由資料管理者負舉證責任；同意以書面為之時，須與其他事項清楚分離；明定當事人有權隨時撤回其同意，且撤回同意應與給予同意一樣容易；同意僅得針對特定目的為之，且有關契約的履行或服務的提供，不得以當事人同意使用與履行契約或提供服務無關的個人資料為條件。

4. 告知規定之再強化

針對目前廣受批評之告知徒具形式，當事人甚少閱讀之問題，草案也試圖加以回應，一方面要求以圖形化之方式，方便當事人迅速閱讀吸收基本重要資訊；另一方面則進一步擴大應告知事項的範圍，除既有的資料管理者名稱、蒐集資料目的、個人資料的收受者(recipient)或其類別、當事人相關權利外，更新增 8 項告知內容，包括：有關資料安全維護的資訊、資料儲存期間或儲存期間的決定標

準、當事人有權向監督機關提起申訴及監督機關的聯絡資料、資料管理者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定、是否進行資料剖析（profiling）與資料剖析的方式及對當事人可能的影響、關於自動化處理個人資料的運作邏輯、過去12個月內是否曾將個人資料提供予公務機關，以及其他為維護資料公平使用所必要的資訊。

5. 蒐集、處理與利用要件之調整

除了釐清部分既有之蒐集、處理與利用要件內涵外，本次修正最重要，但也最具爭議之內容之一即是是否因應巨量資料時代之資料（再）利用需求，放寬資料之利用要件，此部分雖在歐盟個資規則中有所著墨，例如強調技術上或組織上強化當事人權利保護之措施，但卻也留下大幅空間，讓各會員國之立法者再行具體化。

6. 資料管理者與利用者義務之增加

歐盟個資規則除將統一個人資料外洩之通報義務外，對於具有一定規模之資料管理者，將強制要求設置資料保護人員(data protection officer)；更有甚者，將強制資料管理者在處理特定種類之個人資料前，必須進行「隱私影響評估(privacy impact assessment)」，以更妥善保護資料當事人之隱私。

## 第三節　歐盟個資規則之架構與主要內容

### 第一項　規範對象與適用地域範圍

#### 第一款　規範對象

關於歐盟個資規則的規範對象，可以分「規範客體」以及「適用主體」兩方面加以說明。首先在規範客體上，歐盟個資規則延續指令的規定，將規範範圍限定於**「全部或部分以自動化方式蒐集、處理或利用的個人資料」**，至於以「非」自動化方式蒐集、處理或利用的情形，為避免打擊範圍過大，也僅限於**「構成檔案系統（filing system）一部分，或『為』構成檔案系統一部分而蒐集、處理或利用的個人資料」**才有適用（個資規則第 2 條第 1 項參照）。

應說明者，所謂檔案系統的定義，歐盟個資規則仍延續指令「個人資料檔案系統」的規定，指：**「可以特定條件存取的結構化個人資料集合，不論是集中、分散或以其他功能或地理因素散佈者」**（個資規則第 4 條第 6 款）。準此，一般零散的紙本資料集合，如不能以一定方式檢索，仍然沒有規則的適用。

至於在**「適用主體」**方面，如同指令既有的規定，歐盟個資規則對於資料管理者（data controller，亦有譯為資料控制者）及受託者（processor）的定義，均包括**「自然人、法人，公務機關，機構或其他組織（natural or legal person, public authority, agency or other body）」**[7]，並「不以」特定組織型態作為認定適用主體的標準。

此一普遍適用主體的規範模式，在現今任何人、團體均有能力透過電子科技與網際網路，大量蒐集、儲存或利用個人資料造成資訊隱私侵害的時代，實有重要意義，也可以避免個人資料保護的漏洞。

當然，將一般自然人納入個人資料保護法制的適用範圍內，要求其遵守與一般公司行號、法人或團體相同的規範標準，不但可能與社會常情有違，實際執行上也可能因一般人欠缺必要的專業知識與資源，而面臨相當的困難。因此，在指令時代即訂有**「自然人純供個人或家庭活動」**目的的排除規定[8]，減緩普遍適用主體後的衝擊。

值得注意者，網際網路的發展，尤其是各種網路交易平台、影音、社群媒體的普及，使得「自然人純供個人或家庭活動」目的的判斷日益困難[9]。例如：自然人將他人的個人資料、照片或影像放置在前述社群媒體或影音網站上，依其隱私設定的不同，最廣可以供全世界不特定人瀏覽、轉傳與留存，此一行為對於個人資訊隱私可能造成的影響恐遠超過其他受到規制機關、團體的行為。此與原來

[7] GDPR Article 4 (7) & (8).
[8] Directive Article 3.2.
[9] 劉定基，個人資料的定義、保護原則與個人資料保護法適用的例外－以監視錄影為例（上），月旦法學教室第 115 期，2012 年 5 月，頁 53-54。

將個人或家庭使用活動排除的初衷是否相符，即生疑義。

準此，在本次歐盟個資規則修正過程中，「自然人純供個人或家庭活動」的排除規定，就成為檢討的重點。在歐盟執委會最初的草案中，即增加**「未獲得任何利益（without any gainful interest）」**的要件，試圖限縮此一排除規定的範圍。然而，在歐洲議會討論過程中，「公民自由、司法與內政委員會（Committee on Civil Liberty, Justice, and Home Affairs, LIBE Committee）」的報告即質疑「自然人純供個人或家庭活動」目的，有時可能包含獲得利益的行為，例如：向其他人出售私人物品，於此情形，只要與個人職業或商業活動無關，仍然「不應」納入規制的範圍[10]，因此建議刪除「未獲任何利益的文字」。此外，上述 LIBE Committee 報告也指出，自然人為個人或家庭活動處理、利用個人資料，而使該資料可能得以被特定人或不特定人存取，也應該是判斷是否應受到管制的因素之一[11]。

受到此一報告的影響，歐洲議會一讀通過的草案條文即刪除未獲得任何利益的要件。又，針對自然人因個人或家庭活動目的而「公開（publication）」個人資料的情形，歐洲議會一讀通過的草案條文新增僅在**「可合理預期僅得由數量有限之人存取」**的情形下，方得適用排除規定的文字[12]。考察此一新增規定的立法目的，似乎寓有促使個人注意維護自身與他人隱私，積極利用（社群）網站隱私設定功能之意。然而，上述草案文字在進入執委會、議會與理事會三方協商時又有轉折，最後通過的版本則回到原先指令的文字，沒有新增任何要件。

惟應注意者，依據立法說明，所謂「個人或家庭活動」仍不得與職業或商業活動有關（with no connection to a professional or commercial activity），其範圍包括通訊、地址資料，或在個人或家庭目的內的社群及線上活動[13]。從歐盟個資規則最後定案的文字刪除「可合理預期僅得由數量有限之人存取」的要件，似乎顯

[10] LIBE Committee, Draft Report 11 & 61 (2013).
[11] *Id*. at 11.
[12] 相關規定文字的原文為: This exemption also shall apply to a publication of personal data where it can be reasonably expected that it will be only accessed by a limited number of persons.
[13] GDPR Recital (18).

示歐盟欲賦予個人在社群網站與線上活動時較高的彈性，同時避免規則對個人或家庭活動過度的干預。

### 第二款　適用地域範圍

相較於現行指令以資料管理者在「歐洲經濟區(European Economic Area, EEA)」內有住居所或機構，或利用 EEA 境內的「設備(equipment)」蒐集、處理或利用個人資料，才有各國個人資料保護法適用的規定[14]，歐盟個資規則適用的地域範圍則明顯擴大，甚至將純粹在歐盟領域外的資料管理者，也納入適用的範圍。依據歐盟個資規則第 3 條的規定：

> **本規則適用於設立於歐盟境內之資料管理者或受託者所為之個人資料處理活動；不論該資料處理活動是否發生於歐盟境內。**
>
> **本規則適用於非設立於歐盟境內之資料管理者或受託者，對於歐盟境內之資料當事人為以下行為而蒐集、處理或利用個人資料之情形：**
>
> **(a) 提供商品或服務；無論資料當事人是否需付款**
>
> **(b) 在歐盟境內的行為（behaviour）進行監控（monitor）**
>
> **...（第三項：略）**

應說明者，第 3 條第 1 項所謂「設立於」歐盟境內的資料管理者或受託者，係指透過穩定的安排，而存在有效且確實的活動，即為已足；至於在法律形式上，究竟是透過分公司或有法人格的子公司，並非決定性的因素[15]。

所謂提供商品或服務，並非僅是客觀上的判斷，而須考量資料管理者的主觀要素，亦即資料管理者或受託者須「認知（envisage）」其商品或服務是提供給位

[14] 關於現行指令規定的說明，參見劉定基，雲端運算與個人資料保護－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究，第 43 期，2014 年 8 月，頁 11-14。
[15] GDPR Recital (22).

於歐盟境內的資料當事人。因此，若僅僅是在歐盟境內可以連結到資料管理者、受託者或其他中介者的網站、電子郵件地址或其他聯繫方式，或資料管理者使用其所在的第三地一般使用的語言進行商品或服務的交易，均不足以認定資料管理者符合規則要求的主觀認知要素。相對地，如果使用歐盟會員國使用的語言、貨幣進行交易，或提及歐盟境內的消費者或使用者，即可能被認為資料管理者認知其提供商品或服務予歐盟境內的資料當事人[16]。又，值得注意者，由於歐盟個資規則明文規定不論資料當事人是否支付費用，因此即便是提供「免費」的商品或服務，仍然受到規範。

最後，究竟何種個人資料的蒐集、處理或利用行為構成「監控」，依據歐盟個資規則立法理由的說明，係指資料當事人在線上遭到追蹤（track），包括後續可能使用個人資料處理、利用技術對自然人進行剖析（profiling）以對其做成決定，或分析、預測其個人喜好、行為或態度[17]。

### 第二項　保護之客體－個人資料之定義

#### 第一款　配合科技發展而稍加修正的個人資料定義

在歐盟個資規則中，個人資料的定義基本上與指令時代相同，均指「**任何有關一個已識別（identified）或足資識別（identifiable）自然人的資料**」。相較於指令舊有的規定，歐盟個資規則僅在定義「足資識別」的資料時，配合網路與（通訊）科技的發展，有稍微詳細的說明。依據歐盟個資規則第 4 條的定義，所謂「足資識別的自然人」係指：「**一個可以透過『識別符號（identifier）』，例如：姓名、識別號碼、位置資料（location data）、線上識別碼（online identifier），或經由其他一項或多項身體、生理、基因、精神、經濟、文化或社會身分特徵，直接或間接識別的自然人**」。上述個人資料的定義，在規則歷次草案中並沒有重大改變[18]，

[16] GDPR Recital (23).
[17] GDPR Recital (24).
[18] 唯一的差異是，在執委會提出的草案中，「足資識別」的定義是放在「資料當事人（data subject）」的定義規定內而已。

可見歐盟執委會、議會與理事會對之具有高度共識。

關於上述條文中所稱的「位置資料」，規則並未加以定義[19]。而所謂「線上識別碼」，參考歐盟個資規則的立法說明，應指由裝置、應用程式、工具或網路協定所賦予的（獨特）識別碼，例如：網路協定位置（internet protocol addresses），小型文字檔案識別碼（cookies identifier）或其他識別碼（例如：無線射頻識別標籤，radio frequency identification tags）[20]。應說明者，歐盟個資規則直接將位置資料與線上識別碼例示為「可能」足資識別的個人資料，與指令第 29 條工作小組長期以來認為位置資料、網路協定位置、小型文字檔案識別碼在多數情形屬於個人資料的見解相同[21]，此次將其納入法條中，應有助於避免可能發生的爭議。

其實，何謂「足資識別」的資料，或究竟是否構成「間接識別」，一直都是個人資料定義的難題。在指令時代，立法理由即曾表示應考量：「資料管理者或任何第三人為識別特定人，所有合理可能使用的方式（all the means likely reasonably to be used either by the controller or by any other person to identify the said person）」[22]。

然而，對於「所有合理可能使用的方式」應如何判斷的關鍵問題，指令卻沒有進一步說明。在本次歐盟個資規則制定前，指令第 29 條工作小組曾於 2007 年的意見中，建議必須綜合考量以下因素：查詢所需花費的成本、該資料的使用目的、該資料處理的方式、資料管理者預期的利益、所涉及的個人利益、相關組

[19] 具體而言，位置資料可包括透過「全球定位系統」、「基地台位置資訊」以及「WiFi 無線接收裝置的 MAC 位址」所顯示的個人位置資料。關於現代定位科技與隱私權的保障，參見李明勳，合理隱私期待之研究－以定位科技為例，國立政治大學法律學研究所碩士論文，2013 年 7 月，頁 73-139。

[20] GDPR Recital 30.

[21] *See generally* Article 29 Working Party, Opinion on the Use of Location Data with a View to Providing Value-added Services (November 2005), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (June 20, 2007) , *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf [hereinafter *Personal Data Opinion*] (last visited: Dec. 26, 2016).

[22] Directive Recital 26.

織或技術上的風險(如：違反保密義務的可能)，如資料將長時間儲存，並應將預計保存期間內因科技進步或其他原因而導致識別的可能性，一併納入評估[23]。或許受到前述工作小組建議的影響，在本次歐盟個資規則的立法說明中，即明確表示所謂合理可能使用方式的判斷，必須考量「所有客觀因素，例如：識別所需要的成本與時間，並將資料蒐集、處理或利用時可得的科技以及相關科技的發展一併納入考量」[24]。

### 第二款　新增「去連結（pseudonymisation）資料」的定義

在歐盟個資規則有關個人資料定義的規定中，另一項值得重視的發展是新增「去連結資料」的定義。依據歐盟個資規則第第 4 條第(5)項，所謂「去連結」指：「**在不使用額外資料的情形下，無法將個人資料歸屬於特定個人的資料處理或利用方式；但該額外資料必須分別保管，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**」[25]。

關於上述規定，有以下幾點值得進一步說明。首先，在歐盟執委會最初提出的草案版本中，並沒有去連結資料的相關規定，而是到了 LIBE Committee 報告及歐洲議會一讀版本的草案中才第一次出現。其後，在歐盟理事會、三方協商版草案，乃至於最後通過版本的立法理由中，都明確說明使用去連結資料有助於降低資料當事人的風險，並可協助資料管理者達成資料保護的義務[26]；上述版本草案的立法理由甚至進一步表示，為提供使用去連結資料的誘因，即便是同一資料管理者，只要將額外資料分別保存，並採取技術及組織上的措施遵守規則的規定，也可以使用去連結的資料[27]。

---

[23] *See Personal Data Opinion, supra* note 21, at 11-12.
[24] GDPR Recital 26.
[25] 本項規定的原文為：" 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."
[26] GDPR Recital 28.
[27] GDPR Recital 29.

其次，更重要者，歐盟個資規則後續條文也將去連結資料融入相關資料保護機制的設計之中。例如，歐盟個資規則第 6 條第 4 項，類似我國個資法個人資料目的外利用，資料管理者必須判斷後續利用目的與原始蒐集目的是否相容（compatible），而「是否存在適當的安全措施，包括加密或去連結」即是其中一項考量因素[28]。又如，歐盟個資規則第 89 條特別針對「基於公益的檔案保存、科學或歷史研究目的，或統計目的」的資料利用加以規範，其中也強調必須有符合規則要求的適當安全措施，以保障資料當事人的權利與自由；而所謂的安全措施，則可能包括使用去連結資料[29]。

除上述兩個條文外，在歐盟個資規則第 25 條（透過設計保障個資及預設個資保護）、第 32 條（資料蒐集、處理或利用的安全）及第 40 條（行為準則）等規定中，也都有提及去連結（資料）；或將之作為安全維護措施的例示，或將其列為相關行為準則得規範事項之一。

### 第三款　不可回復的去識別資料

最後，如同指令時代的處理方式，雖然在歐盟個資規則本文中並沒有正式定義「不可回復的去識別資訊（anonymous information）」，但在立法理由中，卻對此一「不受」規則規範的「非」個人資料有較指令更為明確說明。依據歐盟個資規則立法理由第 26 點，所謂「不可回復的去識別資料」指「**與一已識別或足資識別的自然人無關的資訊（information which does not relate to an identified or identifiable natural person）**」或「**原本屬於個人資料，但經過去識別化處理，已無法（再）識別資料當事人（personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable）**」。

如資訊符合上述定義，有關個人資料保護的各項原則即無適用餘地；即便為統計或研究目的使用此等不可回復的去識別資料，也不在歐盟個資規則的規制範

[28] GDPR Section 4 (e), Article 6.
[29] GDPR Section 1, Article 89; GDPR Recital 156.

圍。然應注意者，依據歐盟個資規則第 89 條第 1 項的規定，為檔案保存、科學或歷史研究目的或統計目的使用個人資料，如相關利用目的可以利用無法（再）識別特定資料當事人的方式達成時，歐盟個資規則要求資料管理者或受託者應使用此種方式，似寓有鼓勵使用不可回復的去識別資料之意。

### 第三項　資料處理之要件

#### 第一款　一般資料蒐集、處理與利用的要件

關於一般個人資料蒐集、處理或利用的合法要件，歐盟個資規則於第 6 條第 1 項定有六款事由，基本上延續指令既有的規定。然而，值得注意者，對於部分合法要件，歐盟個資規則有較指令更明確的定義與嚴格的要求。以下即針對有特別修正的部分加以討論、說明。

**一、 當事人同意**

在指令時代，「**資料當事人『明確地（毫不含混地，unambiguously）』同意**」，是個人資料合法蒐集、處理或利用的要件之一。在歐盟個資規則中，此一要件仍然維持，只是文字稍加修正，成為：「**資料當事人同意為了一項或數項特定目的，蒐集、處理或利用其個人資料**」。兩相比較，歐盟個資規則將同意的內涵完全移至定義條文處理，故將「明確地」的文字刪除，並特別強調當事人同意必須與特定目的結合。

值得注意者，相較於指令對於「同意」僅簡單規定，歐盟個資規則不但對同意的內涵有更為仔細的定義，且針對同意的條件（conditions for consent）及未成年人的同意都訂有特別規定。

首先，在同意的定義上，指令僅規定：「**同意是資料當事人經告知後，任何出於自由意願，允許其個人資料被蒐集、處理或利用的具體表示（any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed）**」。相對地，歐盟個資規則歷次草案及最終通過的版本第 4 條第（11）款，均將同意的定義修正為：

「**同意是資料當事人經告知後，任何出於自由意願，以聲明或清楚、積極的行為，允許其個人資料被蒐集、處理或利用的具體、明確表示（any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her**）」。比較前後兩項規定，新法主要增加：「**以聲明或清楚、積極的行為**」的要件，希望釐清指令時代「單純不作為（沈默）」是否符合同意要求的爭議[30]。

應注意者，即便歐盟個資規則新增此一要件，有關同意的形式，仍不以書面為限。依據立法理由的說明，任何積極的行為，例如：書面聲明（包括以電子方式為之）、口頭聲明均屬之；在實際操作上，在瀏覽網頁時，勾選同意的欄位、選擇技術上設定，或其他聲明或行動，只要能清楚表現資料當事人允許的意思，均符合規則的要求[31]。相對地，沈默、已預先勾選同意的欄位或不作為，都與規則同意的要件不符[32]。

其次，關於同意的條件，是本次歐盟個資規則新增的一大特色。從最初歐盟執委會提出的草案版本就有此一規定，其後的歷次版本也都予以維持，僅相關條件內容有所修正而已。以下即針對規則最終通過版本第 7 條所臚列的四項條件，加以說明與分析。第一、**以同意作為合法使用個人資料的事由時，當事人是否同意，應由資料管理者「證明（demonstrate）」**。應注意者，雖然最終通過的條文並未採取先前草案版本所使用的「負舉證責任（bear the burden to proof）」文字，但二者實際上應無明顯差異。關於此一條件，應可認為是歐盟個資規則沒有強制規定當事人同意須以「書面」為之的配套措施；亦即，藉由要求資料管理者證明

[30] 其實，在指令時代，歐盟資料保護工作小組即認為，因指令使用「表示(indication)」及「表明(signifying)」等字，解釋上資料主體應有一定的「作為(action)」方屬之，單純的不作為(或沈默)，不得認為符合指令同意的要求。Article 29 Data Prot. Working Party, Opinion 15/2011 on the Definition of Consent 11, No. 01197/11/EN, WP 187 (July 13, 2011) [hereinafter WP 187], *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.(last visited: Dec. 26, 2016).

[31] GDPR Recital 32.

[32] *Id.*

同意的存在，緩和了欠缺書面證明文件對資料當事人可能造成的不利益，並使資料管理者可以自行斟酌取得書面同意的成本與將來發生爭議舉證困難的風險[33]。

第二，**如果當事人同意是以書面聲明為之，而該書面同時包含其他事項，則當事人同意的部分必須與其他事項清楚分離，並且以清晰可理解、易於接近、清楚且淺白的文字呈現。任何違反本規則要求的聲明，都沒有拘束力。**此一規定類似我國個資法 104 年修正「前」第 7 條第 2 項規定的「單獨書面同意」（現行個資法施行細則第 15 條），但適用於所有書面同意的情形（與我國個資法限於目的外利用同意不同），且對資料管理者尋求當事人同意時所使用文字是否淺顯易懂、容易理解等，多有要求。考察此一條件的目的，主要在使當事人對同意的事項有清楚認識，避免資料管理者以夾帶方式，將個人資料使用的同意隱藏在其他事項之中，使當事人在不注意的情形下給予同意。

第三，**當事人有權隨時撤回其同意。當事人嗣後撤回同意，對撤回前基於同意所為蒐集、處理或利用的合法性不生影響。在當事人同意前，應告知上述事項。撤回同意應與給予同意一樣容易。**此一規定進一步確保當事人的自主權，只有當事人可以無礙的選擇撤回同意，其同意才是真正自由選擇的結果。

第四，**當評估同意是否出於自由意願時[34]，最重要的考量因素，諸如：契約的履行，包括服務的提供，是否以當事人同意蒐集、處理或利用非屬履行該契約必要範圍內的資料為條件**。此一規定主要在回應目前當事人經常「被迫同意」的問題。詳言之，日後業者如再以履行契約或提供服務「綑綁交換」當事人同意蒐集、處理或利用「無關」的個人資料，否則即拒絕服務的作法，就有可能被認為剝奪當事人選擇機會，而非出於自由意願，影響同意的效力。應說明者，此一規定雖然執行上可能產生不少爭議（例如：如何判斷相關資料與契約履行或服務提

[33] 不過論者有認為此一規定將降低資料管理者使用「當事人同意」作為蒐集合法事由的意願，*see* Paul M. Schwartz, EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation, 12 BNA Privacy and Security Law Report 718 (2013).

[34] 應說明者，依據立法說明第(43)點，所謂「自由意願」，主要取決於資料當事人是否有真正的選擇機會，或是否能在權益不受損的情形下拒絕或撤回同意。

供是否相關），但若能落實，確實有助於回復個人對於資料的自主控制。

再其次，近年來第 29 條工作小組特別重視資料管理者與資料主體間地位不對等，可能影響後者同意是否出於自由意願的問題，例如：醫病關係、僱傭關係中資料蒐集、處理、利用的同意[35]。針對上述問題，在歐盟執委會最初提出的草案版本中，原本訂有：「**如資料主體與資料管理者間地位明顯不對等，則同意不能作為資料蒐集、處理、利用的基礎**」的同意條件[36]。雖然上述規定最終「並未」成為歐盟個資規則的正式條文，但相同的內涵卻轉而在立法理由中呈現。

依據歐盟個資規則立法理由第(43)點的說明：在具體個案中，如資料主體與資料管理者間地位明顯不對等，則同意不能作為資料蒐集、處理、利用有效、合法的基礎，特別是在資料管理者是公務機關的情況，資料當事人在任何情形下都不太可能出於自由意願而同意。又，如果資料當事人針對不同的個人資料蒐集、處理或利用活動，不能分別（個別）同意，或履行契約、提供服務以當事人同意（個人資料的蒐集、處理或利用）為前提，而該同意又非履行契約所必要，則上述情況下的同意都將被推定非出於自由意願。

最後，歐盟個資規則特別針對未成年人使用「資訊社會服務（information society services）」的同意問題加以規範。依據規則第 8 條的規定：

**1. 當直接提供資訊社會服務予未成年人，且以同意作為蒐集、處理或利用其個人資料的基礎時，該未成年必須年滿 16**

---

[35] *See* WP 187, *supra* note 30, at 13. 以僱傭關係而言，如受僱人基於對雇主的依賴，擔心拒絕同意將遭到差別對待，甚或無法繼續工作，根本沒有拒絕的期待可能性時，受僱人的同意，即非出於自由意願的自主決定，應為無效；此外，在資料蒐集者是政府機關的情形，由於政府機關具有一定的權威，人民的決定原本就容易受到影響；更明顯的例子，如政府機關將資料主體的同意與機關提供的服務加以連結(即不同意即無法獲得一定的服務)，則此時資料主體的同意也無法滿足自主決定的要件。*Id*. at 13-16. 另參劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學，第 218 期，2013 年 7 月，頁 154-156。

[36] 原文為: "Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller." 應說明者，縱然有上述法律所規定的情形，並非指資料管理者不能蒐集、處理、利用個人資料，而僅是在當事人無法自由選擇的情形下，不能以「當事人同意」作為蒐集、處理或利用的正當事由；此時，資料管理者如欲使用個人資料，則應以其他更適當的法定事由作為依據，如在僱傭關係，雇主可以考慮主張履行契約或法定義務，至於在政府機關作為資料管理者的情形，則應直接以相關法律規定作為基礎。例如在前舉 IC 身分證的例子中，歐盟資料保護工作小組即建議政府應直接立法規範 IC 身分證的使用，並以之作為蒐集、處理、利用個人資料的合法基礎。*See* WP 187, *supra* note 29, at 16.

**歲，相關的資料使用才合法。當未成年人未滿 16 歲時，必須由行使親權者表示或授權同意，資料使用才合法。**

**會員國可以依據法律將同意年齡降低，但不得低於 13 歲。**

**2. 資料管理者必須考量現有的科技，付出合理地努力，以確認同意是由行使親權者所表示或授權。**

**3. (略)**

**二、 資料管理者履行法定義務所必要、為履行公益任務或執行職務所必要**

個資規則第 6 條承襲指令時代的規定，仍將「資料管理者履行法定義務所必要」（第 6 條第 1 項(c)款）及「為履行公益任務或執行職務所必要」（第 6 條第 1 項(e)款）列為一般個資蒐集、處理或利用的合法事由。值得注意者，在個資規則的立法理由中，對於上述兩款規定究應如何適用，有較以往更為清楚的說明與指引，有必要稍加介紹。

首先，依據立法理由第 45 點的說明，依據上述兩款規定蒐集、處理或利用個人資料均必須有歐盟或會員國法律的依據（the processing should have a basis in Union or Member State law）。此在基於「履行公益任務」而蒐集、處理或利用個資時，尤其值得注意；換言之，適用該款的前提，仍然必須有法律規定作為公益任務的依歸，不能僅是空泛的主張增進公共利益。

其次，就法律規定的密度而言，立法理由特別強調，此處所謂法律依據，「並未」要求法律針對「個別（each individual）」的資料蒐集、處理或利用行為，逐一具體規定；法律概括地針對數項資料蒐集、處理或利用行為加以規範即為已足。至於蒐集目的、蒐集資料類別、資料當事人範圍、資料利用對象、資料保存期間，以及得主張「履行公益任務或執行職務所必要」此一事由的資料管理者範圍（限於公務機關、受公法規範的私人，或受私法規範的職業團體）等事項，則可以由相關法律進一步規定。

最後，應特別說明者，依據立法理由第 41 點的說明，個資規則所稱的「法

律依據」,「並非」僅限於會員國「國會（parliament）」所制訂的規範（但會員國憲法另有規定者，不在此限）；但相關規定必須具體（precise）、明確（clear），而使受規範者得以預見。

## 三、 利益權衡條款

在指令時代即存在的「利益權衡」條款，在個資規則中也被保留，僅稍有文字更動。然值得注意者，本次個資規則新增禁止公務機關援引利益權衡條款，作為蒐集、處理或利用個資事由之規定；依據立法理由第 47 點之說明，主要係因公務機關蒐集、處理或利用個資之合法基礎應由立法者透過法律明文加以規定，因此排除公務機關適用利益權衡條款。

個資規則第 6 條第 1 項(f)款規定：「**為資料管理者或第三人合法利益（legitimate interest）所必要**」即得蒐集、處理或利用一般個資；**但「資料當事人（特別是當事人為兒童時）對該資料的保護，具有更重要的利益、權利或自由者，不在此限**」。此即所謂利益權衡條款，也可以將其視為一概括的一般個資合法蒐集、處理或利用事由。[37]考察此一規定的目的，主要在彌補其他具體事由的不足，以適應千變萬化的個人資料蒐集情況，並調和個人資料保護與個人資料的合理利用。

關於此一規定，有以下幾點說明。首先，雖然在本次個資規則中，將指令時代原本與「資料管理者」、「第三人」並列的「個人資料揭露對象（parties to whom the data are disclosed）」予以刪除，但從個資規則立法理由第 47 點可以發現，刪除的原因主要是所謂「個人資料揭露對象」已可包括在「資料管理者」的概念中，因此不需單獨規定。

其次，立法理由特別強調，在進行利益權衡時，必須將資料當事人基於其與資料管理者間關係所具有的合理期待，納入考量。例如：在資

[37] 應注意者，利益權衡條款僅適用於一般個人資料；至於特種個人資料，因攸關資料當事人權益，且原則上禁止蒐集、處理或利用，因此並無類似之規定。

料當事人是資料管理者客戶或服務對象的情況下，即可能存在本款所稱的合法利益。至於所謂合理期待，包括資料當事人在資料被蒐集時，依據當時的情境，是否可以合理期待其資料將被用於此一目的；如果資料進一步的利用並非資料當事人可以合理期待，則其對於該資料的保護即可能有較重要的利益。

最後，個資規則的立法理由也例示了一些可能的合法利益，包括：為了避免詐欺（preventing fraud）所絕對必要（strictly necessary）的個人資料蒐集、處理或利用行為，即可能構成資料管理者的合法利益；又如：直接行銷（direct marketing）也「可能（may）」被認為屬於合法利益。

## 第二款　特種資料處理之原則與例外

歐盟個資規則將個人資料區分為一般個人資料及特種個人資料，並分別就不同之資料類型區分其處理之要件。所謂特種資料，係指與民族或種族來源、政治見解、宗教或世界觀確信或所屬工會相關之個人資料，以及得明確識別特定人之基因資料、生物特徵資料，以及個人之健康資料或性生活或性傾向資料（歐盟個資規則第 9 條第 1 項），而上述特種資料原則上不得處理，僅於符合特定前提要件時，方例外得予處理，而歐盟個資規則第 9 條第 2 項即明訂例外得處理特種個人資料之情形，其要件之設定相較第 6 條就一般個人資料所定合法處理要件更為嚴格，包括：

- 當事人表示明確之同意，但若歐盟法或各會員國之法令明訂特種資料處理之禁止不得藉由當事人同意而解除時，則不在此限。
- 該處理為資料管理者或當事人主張其基於勞動法或社會安全或保護之法令所享有之權利所必要。
- 該處理係為保護當事人或其他自然人具生存重要性之法益所必要，且當事人出於身體或法律上原因無法表示同意。

- 該處理透過基於政治、世界觀、宗教或工會所設立之基金會、社團或其他組織提供適當保障，非以營利為目的且係於其法定權限範圍內所為，但該處理僅限於其成員或昔日成員或與為達成其業務目的而有經常性聯繫之人，且該個人資料在未經當事人同意前不得對外公開。

- 欲處理之個人資料已明顯由當事人公開。

- 該處理係為執行（Geltenmachung）、行使或保護（verteidigen）法律上之請求權或為法庭審理範圍內之司法職權所必要。

- 該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性（in angemessenem Verhältnis），維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而基於有重大之公益理由，認有必要者。

- 該處理係出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務之管理，依據歐盟法、會員國之法令或與擔任健康相關職業之成員（einem Angehörigen eines Gesundheitsberufs）間簽訂之契約，並符合第 3 項所定要件及保障，而認有必要者。

- 該處理係於公共衛生領域基於公益理由，例如為防範跨境之嚴重健康危害或為維護健康照護及醫藥產品的高品質及安全標準，並已依歐盟法或會員國法令採行維護當事人權利及自由之適當特殊措施，而認有必要者。

- 該處理係依據歐盟法或會員國法令，與其所欲達成目的間具合理關聯性，維護個人資料保護權利之本質，並訂有保護當事人基本權利及利益之適當特殊措施，而依據第 89 條第 1 項基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，認有必要者。

但針對涉及基因、生物特徵或健康資料之處理，歐盟個資規則第 9 條第 4 項允許各會員國維持或再另行訂定附加之要件，例如限制要件。另外，歐盟個資規則亦相當強調在處理特種個人資料前，應先確保已採行「保護當事人基本權利及利益之適當特殊措施」， 希望透過事前之預防，將特種資料遭到濫用之機會降至最低。

### 第三款　資料處理之特殊情形

歐盟個資規則第 9 章（第 85 條至第 91 條）中分別針對個人資料保護與言論及資訊自由（第 85 條）、官方檔卷之公開（第 86 條）、國家代碼之處理（第 87 條）、受僱者資料之處理（第 88 條）以及基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理（第 89 條）等個人資料處理之特殊情形，為進一步之規範。

#### 第一目　個人資料保護與言論及資訊自由保障

歐盟個資規則第 85 條著眼於個人資料保護以及資訊公開流通與意見表達之權利間之相互平衡，亦被稱為是「媒體特權（Medienprivileg）」條款，其採行開放式之立法，透過第 85 條第 1 項將基於新聞報導、學術、藝術或文學目的之個人資料處理，交由各會員國自行訂定法規予以規範，並允許其就歐盟個資規則第 2 章（基本原則）、第 3 章（當事人權利）、第 4 章（管理者及受託利用者）、第 5 章（個人資料之第三國或國際組織傳輸）、第 6 章（獨立監督機關）及第 9 章（特殊處理情形）之規定，為不同或例外規定，但以為求取個人資料保護與言論及資訊自由之平衡所必要者為限。但此種以概括條款（Öffnungsklausel）形式予以規範之作法，亦招致批評，認其對協調歐盟個人資料保護與言論自由之平衡毫無建樹，而仍須仰賴後續各會員國之立法者，方可能有所進展[38]。

[38] Tinnefeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas, Einführung in das Datenschutzrecht, 5. Aufl., 2014, S. 175.

而針對各會員國依據第 85 條第 2 項所訂定之法令，包括於後續所有相應修正之法律或該法令之修訂，皆應立即告知歐盟執委會（第 85 條第 3 項）。

### 第二目　個人資料保護與官方檔卷之公開

歐盟基本權利憲章即已揭示歐盟各機構公開透明其資訊之重要及必要性[39]，歐盟個資規則第 86 條亦規定行政機關、公法機構或履行公益任務之私法機構所持有官方檔卷（amtliche Dokumenten）中之個人資料，得由該行政機關或機構依據其應遵循之歐盟或各會員國之法令公開，以求取官方檔卷向公眾公開與本規則所欲保護之個人資料權利之平衡。

### 第三目　國家代碼之處理

歐盟個資規則第 87 條授權各會員國得進一步規定，在何種特定條件下，一般所理解之國家代碼（nationale Kennziffer）或其他標示，得作為處理之標的。一般所理解之國家代碼或其他標示僅得作為確保依據本規則所欲保障之當事人權利或自由適於實踐時方得處理。

### 第四目　受僱者之個人資料保護

受僱者之個人資料保護（Beschäftigtendatenschutz），係指針對受僱者或勞工與僱傭或勞動關係密切相關個人資料之處理行為予以規範，於此特別關注者，乃基於聘用、履行或終止僱傭或勞動契約之目的，包括履行法令或團體協約所定義務、管理、工作計畫及組織、工作場所之平等及多樣性、工作場所之健康及安全、保護雇主或客戶之財產權、受僱者個別或集體權利之行使等，而處理受僱者個人資料之行為（第 88 條第 1 項）。

---

[39] 歐盟基本權利憲章第 42 條明訂有接近歐盟機構文件之權利，據此得主張公開之標的及於歐洲議會、理事會及執委會所持有之文件，文件之概念採廣義之理解而包括所有形式之載體，紙本、以電子形式儲存之聲音、圖片、影音，或是僅得於內部系統使用之檔案均屬之。此一權利之主張得與其他權利相互重疊，例如於歐盟基本權利憲章第 41 條規範每個人得要求良好行政的權利，並進一步於第 2 項第 2 款闡明其保障範圍包括每個人皆享有得近用與其相關檔卷之權利;或是前述歐盟基本權利憲章第 11 條第 1 項接收資訊之自由等。 此一接近歐盟機構文件之權利主要透過歐盟第 1049/2001 號規則予以具體落實，並以之作為請求之依據。

歐盟個資規則就受僱者之個人資料保護，雖未選擇細節性之規範模式，而是以概括條款之形式，交由各會員國自行訂定法令或藉由簽訂團體協約（Kollektivvereinbarung）規範之，以確保受僱者於工作環境中應享有之個人資料保護，但其無疑仍應受到歐盟個資規則所揭示一般性原則之拘束，例如：目的拘束原則、資料縮減原則、透明原則等，並於歐盟個資規則第 88 條第 2 項中特別強調，其所制定之相關法令或簽訂之團體協約中，應顧及為維護人性尊嚴而採行之適當及特殊措施，當事人之合法利益與權利，並特別關注處理過程之透明，公司集團間或與公司共同進行經濟上活動之團體間的資料傳輸，以及工作場所之監控系統。而各會員國依據第 88 條第 1 項所頒訂之法令，應於 2018 年 5 月 25 日前告知執委會，後續之法令修訂，亦應立即告知（第 88 條第 3 項）。

另外，一旦該處理係出於健康照護或為判斷受僱者工作能力之勞動醫學，為了醫學上之診斷、健康或社會領域之照護或治療或為了健康或社會領域之體系或服務管理所必要，且該處理係由專業人員親自或在其監督下為之，而相關人員依法負有保密義務時，歐盟個資規則第 9 條第 2 項第 h 款亦允許例外處理受僱者之特種資料。

### 第五目　基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的而進行之個人資料處理

歐盟個資規則針對基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的，而進行之個人資料處理，賦予其特殊之優先地位：首先，歐盟個資規則第 5 條第 1 項第 b 款後段針對基於上述目的所為資料處理，排除目的拘束原則之適用，亦即，基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的等非原始目的，進一步處理個人資料之行為，被視為目的內之處理；其次，歐盟個資規則第 9 條第 2 項第 j 款賦予各會員國就基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，認有處理必要之特種資料，享有自行訂定例外規

範之空間，但其連結第 89 條所定要件，強調應提供充分之保障，採行技術上或組織上之相關措施，強化個人資料之保護，例如：運用不可回復之去識別化或是以去連結（Pseudonymisierung）的技術進行處理；最後，歐盟個資規則第 89 條第 2 項[40]及第 3 項[41]中，針對當事人特定權利之行使，一旦可能導致上述目的無法達成或受到嚴重妨礙時，即得予以限制之，但該限制以達成目的所必要者為限。

### 第六目　教會及宗教團體組織現行資料保護規範之適用

歐盟個資規則同樣適用於教會及宗教團體組織，但就其處理個人資料之規範，歐盟個資規則第 91 條第 1 項係以概括條款之形式予以規範：針對在歐盟個資規則生效前，教會及宗教團體組織適用以處理個人資料之規定，在與歐盟個資規則相互合致之前提下，得繼續適用，因此，各會員國針對教會及宗教團體組織處理個人資料，並無訂定新規範之急迫性，但仍應全面檢視現行規範是否與歐盟個資規則之內容有所歧異或衝突，而為適當修正或補充。

另外，歐盟個資規則第 91 條第 2 項要求教會及宗教團體組織處理個人資料之行為，應受獨立監督機關之監督，但允許其以特殊形式為之，以確保教會在憲法或歐洲法層次上所享有之自治權限，但該監督機關仍應符合歐盟個資規則第 6 章對監督機關之要求，特別是應確保其得獨立行使職權。

但上述歐盟個資規則就資料處理特殊情況之相關規定中，可初步發現，其透過置入大量的不確定法律概念以及概括條款，以及藉由法益權衡之方式，留給各會員國立法者在後續型塑其國內個人資料保護法制時，相當大的形成空間。因此，

[40] 歐盟個資規則第 89 條第 2 項：「基於學術或歷史研究目的以及統計目的處理個人資料，得於歐盟法或各會員國之法令中保留同條第 1 項所定條件與保障之適用，當第 15 條、第 16 條、第 18 條及第 21 條所定權利可能導致該特殊目的無法達成或受到嚴重妨礙且此限制係屬達成目的所必要者。」

[41] 歐盟個資規則第 89 條第 3 項：「基於公益之檔案儲存目的處理個人資料，得於歐盟法或各會員國之法令中保留同條第 1 項所定條件與保障之適用，當第 15 條、第 16 條、第 18 條、第 19 條、第 20 條及第 21 條所定權利可能導致該特殊目的無法達成或受到嚴重妨礙且此之限制係屬達成目的所必要者。」

即便歐盟採用「規則」之立法形式，但其實質內涵，仍有待各會員國之立法者進一步具體詮釋，而使歐盟個資規則有指令化之趨勢，但亦使得歐盟個資規則與各會員國法制間的互動與交互影響，受到高度關注。[42]

### 第四項　當事人之權利

#### 第一款　查詢、閱覽與複製權

個資規則第 15 條賦予當事人查詢、閱覽與複製的權利。此一權利在指令時代即已存在，但新法規定的權利內涵則更為豐富，除既有的答覆查詢是否有蒐集、處理或利用當事人的個資、蒐集目的、個資種類、利用對象或其類型（特別是位於第三國或國際組織的利用對象）、資料來源，以及是否使用自動化決定及其邏輯以外，個資規則進一步規定當事人有權取得以下資訊：當個資被傳遞至第三國或國際組織時，資料管理者依第 46 條規定所採取的適當安全措施為何、資料預計的保存期間或用以決定保存期間的標準及相關權利（包括更正、刪除、異議及向監督機關提出申訴）的教示資訊。

值得注意者，本次個資規則對於答覆查詢的「方式」有明確規定，亦即當資料當事人以電子方式（electronic means）提出查詢等申請時，除當事人另有表示外，資料管理者應以常用的電子格式（commonly used electronic form）答覆查詢或提供相關資訊。而在立法理由第 63 點中更提及，如果可行，資料管理者應使資料當事人得以從遠端透過安全的查詢系統( remote access to a secured system)，直接查詢其個人資料。

又，依據上述立法理由的說明，資料當事人行使此一權利應有合理間隔（reasonable interval）；如資料管理者所保有的個人資料數量龐大，資料管理者可要求當事人具體指明其所查詢的個人資料究竟為何，或請其指明特定的蒐集、處

[42] Benecke, Alexander/ Wagner, Julian, Ö ffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG- Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 10/2016, S.604-608. Kühling, Jürgen/ Martini, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 12/2016, S. 449-450.

理或利用活動，以方便提供資訊。

### 第二款　更正權

歐盟個資規則第 16 條賦予當事人有權要求管理者立即更正其持有之不正確之個人資料，在與處理目的相符之範圍內，當事人有權要求將不完整之個人資料補全，即便是透過附加說明之形式。

各會員國得針對基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的，處理個人資料之行為，得訂定法令限制當事人更正權之行使，若該權利之主張可能導致上述目的無法達成或受到嚴重妨礙，且此限制係屬達成目的所必要（歐盟個資規則第 89 條第 2、3 項）。但若該個人資料之處理係基於多重目的同時進行，僅得就基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的所為之處理行為，限制當事人之權利（歐盟個資規則第 89 條第 4 項）。

### 第三款　刪除權（被遺忘之權利）

刪除權實為個人資料保護法制中，當事人自主控制權利之具體展現，但人民作為個人資料之主體，其所得主張傳統權利的類型，其內涵應如何配合科技的發展與進步相應演進，值得關注。[43]隨著資料數量爆炸性地成長，搜尋引擎應運而生，然而，在輕敲鍵盤與滑鼠，不費吹灰之力，即可不受限於時間、空間快速彙整資訊，已然成為現今之常態，昔日隨著時間流逝，會自然逐漸被人們淡忘的期待，似成為奢求。但 2014 年 5 月 13 日，歐洲法院作成 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González 案[44]判決，卻是首次深入討論「被遺忘之權利（Recht auf Vergessenwerden）」在個資保護上，作

[43] 劉靜怡，社群網路時代的隱私困境：以 Facebook 為討論對象，臺大法學論叢，第 41 卷第 1 期，2012 年 3 月，頁 43-45。

[44] EuGH, Urt. v. 13. 05. 2014, C-131/12, Google Inc.v Agencia Española de Protección de Datos (AEPD), *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN (last visited:Dec. 26,2016).

為基本權利的發展及其意涵，[45]其中包括其於歐盟基本權利憲章中之依據、保護範圍、限制之限制以及基本權利第三人效力等精彩之論證。[46]

「被遺忘之權利」在歐盟個資保護法制中之發展，在 1995 年個人資料保護指令第 12 條第 b 款中，即可窺其一斑：其要求各會員國應確保，當事人於資料管理者未遵循指令處理個人資料，特別是當資料不完整或不正確時，得要求資料管理者更正、刪除或限制該資料之使用；[47]而在 2012 年提出之歐盟個資規則草案，歐盟執委會及議會所提出之版本中，亦分別得見對於被遺忘權利之著墨；[48]隨著歐盟個資規則之公布，更將其明訂於第 17 條中，與刪除權並列，並就其行使要件作了更精確之闡明，以樹立歐盟各國一體適用之標準。[49]

依據歐盟個資規則第 17 條第 1 項規定，當事人有權要求資料管理者立即刪除其個人資料，而於有下列原因之一時，資料管理者負有刪除之義務：

- 該個人資料對於當時蒐集或處理之目的已無必要。
- 當事人撤回（widerrufen）依據第 6 條第 1 項第 a 款或第 9 條第 2 項第 a 款處理資料所需之同意，且該處理欠缺其他之法律依據。
- 當事人依據第 21 條第 1 項對於處理提出異議(Wiederspruch)，且該處理未具備有更優先之正當理由，或當事人依據第 21 條第 2 項對於處理提出異議。
- 個人資料被違法的處理。

---

[45] 但被遺忘的權利在歐洲法院判決做成後，究竟應如何在實務上取得具一致性之判斷標準，展開了對隱私權、知的權利與表達權利的論辯，包括刪除之作業時間、個人資料保護與公益間之權衡等，仍多有爭論，相關判決請參考 LG Köln, 13. 8. 2015-28 O 75/15. LG Heidelberg, 9. 12. 2014- 2 O 162/13. OLG Hamburg, 7. 7. 2015, 7 U 29/12. Meyer, Sebastian/ Rempe, Christoph, Aktuelle Rechtsentwicklungen bei Suchmaschinen, K&R 5/2016, S. 311.

[46] Boehme-Neßler, Volker, Das Recht auf Vergessenwerden- Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 13/2014, S.827-829.

[47] 依據歐洲法院於 Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González 案中之見解，1995 年個人資料保護指令中所謂「未遵循指令處理個人資料」，並不限於狹隘之違反指令規範內容之行為，尚得及於該資料之使用，與原始蒐集之目的相較，已顯不適當、不相關或逾越之情形。

[48] 楊智傑，個人資料保護法制上「被遺忘權利」與「個人反對權」；從 2014 年西班牙 Google v. AEPD 案判決出發， 國會月刊，第 43 卷第 7 期，2015 年 7 月，頁 21-24。

[49] Kühling, Jürgen/ Martini, Mario, a.a.O. Fn.40, S. 450.

- 個人資料的刪除係資料管理者依據歐盟法或各會員國法規履行法定義務所必要。

- 個人資料已由資訊社會所提供服務依據第 8 條第 1 項所蒐集。

針對依據第 17 條第 1 項負有刪除義務之資料管理者，已將個人資料公開之情況，其應考量現行可行之科技技術及履行費用，採用適當之措施與技術形式，通知處理該個人資料之資料管理者，關於當事人所提出刪除所有與其個人資料之連結或其影本或複本之要求（第 17 條第 2 項）。由於被遺忘權之主張，並非「刪除搜尋結果所連結之資訊」，而多係「刪除搜尋結果之連結」，故其適用之判斷與刪除權仍有其差異，屬因應網路世代所發展出之新興權利，此一條款中所稱應通知之資料處理者，大多是針對經營網路搜尋引擎之業者，因資料一旦公開，往往即已進入搜尋引擎所連結之廣大資料庫中，而針對應刪除之個人資料，其連結亦應相應脫鉤，才有可能在網路的世界中，尋求被遺忘的可能性。但對於被遺忘之權利所得主張之範圍，以資料管理者「依據第 17 條第 1 項負有刪除義務」，並「已將個人資料公開」作為前提，但並不限於「資料不完整或不正確」之情況；且將原先 2012 年歐盟個資規則草案中，[50]對於「資料管理者對於授權第三人公開個人資料之情形，應為該公開負責」，之規定，轉變為僅負通知義務，以減輕資料管理者之義務。[51]

但當事人對於其所享有刪除權或是被遺忘權之行使，並非未受有限制，歐盟個資規則第 17 條第 3 項規定，當該個人資料之處理係為了下列情形所必要時，當事人即不得主張同條第 1 項及第 2 項之權利：

- 行使表達言論及資訊權。[52]

[50] 關於 2012 年草案規定之討論與評析，請參考徐彪豪，M2M 時代下的資料保護權利之進展-歐盟與日本觀察，科技法律透析，25 卷 11 期，2013 年，頁 53-55。
[51] 除了依據歐盟個資規則第 17 條第 2 項通知相關資料處理者外，第 19 條亦同時課予通知接收者之義務。
[52] 例如歐盟個資規則第 85 條針對保障言論自由及資訊自由，處理個人資料之情況，即於第 1 項

- 為履行依據歐盟或各會員國法令所課予資料管理者之法定義務或管理人受託履行與公益相關或行使公權力所需之任務。

- 依據第 9 條第 2 項第 h 款及第 i 款及第 9 條第 3 項基於公共健康領域內之公益理由。

- 依據第 89 條第 1 項基於公益儲存檔案之目的，學術或歷史研究目的或統計目的，而刪除權之行使可能對上述目的之實現造成嚴重妨礙或使其無法達成。

- 法律上權利之主張、行使或防禦。

因此，被遺忘之權利在主張時，勢必須於個案中，與其他利益進行權衡，包括公益及可能涉及之第三人利益，包括：言論自由、資訊自由、新聞自由或是學術自由等，其判斷的面向，包括涉及資料之類型、對於當事人私人生活之影響程度、公眾知的權利、當事人之身分角色（例如是否屬公眾人物），[53]而此處之法益權衡，亦往往是被遺忘權利在實務操作上所遇到的最大挑戰。

**第四款　限制處理**

歐盟個資規則第 18 條明訂，當事人若無意主張第 17 條之刪除權，則其亦可要求資料管理者及受託者限制對其個資之處理，相較於 2012 年的草案版本，歐盟個資規則選擇將此權利由刪除權與被遺忘權之規定中分離出來，單獨作為當事人得主張之權利類型之一，其亦提供了當事人對於自身個資自主控制權利與其他公益之間，例如：新聞自由、學術自由等，一個適度的緩衝空間。

當事人得限制資料管理者處理行為之情形包括：

- 當事人個人資料之正確性有疑義時。而於此情況下之限制處理，其期間之設

中授權各會員國得自訂法規，限制同規則中第 3 章中所定當事人權利之行使。

[53] Boehme-Neßler, Volker, a.a.O. Fn.44, S.829-830. 許炳華，被遺忘的權利：比較法之觀察，東吳法律學報，第 27 卷第 1 期，2015 年 7 月，頁 147-154。

定，應使資料管理者得有充分的時間查證該個人資料正確性；

- 處理係不合法，且當事人表明拒絕刪除，反而要求限制其個人資料之使用；
- 該個人資料之處理對於處理目的之達成已無必要，但其對於當事人主張、行使或防禦法律上權利仍有必要時；
- 當事人依據第 21 條第 1 項，對於處理提出異議，在尚未確認資料管理者處理之利益高過當事人所主張利益前，當事人得主張限制處理其個資。

若當事人主張上述之限制處理，則其個人資料除了本身之備份外，僅得於下列情形，方得處理之（歐盟個資規則第 18 條第 2 項）：

- 當事人同意；
- 為了主張、行使或防禦法律上權利；
- 為保護其他自然人或法人之權利；
- 出於維護歐盟之或會員國重要公益之理由。

而在限制處理結束前，資料管理者應即通知該當事人（歐盟個資規則第 18 條第 3 項）。

**第五款　通知義務**

歐盟個資規則第 19 條規定，管理者負有通知義務（Mitteilungspflicht），其應通知所有個人資料之接收者，任何依據第 16 條，第 17 條第 1 項及第 18 條所提出個人資料更正、刪除或限制處理之主張。但若通知顯不可能或需耗費不合比例之費用時，不在此限。若當事人要求，管理者應提供關於接收者之資訊。

各會員國得針對基於公益之檔案儲存目的，處理個人資料之行為，得訂定法令限縮通知義務之履行，但以該權利之主張可能導致上述目的無法達成或受到嚴重妨礙，且此限制係屬達成目的所必要者為限（歐盟個資規則第 89 條第 3 項）。

**第六款　資料可攜權**

歐盟個資規則第 20 條定有資料可攜權（Recht auf Datenübertragbarkeit），此

一權利可望得強化當事人對於其個人資料之掌控能力，所謂資料可攜權，即為當事人移轉其個人資料的權利，例如：將資料從一個資料管理系統移動到另一個系統，而不會受到資料管理者阻擋。當事人有權要求已獲取其資料之資料管理者，以有組織的、常用的及機器可辨識之格式提供其個人資料之複本，且其有權透過該資料管理者無障礙地將該個資傳輸予其他資料管理者，此一規定尤其減輕了當事人在不同社會網絡（soziales Netzwerk）間轉換時，資料傳輸之困難度，而無須憂慮資料遺失或因此需重新建立資料檔案[54]，但其僅限於藉由自動化程序完成之資料處理，且必須經當事人同意或基於與當事人間之契約關係，方得為之。當事人可自行選擇，其欲自行交付個人資料或經由已持有其個人資料之管理者直接將其個人資料傳輸予另一資料管理者（第 20 條第 2 項）。惟資料可攜權之行使，以不妨礙他人權利及自由為前提（第 20 條第 4 項）。

歐盟個資規則第 20 條第 3 項明訂，同規則第 17 條所定當事人之刪除權，其主張不因此受到影響，且該權利不適用於資料管理者為行使與公益相關之任務或受託行使公權力之所必要之資料處理（第 20 條第 3 項）。但各會員國得針對基於公益之檔案儲存目的，處理個人資料之行為，得訂定法令限制當事人資料可攜權之行使，若該權利之主張可能導致上述目的無法達成或受到嚴重妨礙，且此限制係屬達成目的所必要（歐盟個資規則第 89 條第 3 項）。

### 第七款　異議權

歐盟個資規則第 21 條賦予當事人對於基於公益、行使公權力或依據管理者或第三人之權益所進行之合法處理，有表示一般性異議之權利，當當事人行使異議權，管理者僅得於其可證明處理之急迫正當性，高過當事人之法益、權利或自由時，方得繼續為之。無條件之異議權僅於基於直接行銷目的所為之資料處理，方有其適用（第 21 條第 2、3 項），當事人應以明確、可理解之形式，與其他資

[54] Kühling, Jürgen/ Martini, Mario,a.a.O. Fn.40, S. 450.

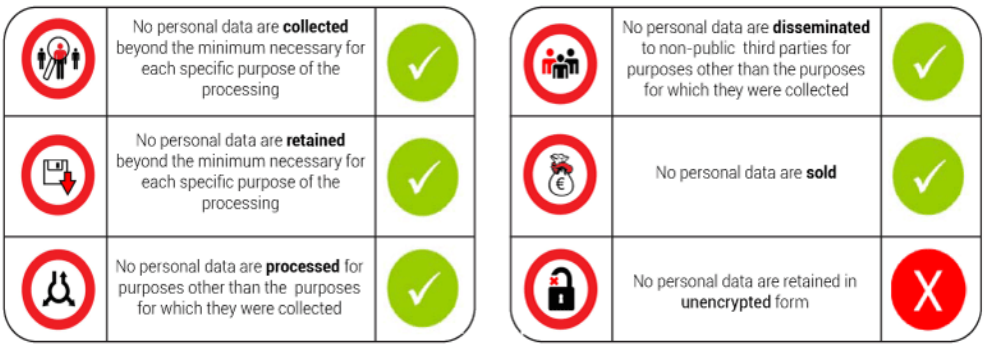
訊分離，單獨表示異議（第 21 條第 4 項）。

各會員國得針對基於公益之檔案儲存目的、學術或歷史研究目的以及統計目的處理個人資料之行為，訂定法令限制當事人異議權之行使，但以該權利之主張可能導致上述目的無法達成或受到嚴重妨礙，且此限制係屬達成上述目的所必要者為限（歐盟個資規則第 89 條第 2、3 項）。

## 第五項　資料管理者之義務（告知、通知、安全維護）

### 第一款　告知義務

歐盟個資規則草案本次修正的重點之一即在於告知義務的修正。在草案階段，除曾極具創意地試圖新增「圖形化、標準化」的告知方式，以方便當事人迅速閱讀吸收基本重要資訊（見下圖），[55]也進一步擴大應告知事項的範圍，其目的似在於回應目前當事人難以消化相關告知資訊，或未能獲得充分資訊，以致無法有意義行使資料自主權的質疑。




雖然個資規則最後通過的版本與草案稍有不同，但基本方向仍然維持「確保當事人容易瞭解」、「擴大告知事項範圍」的基調。以下即扼要說明本次新增規定的內容。

[55] 個資規則草案曾試圖新增第 13a 條，要求資料管理者應先將以下六項「標準資訊政策（standard information policy）」以「圖形及文字併陳」的方式告知當事人，包括：是否僅蒐集目的最小必要（minimum necessary）範圍內蒐集個人資料、所蒐集個人資料的保存期限是否逾越蒐集目的的最小必要範圍、是否進行蒐集目的以外的利用、所蒐集的個人資料是否傳遞予商業第三人（commercial third party）、所蒐集的個人資料是否出售或出租，以及所蒐集的個人資料是否以非加密方式保存。

首先，個資規則草案第 12 條新增「**告知的一般性要求**」，將告知內容形式、告知方式、費用收取、當事人權利濫用等事項集中予以規定。應說明者，相關規定不僅適用於告知事項，即便是前述有關當事人權利行使的告知與答覆，也有適用。

依據第 12 條第 1 項的規定，告知事項內容：「**應簡潔、清楚易懂、具有可接近性，並使用淺白詞語，向兒童告知時，尤應遵守此一規定**」。同項後段則針對告知的「方式」加以規定，原則上應以「**書面或其他方式（包括：適當時，得以電子方式）告知；如資料當事人要求，且其身分經確認，相關資訊可以口頭方式告知**」。

第 12 條第 5 項進一步規定：「依據第 13 條及第 14 條提供資訊，或依第 15 條至第 22 條及第 34 條所為之通訊或其他行為均應免費為之。」此外，對於資料當事人「明顯無理由或濫權（manifestly unfounded or excessive request）的請求（特別是重複申請的情形）」，第 5 項後段也允許資料管理者選擇：「（a）考量提供資訊或通訊或其他行為的行政成本，收取合理費用；或（b）拒絕處理該請求。」然資料管理者對於相關請求明無理由或濫權應負擔舉證責任。

至於在草案階段曾提出的圖形化、標準化告知，最終並未強制採行。依據個資規則第 12 條第 7 項規定，資料管理者得自由選擇是否搭配其他告知事項一併為之，以便資料當事人輕鬆掌握與瞭解資料蒐集、處理或利用的活動。有關標準圖示的內容及取得程序，則授權執委會另行規定（第 12 條第 8 項），不在規則本身予以規範。

其次，在告知事項的內涵上，不論是直接蒐集或間接蒐集的告知事項，歐盟個資規則都有增加；同時，更值得注意的是新法採取「兩階段告知」的模式，亦即區分必要告知的「基本告知事項」，以及為了確保資料蒐集、處理或利用公平與透明的「進階告知事項」。

詳言之，在個人資料是直接向當事人蒐集的情形（直接蒐集），依據第 13 條第 1 項的規定，資料管理者在取得個人資料時即必須告知以下基本事項：

- 資料蒐集者的名稱及聯絡方式
- 資料保護專責人員聯絡方式（如有適用）
- 蒐集資料的目的及合法事由
- 基於第 6 條第 1 項(f)款蒐集時的合法利益為何
- 個人資料的收受者或其類別
- 資料管理者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定

除上述事項外，如為確保資料蒐集、處理或利用的公平或透明所必要，資料管理者須進一步告知以下資訊（第 13 條第 2 項）：

- 個人資料保存期限或其決定標準
- 當事人相關權利
- 當事人得隨時撤回其同意
- 當事人向監督機關提出申訴之權利
- 提供資料是否是基於法律規定或契約要求或締結契約所必須、當事人是否得自由選擇提供個人資料及不提供對其權益的影響
- 是否存在自動化決定（automated decision-making），包括資料剖析（profiling），與自動化決定的邏輯與對當事人可能的影響

依據第 13 條第 4 項的規定，以上告知事項（不論是基本告知或是進階告知），只有在當事人已知悉相關資訊的情形下，才能免除。

至於資料管理者「並非」自資料當事人處取得個人資料的情形（間接蒐集），告知事項也分為兩階段。依據第 14 條第 1 項的規定，基本告知事項包括：

- 資料蒐集者的名稱及聯絡方式
- 資料保護專責人員聯絡方式（如有適用）
- 蒐集資料的目的及合法事由
- 蒐集個人資料之類別
- 個人資料的收受者或其類別
- 資料管理者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定

而為確保資料蒐集、處理或利用的公平與透明所必要，間接蒐集時須進一步告知以下資訊（第 14 條第 2 項）：

- 個人資料保存期限或其決定標準
- 基於第 6 條第 1 項(f)款蒐集時之合法利益為何
- 當事人相關權利
- 當事人得隨時撤回其同意
- 當事人向監督機關提出申訴之權利
- 個人資料的來源以及是否源自一般可得的來源
- 是否存在自動化決定，包括資料剖析，與自動化決定的邏輯與對當事人可能的影響

應說明者，在間接蒐集的情形，因資料管理者取得個人資料時並未與資料當

事人接觸，因此應於何時告知上述事項即可能產生疑義。在指令時代，第 11 條第 1 項規定，資料管理者應於錄存（recording）個人資料或第一次利用（向第三人揭露）個人資料時，進行告知。本次個資規則修正，則將告知的時點，細分為以下三種情形（第 14 條第 3 項）：

- 在取得個人資料後合理期間內（within a reasonable period）告知；但考量個人資料蒐集、處理或利用的具體情形，至遲應於一個月內為之；
- 若將使用該個人資料與當事人聯繫，至遲應於第一次與當事人聯繫時告知；或
- 若該個人資料預計將對第三人揭露，至遲應於第一次揭露時告知。

最後，有關間接蒐集的告知義務，依據個資規則第 14 條第 5 項的規定，在以下情形不予適用：

- 當事人已經知悉相關資訊；
- 提供資料不具可能性（impossible）或將涉及不成比例的努力，特別是基於公益目的的檔案保存、科學或歷史研究目的或統計目的，或提供基本告知事項將嚴重影響資料蒐集、處理或利用目的的達成；
- 資料管理者係基於歐盟或會員國法律取得相關資料，且對資料當事人的合法利益有適當保障；
- 基於歐盟或會員國法律所課予之職業上保密義務

### 第二款　個資外洩的通知義務

本次歐盟個資規則修正，將發源於美國法制的「個資外洩通知（data breach notification）」義務，納入一般性的個人資料保護規範中。此前，歐盟曾在 2002 年電子通訊隱私指令（2002/58/EC）中規定了此一義務，但適用範圍有限。有關

個資外洩通知義務的規定，在新法中共有兩個條文，分別規定對監督機關的通知義務及對資料當事人的通知義務。

就前者而言，個資規則第 33 條第 1 項規定：「當個人資料外洩，資料管理者應避免不當拖延（without undue delay），並在可能的情形下（where feasible），於知悉（become aware of）事件發生後 72 小時內，通知第 55 條規定所定的監督機關。但個資外洩不至於（unlikely）對自然人自由與權利產生危險者，不在此限。通知未能於 72 小時內為之者，資料管理者於通知時應說明理由。」在資料委託他人處理的情形，個資規則也明文規定：「受託者在知悉個資外洩後，應避免不當拖延，通知資料管理者」（第 33 條第 2 項），亦即統一由資料管理者負責通報。至於向監督機關通知的內容，依第 33 條第 3 項的規定，包括：

- 個資外洩事件本質的描述，包括受影響當事人之種類及其大略人數，以及外洩個人資料的種類及大略數量；
- 資料保護專責人員或其他聯絡窗口的姓名及聯絡方式；
- 描述個人資料外洩可能的影響
- 描述資料管理者已經採取或即將採取的因應措施，包括減輕或緩和個人資料外洩可能造成不利影響的作法。

有關個資外洩時向資料當事人的通知，個資規則第 34 條第 1 項則規定：「當個人資料外洩可能導致自然人自由或權利的高度風險（high risk）時，資料管理者應避免不當拖延，將個資外洩情事，通知資料當事人。」至於通知的形式與內容，個資規則也有要求；依據同條第 2 項的規定，除應以清楚淺白文字描述個資外洩的情形外，通知內容至少應包括以下三項資訊：

- 資料保護專責人員或其他聯絡窗口的姓名及聯絡方式；
- 描述個人資料外洩可能的影響

- 描述資料管理者已經採取或即將採取的因應措施，包括減輕或緩和個人資料外洩可能造成不利影響的作法

值得注意者，有關個資外洩對資料當事人的通知義務，除第 34 條第 1 項以「可能導致自由或權利的高度風險」作為啟動要件外，同條第 3 項更進一步列舉三項豁免通知的事由，以減輕資料管理者的負擔，並避免過度通知可能產生的「狼來了」效應（亦即資料當事人對於頻繁通知感到麻木或輕忽）。此三項事由包括：

- 資料管理者對於外洩的個人資料已採取適當地技術及組織上保護措施，例如：加密，使未經授權者，無法理解資料的內容。
- 資料管理者在事發後採取措施，使第 1 項所稱當事人自由或權利的高度風險不至於實現。
- （個別通知）須付出不合比例的努力（disproportionate effort）。於此情形下，資料管理者應採取公告或其他類似措施，使資料當事人以相同有效的方式知悉通知內容。

最後，第 34 條第 4 項規定，若資料管理者未依規定將個人資料外洩的情形通知當事人，監督機關於考量個資外洩導致高風險的可能性後，得命資料管理通知，或決定第 3 項各款豁免通知事由是否存在。

### 第三款　資料保護影響評估

本次歐盟個資規則修正的亮點之一，就是新增「資料保護影響評估（data protection impact assessment）」制度（第 35 條參照）。以下即分別針對此一制度的啟動要件、評估內涵、程序要求等事項，加以說明。

第一，在影響評估的啟動要件上，第 35 條第 1 項先「抽象」的規定：「凡特定類型的個人資料蒐集、處理或利用，特別是使用新科技，並考量其性質、範圍、情境及目的，可能對自然人的自由及權利產生高度風險時，資料管理者應先針對

預計資料活動對個人資料保護的影響，進行評估。」應說明者，由於此一評估的對象，是特定類型的資料蒐集、處理或利用活動，因此本項規定特別表明：「對於可能產生類似高風險的相似資料蒐集、處理或利用活動，可以僅進行一次評估。」

除了上述第 1 項的抽象規定外，第 35 條第 3 項特別針對三種具體情形，要求進行影響評估：

- 基於個人資料的自動化蒐集、處理或利用，包括剖析，對自然人個人進行系統性及大規模的分析，並據以對特定個人作成具有法律效果的決定或產生類似影響。
- 大規模蒐集、處理或利用第 9 條第 1 項規定的特種個人資料或第 10 條規定的前科資料。
- 大規模且系統性地監控公眾場所。

除了費心地對資料保護影響評估此一新制度的啟動要件，分別從抽象與具體兩方面直接加以規定外，個資規則第 35 條第 4 項進一步要求監督機關對外公告「應」進行資料保護影響評估的資料蒐集、處理或利用活動；同條第 5 項則授權監督機關得公告「不需」進行評估的資料蒐集、處理或利用活動，以資遵循。

第二、有關資料保護影響評估的內容，依據個資規則第 35 條第 7 項的規定，至少應包括以下事項：

- 對於預計進行的蒐集、處理或利用活動及其目的的系統性描述，包括：資料管理者所主張的合法利益。
- 蒐集、處理或利用活動達成目的必要性（necessity）與比例性（proportionality）的評估
- 對於資料當事人自由與權利所造成風險的評估

- 回應風險所預計採取的措施，包括保護措施、安全措施，以及考量資料當事人與其他關係人權利與合法利益，確保個人資料保護與符合本規則要求所採取的機制。

第三、有關資料保護影響評估的程序事項，包括第 35 條第 2 項規定，「當資料管理者有指定資料保護專責人員時，在進行評估時，應徵詢其意見」；同條第 9 款進一步規定：「適當時，資料管理者應就預計的資料蒐集、處理或利用，請資料當事人或其代表表示意見；但為保護商業或公共利益，或維護資料活動安全者不在此限。」

## 第六項　主管及監督機關

歐盟個資規則就個人資料保護之監督，最終仍維持二根支柱（Zwei-Säulen-Modell）之監管模式。[56]第一根支柱係藉由課予資料管理者及受託者設置資料保護監察人（Datenschutzbeauftragte）之義務，第二根支柱則是要求各會員國應建立一或多個獨立監督機關。

針對第一根支柱所要求設置之資料保護監察人，其相關規範見於歐盟個資規則第 4 章第 4 節（第 37-39 條）。其就應設置資料保護監察人之情形，明訂於歐盟個資規則第 37 條第 1 項，包括：由公務機關或公法組織（öffentliche Stelle）進行資料處理之情況，但法院於行使其司法職權之範圍內不在此限（第 1 款），另外，若在處理過程中，依據其形式、範圍及/或目的，必須廣泛地對當事人採行持續性並系統化的監視（第 2 款），或有處理第 9 條所稱特種個人資料或是第 10 條所定關於犯罪判斷及犯罪行為之個人資料的需求時（第 3 款），資料管理者及受託者皆應任命資料保護監察人。[57]但企業集團得任命共同之資料保護監察人

[56] Voßhoff, Andrea/ Hermerschmidt, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung, PinG 2/2016, S. 58.

[57] 若以德國聯邦個人資料保護法第 4f 條第 1 項為例，其就資料保護監察人（Beauftragter für den Datenschutz）之設置，即有較為明確之要件規範：無論是公務機關或非公務機關，只要有以自動化方式蒐集、處理或利用個人資料之情形，皆應以書面指定資料保護監察人；非公務機關至遲於開始行使其職權後 1 個月內需完成任用（第 2 句）；若是以其他方式蒐集、處理或利用個人資料，

（第 37 條第 2 項）；公務機關或公法組織亦得依據其組織架構及規模，任命共同之資料保護監察人（第 37 條第 3 項）；資料管理者或受託者，除了第 1 項所定應任命資料保護監察人之情況以外，亦得由其所屬之協會（Verband）及其他工會組織（Vereinigung），任命一位資料保護監察人（第 37 條第 4 項）。[58]資料保護監察人得為資料管理者或受託者之雇員，但其履行其任務時，不接受其指令，而是直接向資料管理者及受託者之最高管理階層為報告，但不因其執行任務之行為，而遭受解職或其他不利之待遇。[59]資料保護監察人之任命應關注其職業之資格，特別是其於資料保護法令及實務領域之專業智識，以及其履行任務之能力。資料保護監察人關於資料保護監察人之聯絡資訊，應對外公開並告知監督機關。

歐盟個資規則第 39 條明列資料保護監察人所擔負之任務，但並不以此為限：

- 告知資料管理者或受託者及其負責處理資料之雇員，關於其依據本規則以及依據其他歐盟或各會員國之資料保護規範，所擔負之義務，並提供及諮詢；
- 監督歐盟個資規則、其他歐盟或各會員國之資料保護規範、資料管理者或受託者之個人資料保護策略之遵行，包括職權之劃分、對於參與處理程序人員之教示（Sensibilisierung）及教育，以及與其相關之審查；
- 依請求提供資料保護影響評估之結果以及依據第 35 條實施監督相關之諮詢；

---

而有 20 位以上因此受僱時，亦同（第 3 句）。但非公務機關至多由 9 位雇員持續負責進行個人資料自動化處理時，不適用上述第 1 句及第 2 句之規定（第 4 句）。若公務機關組織架構所必須，多個領域得共同任命一名資料保護監察人（第 5 句）。而針對非公務機關執行遵守事先管控之自動化處理，基於業務上傳遞、匿名化傳遞或市場及意見調查之目的，以自動化方式處理個人資料者，不問其負責進行個人資料自動化處理之雇員人數，均應指定一名資料保護監察人（第 6 句）。

[58] 針對歐盟個資規則第 37 條第 4 項所定資料保護監察人之類型，若其明訂於歐盟或各會員國之法令時，則任命此種資料保護監察人將成為資料管理者及受託者之義務。

[59] 歐盟個資規則第 38 條第 3 項針對資料保護監察人之地位明定：「資料管理者及受託者應確保，資料保護監察人於履行其任務時，不接收關於履行任務之指示。資料管理者及受託者不得因資料保護監察人執行其任務之行為，而予以解職或不利之待遇。資料保護監察人直接向資料管理者及受託者之最高管理階層為報告。」

- 與監督機關共同合作；
- 作為監督機關處理與（資料）處理有關問題之受理單位（Anlaufstelle），包括依據第 36 條提供之前期諮詢（vorherige Kosultation），以及對於其他問題提供之建議。

相較於 1995 年歐盟個人資料保護指令，歐盟個資規則加重了資料保護監察人所擔負之任務，賦予更大保護個人資料之責任。個人資料保護監察人之設置，除了對於協調與強化歐盟個人資料保護體系有重大意義外，對於資料保護影響評估制度之落實，其亦扮演著關鍵性的角色。

第二根支柱要求各會員國應建立一或多個獨立監督機關，相關規定主要見於第 6 章，其一共分為二節，第 1 節著重於監督機關之獨立性（第 51-54 條），第 2 節則是規範監督機關之管轄、任務與職權（第 55-59 條）。透過上述規範，提供各會員國於建置其國內之個資保護監督機關時之框架，但細節之規範，例如調查權行使之程序及方式、其得訂定相關標準之具體內容等，仍將其留給各國立法者為進一步之型塑。於下將就歐盟個資規則對於監督機關之獨立性及其管轄、任務與職權之規定分別予以說明。

### 第一款　監督機關之獨立性

呼應歐盟基本權利憲章第 8 條第 3 項之規定：「關於本條之遵循應交由一獨立機構（unabhängige Stelle）監督。」歐盟個資規則亦強調透過確保監督機關之獨立性以強化個人資料之監管，歐盟個資規則第 51 條第 1 項即要求各會員國應設立一或多個獨立機關，作為本規則之主管機關，以確保自然人之基本權利及自由在資料處理過程中之保障以及使歐盟內個人資料之自由流通更為簡便（簡稱監督機關）。所有監督機關應共同致力於歐盟個資規則於歐盟一致性地適用。其彼此之間以及與歐盟執委會間應相互合作，以達成此目的。

為確保監督機關之獨立性，歐盟個資規則第 52 條明訂所有監督機關均依據歐盟個資規則全然獨立地履行任務或行使職權（第 1 項），監督機關之成員依據歐盟個資規則履行任務或行使職權時，不受到外界直接或間接之影響，亦無須請示或接受指示（第 2 項），並不得為與其擔任職務不相符之行為且不得於擔任職務期間執行其他與其職務不相符之有償或無償之職權（第 3 項），而每個會員國亦應確保各個監督機關所需人員、技術及經費來源、空間及設備之設置，以使監督機關在職務協助、共同合作及委員會中協力之任務及職權得以實踐(第 4 項)，並確保各個監督機關享有機關人事決定權（第 5 項），且財政僅受到不影響其獨立性之監督（第 6 項）。

在以維護監督機關獨立性之前提下，歐盟個資規則第 53 條針對各會員國內所設立之監督機關訂定一般性之要件，要求各會員國內所設立監督機關之成員應透過透明之程序，經由國會、政府、國家元首或依法賦予任命權限之獨立單位任命之（第 1 項）。每個成員需具備履行任務或行使職權所需資格、經驗及專業，特別是在個人資料保護之領域（第 2 項）。各成員之任期隨著職務期間結束而停止，其辭職或強制退休，依據各會員國之法律為之（第 3 項）。各成員職位之解除，僅得於其有重大失誤或履行任務之前提資格不復存在時，方得為之（第 4 項）。

針對監督機關之設置、監督機關成員所必要之資格予其他前提要件、任命監督機關成員之規範及程序、監督機關成員之任期[60]、是否以及何時重新任命監督機關成員以及監督機關成員與人員於任職期間與離職後之義務、禁止行為等，歐盟個資規則第 54 條第 1 項皆授權各會員國自行訂定法令規範之。但第 54 條第 2 項明文課予監督機關之成員及人員，於其任職期間或離職後，對於其於履行任務或行使職權時所知悉之所有秘密資訊，皆應負有保密之義務

[60] 歐盟個資規則第 54 條第 1 項第 d 款規定，監督機關成員任期至少 4 年，但其不適用於任期自 2016 年 5 月 24 起算者，當不同時間之任命係為維護監督機關之獨立性所必要者，部分任期可能較短。

（Verschweigenheitspflicht）。

### 第二款　監督機關之管轄、任務與職權

#### 第一目　管轄

所有監督機關履行任務或行使職權時，代表其所屬會員國之主權（歐盟個資規則第 55 條第 1 項）。其管轄範圍及於所有行政機關或私人單位依據歐盟個資規則第 6 條第 1 項第 c 款及第 e 款所為之處理（歐盟個資規則第 55 條第 2 項）。 但法院於其職權範圍內所為處理，非屬監督機關之監督範圍（歐盟個資規則第 55 條第 3 項）。

資料管理者或受託者之主要許可或唯一許可，由最高監督機關作為主管機關依據歐盟個資規則第 60 條核發（歐盟個資規則第 56 條第 1 項），其亦作為處理資料管理者或受託者逾越處理範圍問題的專責機關（歐盟個資規則第 56 條第 6 項）。但所有監督機關皆得處理向其提出之申訴或可能違反歐盟個資規則之行為，但僅以其與該監督機關所屬會員國核發許可相關或當事人僅於其所屬會員國內明顯地受到影響者為限（歐盟個資規則第 56 條第 2 項），並應立即通報最高監督機關，在通報後三週內，最高監督機關應決定，其是否應依據第 60 條所定程序處理，同時應關注資料管理者或受託者於通報之會員國內是否持有許可（歐盟個資規則第 56 條第 3 項）。最高監督機關決定處理時，適用第 60 條之程序。通報之監督機關得就該情況擬具決議草稿，最高監督機關決議時，應將其納入考量（歐盟個資規則第 56 條第 4 項）；若最高監督機關決定不處理，則由通報之監督機關依據歐盟個資規則第 61 條及第 62 條處理之（歐盟個資規則第 56 條第 5 項）。

#### 第二目　任務

依據歐盟個資規則第 57 條第 1 項，監督機關之任務包括：

- 監督並執行歐盟個資規則之適用，

- 使公眾知悉與資料處理相關之風險、規範、保障及其權利並為相應之說明。同時應特別關注對於孩童之特殊措施，

- 提供各國國會、政府及其他機構和歐盟個資委員會就保護自然人於資料處理時之權利及自由所採行行政和立法措施之諮詢，以求取各會員國法令之一致，

- 讓資料管理者和受託者知悉其依據歐盟個資規則所負擔之義務，

- 應任何當事人的詢問，提供其關於依據歐盟個資規則所得主張權利之資訊，或為了達成此一目的，與其他會員國之監督機關共同合作，

- 依據第 80 條處理當事人所提出申訴或由單位、組織或協會所提出之申訴，就申訴標的於適當範圍內進行調查，並於適當期限內通知申訴人調查之進行及其結果，特別是當需要更進一步調查或有與其他監督機關協調之必要時。

另外，同條第 2 項要求所有監督機關應簡化申訴之程序，如提供電子形式之申訴表格，但不得因此排除其他通訊之方式。

- 與其他監督機關合作，包括資訊交流、職務協助，使歐盟個資規則得一致地被適用與執行。

- 調查歐盟個資規則施行之情況，可同時參考其他監督機關或機關之資訊：

- 密切關注影響個人資料保護重大發展，特別是資訊與通訊技術之發展與實務操作（Geschäftspraktiken），

- 確立第 28 條第 8 項及第 46 條第 2 項第 d 款所稱標準契約條款（Standardvertragsklauseln），

- 建立並執行依據第 35 條第 4 項需進行資料保護影響評估（Datenschutz-Folgenabschätzung）之處理型態的清單，
- 提供關於第 36 條第 2 項所稱處理流程之諮詢，
- 推動制定第 40 條第 1 項之行為準則（Verhaltensregeln），其中應提供第 40 條第 5 項所規範之充分保障，並提供意見以及批准該準則，
- 引進資料保護驗證機制（Datenschutzzertifizierungsmechanism），提議第 42 條第 1 項之資料保護標章或驗證標章（Datenschutzsiegeln und -prüfzeichen），以及批准依據第 42 條第 5 項提出之驗證標準，
- 定期審核依據第 42 條第 7 項所核發之驗證，
- 整理並公布對於依據第 41 條監督行為準則遵循單位之認證（Akkreditierung）以及依據第 43 條之驗證單位（Zertifizierungsstelle）之標準，
- 對依據第 41 條監督行為準則遵循之單位以及依據第 43 條之驗證單位進行認證，
- 核准第 46 條第 3 項所稱契約條款及規定；
- 核准第 47 條所稱內部具拘束力條款；
- 負責歐盟個資委員會之職務報告；
- 建立關於違反歐盟個資規則以及依據第 58 條第 2 項所採行相應措施之內部目錄，
- 執行任何其他為落實個人資料保護之任務。

監督機關上述任務之履行，對於當事人或資料保護官皆屬免費（第 57 條第

3 項）。但對於顯無理由或-特別是針對經常性重複之情況-無節制（exzessiv）之查詢，監督機關得要求依據行政支出繳交適當費用或拒絕依據該查詢行使職權，但監督關對於查詢顯無理由或無節制之情形負有舉證責任（第 57 條第 4 項）。

歐盟個資規則中對於監督機關之任務範圍予以擴張，其不僅是針對非公務機關之資料資料管理者與受託資料管理者，同時及於公務機關，因此讓個人資料保護監督機關似乎享有高於其他機關之權限，甚至可以透過訂定命令拘束其他行政機關在其職權範圍內之個人資料處理行為，例如：限制其傳輸個人資料至第三國或要求刪除特定個人資料等，亦因此引發在既有行政組織架構中，行政機關間互動模式之討論，包括權限之劃分、機關間爭議之排解等[61]。

### 第三目　職權

#### 1. 調查權

任何監督機關依據歐盟個資規則第 58 條第 1 項，得行使下列調查權（Untersuchungsbefugnisse）：

- 向資料管理者、受託者或其代表指明，履行任務所需要其提供之所有資訊。
- 以資料保護審核形式進行之調查。
- 依據第 42 條第 7 項審核驗證。
- 提醒資料管理者或受託者避免違反歐盟個資規則之行為。
- 自資料管理者及受託者處取得其履行任務所必要之個人資料及資訊。
- 依據歐盟或各會員國之程序法令進入資料管理者及受託者之營業處所，

[61] Schaar, Peter, Datenschutz-Grundverordnung: Arbeitsauftrag für den deutschen Gesetzgeber, PinG 2/2016, S. 64. Voßhoff, Andrea/ Hermerschmidt, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung, PinG 2/2016, S. 59.

包括所有處理資料之設施及工具。[62]

**2. 輔助權**

任何監督機關依據歐盟個資規則第 58 條第 2 項，行使被下列輔助之職權(Abhilfebefugnisse)：

- 警告資料管理者或受託者其預計採行之處理流程可能違反歐盟個資規則。
- 警告資料管理者或受託者其所採行違反歐盟個資規則之處理流程。
- 向資料管理者或受託者指明，滿足當事人依據歐盟個資規則所享有權利。
- 向資料管理者或受託者指明，其處理流程應透過特定方式、於特定時間內達到歐盟個資規則之要求。
- 向資料管理者指明，通知個人資料受侵害之當事人。
- 處以暫時或永久的限制處理，包括禁止（處理）。
- 個人資料之更正或刪除或依據第 16、17 及 18 條之限制處理，以及通知依據第 17 條第 2 項及第 19 條公開個人資料之接收者，應採行之措施。
- 廢止驗證或要求驗證機關廢止依據第 42 及 43 條核發之驗證，或要求驗

[62] 對於進入檢查之權限，歐盟個資規則並未對於其程序、方式、範圍等為細節性之規範。若參考德國聯邦個人資料保護法（BDSG）中，分別針對聯邦及各邦之資料保護監察官對公務機關及非公務機關之監督權限之規定：第一，第 24 條針對公務機關之監督，於第 4 項中規定，聯邦公務機關負有義務，配合聯邦資料保護監察官及代表該機關之人之職權行使（第 1 句）。特別是針對答覆問題以及提供資料閱覽，特別是其已儲存及在資料處理程序中的資料；並應確保其得於任何時間進入辦公處所(Diensträume)（第 2 句）。但當聯邦最高機關認定，答覆或閱覽會危及聯邦或邦之安全時，即不適用第 2 句之規定。第二，同法第 38 條，針對非公務機關，由各邦之資料保護監察機構作為監督機關，其中第 4 項明訂，受監督機關委託行使監督權限之人，享有於營業或上班時間，進入該組織之不動產及營業處所，採行檢查審視之職權，當其屬履由監督機關交付任務有必要者（第 1 句）。其得閱覽經營資料，包括已儲存及在資料處理程序中的資料（第 2 句）。有答覆義務者對於上述措施負有容忍義務。

證機關停止驗證，當不符或或不再符合驗證之標準。

- 依據第 83 條處以罰金，依據個案之情況加上或以第 58 條第 2 項所定措施取代之。
- 暫時停止向位於第三國或國際組織之接收者傳輸資料。

**3. 許可權及諮詢權**

任何監督機關依據歐盟個資規則第 58 條第 3 項，行使下列許可及諮詢之職權（Genehmigungsbefugnisse und beratende Befugnisse）：

- 依據第 36 條之事前協商程序，提供資料管理者諮詢。
- 對於所有與個人資料保護相關之問題，自行或經詢問向各國國會、各會員國政府，或在符合各會員國法令之規定下，向其他機構及單位以及公眾提供意見。
- 核准依據第 36 條第 5 項之處理，當會員國之法令要求此種事前許可時。
- 提出意見，並批准依據第 40 條第 5 項擬定之行為準則草案。
- 依據第 43 條對驗證機關進行認證。
- 發給與第 42 條第 5 項相符之驗證，及批准對於驗證之評論。
- 依據第 28 條第 8 項及第 46 條第 2 項擬定資料保護之標準條款。
- 依據第 46 條第 3 項第 a 款許可契約條款。
- 依據第 46 條第 3 項第 b 款核准行政協約(Verwaltungsvereinbarung)。
- 依據第 47 條許可內部具拘束力之規範。

監督機關行使歐盟個資規則所賦予職權，應同時提供適當保障，包括有效

之一致性（歐盟個資規則第 58 條第 4 項）。所有會員國依據歐盟個資規則第 58 條第5項，得透過法令賦予其監督機關向司法機關舉發違反本規則行為之權限，同時進行或參與該司法程序，以落實歐盟個資規則之規定。

歐盟個資規則第 59 條課予監督機關應就其業務提交年度報告，其中包含舉發違規之清單及依據第 58 條第 2 項採行之相應措施。該報告除應轉知各會員國之國會、政府及其他依據各會員國法令所指定之機關外，亦應對公眾、執委會及歐盟個人資料保護歐盟個資委員會（Europäischer Datenschutzausschuss）公開。

### 第三款　監督機關間之合作與協調：歐盟個人資料保護委員會

歐盟個資規則要求各會員國應建立一或多個監督機關，而各會員國之監督機關間應如何共同合作，以確保齊一之個人資料保護水準，即有其重要性。為確保各監督機關在執行與適用歐盟個資規則的和諧，歐盟個資規則第 7 章中，就監督機關彼此之間之合作與協調機制予以明文規範（第 60-67 條），並於歐盟層級設立歐盟個人資料保護歐盟個資委員會（第 68-76 條），以確保歐盟個資規則於歐盟內適用之一致性，以下及針對歐盟個人資料保護歐盟個資委員會之組織及任務為簡要介紹。

#### 第一目 組織

歐盟個人資料保護委員會（下稱歐盟個資委員會）屬歐盟機構（Einrichtung）之一，具有獨立之法人格。歐盟個資委員會由各會員國監督機關之首長，[63]以及歐盟個人資料保護監察機構（Europäischer Datenschutzbeauftragte）之代表組成，[64]歐盟個資保護監察機構同時作為歐盟個資委員會之秘書處。歐盟個資委員會由

[63] 會員國若設有一個以上之監督機關負責監督歐盟個資規則訂定規範之施行時，則應協調該會員國之規範，任命一名共同之代表，作為歐盟個資委員會之組成員，歐盟個資規則第 68 條第 4 項參照。

[64] 歐盟個人資料保護監察機構作為歐盟之個人資料保護監督機關，其管轄範圍及於歐盟下之各個部門、機構，關於其設立、任命、任務及職權，則明定於歐盟第 45/2001 號規則中。針對歐盟各部門、機構、辦公室與事務所處理個人資料之行為，歐盟第 45/2001 號規則將優先於歐盟個資規則而適用（歐盟個資規則第 2 條第 3 項）；但歐盟個資規則第 98 條亦指出，歐盟第 45/2001 號規則之內容應由執委會再行檢視，以求與歐盟個資規則所揭示之標準具有一致性。

其主席代表之，主席由歐盟個資委員會成員中以相對多數選出一位主席，二位副主席，任期皆為 5 年；可連任一次。[65]主席除負責召開歐盟個資委員會會議及安排議程，確保歐盟個資委員會任務之即時執行外，並應通知最高監督機關及相關監督機關歐盟個資委員會作成之決議。[66]歐盟個資委員會之決議，原則上以取得組成員相對多數（einfache Mehrheit seiner Mitglieder）之支持行之。[67]執委會有權任命一名代表參與歐盟個資委員會，但無表決權，然而，歐盟個資委員會主席應告知執委會關於歐盟個資委員會之運作情況。[68]

歐盟個資委員會之運作模式，由其自訂議事規則（Geschäftsordnung）行之，該議事規則需有 3 分之 2 以上組成員之同意方得通過。當歐盟個資委員會認有必要時，得依據議事規則保密其討論內容。[69]

### 第二目 任務

為確保歐盟個資規則得獲得一致性之實施，歐盟個資規則第 70 條第 1 項針對歐盟個資委員會之任務為列舉之規定：歐盟個資委員會得自行或應執委會之請求行使職權，其中包括擬定相關細部規範、提供諮詢與意見、進行審查與認證以及推動與促進相關事務等，並要求其執行任務之相關資訊應予公開。

#### 1. 擬定相關細部規範

歐盟個資規則第 70 條第 1 項中賦予歐盟個資委員會擬定相關方針、建議及操作流程之義務，包括：

- 針對第 17 條第 2 項自一般公開之通訊服務中刪除個人資料之連結、影本或副本之程序，擬定方針（Leitlinien）、建議及操作流程（bewährte Verfahren）

[65] 歐盟個資規則第 73 條規定參照。
[66] 歐盟個資規則第 74 條第 1 項規定參照。
[67] 歐盟個資規則第 72 條規定參照。但依據歐盟個資規則第 68 條第 6 項規定：「在第 65 條所定情況下，歐盟個人資料保護監察人僅對於適用於歐盟機關、機構、辦公室及事務所之基本原則及規定，且其內容與本規則之基本原則及規定相符之決議中享有表決權。」
[68] 歐盟個資規則第 68 條第 5 項規定參照。
[69] 歐盟個資規則第 76 條第 1 項規定參照。

（第 d 款）；

- 依本項第 e 款擬定方針、建議及操作流程，以進一步規範依據第 22 條第 2 項與剖析相關決定作成之標準及條件（第 f 款）；

- 依本項第 e 款擬定方針、建議及操作流程，以確認個人資料保護之侵害以及確認第 33 條第 1 項及第 2 項所稱即時性（Unverzüglichkeit），以及資料管理者或受託者應通報個人資料外洩之特殊情況（第 g 款）；

- 依本項第 e 款擬定方針、建議及操作流程，規範個人資料保護之侵害可能會導致第 34 條第 1 項所稱對自然人之權利自由造成高度風險之情況（第 h 款），

- 依本項第 e 款擬定方針、建議及操作流程，就第 47 條對傳輸個人資料所定標準（Kriterien）及要求，其中包括對資料管理者或受託者具拘束力之內部個資保護規定，以及對當事人個人資料保護之其他必要要求，為進一步之規範（第 i 款）；

- 依本項第 e 款擬定方針、建議及操作流程，針對依據第 49 條第 1 項傳輸個人資料之標準及要求，為進一步規範（第 j 款），

- 制定關於監督機關依據第 58 條第 1 項、第 2 項及第 3 項所採行措施及依據第 83 條確認罰鍰的方針（第 k 款）；

- 依本項第 e 款擬定方針、建議及操作流程，以確認對於自然人依第 54 條第 2 項通報違反本規則之共同處理程序（第 m 款）；

- 明確規範第 43 條第 3 項所稱依據第 42 條對驗證單位進行之認證（第 p 款）；

**2. 提供諮詢與意見**

歐盟個資委員會亦於下列情況提供諮詢與意見：

- 提供歐盟執委會對於與歐盟個人資料保護相關疑義之諮詢，包括對於修訂歐盟個資規則的可能建議（第 b 款）；

- 提供歐盟執委會關於內部具拘束力之個資保護規範中，就資料管理者、受託者及監督機關間資訊交換之格式與程序之諮詢（第 c 款）；

- 針對於依據歐盟個資規則第 43 條第 8 項所定驗證要求（Zertifizierungsanforderung），向歐盟執委會提交意見（第 q 款）；

- 針對依據歐盟個資規則第 12 條第 7 項所定圖樣（Bildsymbol），向歐盟執委會提交意見（第 r 款）；

- 向歐盟執委會提交對於判斷第三國或國際組織所提供保護水準之意見，包括評斷該第三國、特定區域、該第三國或國際組織內之一或多個部門是否提供適當之保護水準。為達成上述目的，歐盟執委會應提供歐盟個資委員會所有其所需文件，其中包括與第三國政府、特定區域或特定部門或國際組織之文書往返（第 s 款）；

- 對於歐盟個資規則第 64 條第 1 項協調程序中監督機關所擬決議草稿，依據歐盟個資規則第 64 條第 2 項所提交事務，以及依據歐盟個資規則第 65 條制定具拘束力之決議，包括歐盟個資規則第 66 條所定情況，提交意見（第 t 款）；

- 對於依據歐盟個資規則第 40 條第 9 項於歐盟層級制定之行為準則，提交意見（第 x 款）；

另外，針對歐盟執委會請求歐盟個資委員會提供意見之情形，其得考量事態之急迫程度，訂定期限（歐盟個資規則第 70 條第 2 項）。

### 3. 監督：審查及認證

歐盟個資規則第 70 條第 1 項亦賦予歐盟個資委員會監督之權限：

- 監督及確保於歐盟個資規則第 64 條及第 65 條所稱情況，歐盟個資規則在不損及國內監督機關任務之前提下，正確地被適用（第 a 款）；
- 自主、應會員國之申請或執委會之請求進行審查，與歐盟個資規則施行相關之問題及制定之方針、建議及操作方法，以達成確保其一致性適用之目的（第 e 款）；
- 檢視歐盟個資規則第 70 條第 1 項第 e 款及第 f 款所稱方針、建議及操作流程之實務運作（第 l 款）；
- 依據歐盟個資規則第 43 條認證負責驗證之單位並對其進行經常性之審核，並對依據歐盟個資規則第 43 條第 6 項通過認證之單位以及依據歐盟個資規則第 42 條第 7 項於第三國認證許可之資料管理者或受託者實施公開登記（第 o 款）；

### 4. 推動與促進相關事務

歐盟個資委員會應推動與促進相關事務：

- 推動歐盟個資規則第 40 條行為準則之訂定及歐盟個資規則第 42 條資料保護專門驗證程序及資料保護標章及審查標章之建立（第 n 款）；
- 促進監督機關間之共同合作與資訊及操作流程之有效雙邊及多邊（bilateral und multilateral）交流（第 u 款）；
- 推動培訓計畫及支援監督機關間之人事調動，包括與第三國或國際組織之間（第 v 款）；
- 促進全世界資料保護監督機關在專業知識以及與資料保護規範及實務相關

檔卷之交流（第 w 款）；

**5. 資訊之公開**

歐盟個資委員會對於下列資訊，應予以公開：

- 監督機關之決議以及法院在協調程序中處理問題之電子目錄（歐盟個資規則第 70 條第 1 項第 y 款）。
- 歐盟個資委員會應將其所擬定之意見、方針、建議及操作方法，提供給歐盟執委會與第 93 條所稱委員會，且對外公開（歐盟個資規則第 70 條第 3 項）。
- 歐盟個資委員會就歐盟、第三國及國際組織處理個人資料之情形，應作成年度報告。同時應轉知歐洲議會、理事會及歐盟執委會。（歐盟個資規則第 71 條第 1 項）
- 與歐盟個資委員會成員、第三人代表及鑑定人相關之檔卷，其公開依歐盟第 1049/2001 號規則之規定行之（歐盟個資規則第 76 條第 2 項）。

## 第七項　救濟與處罰

歐盟個資規則於第 8 章（第 77 條至第 83 條）中，分別就救濟、責任及處罰予以規範。在救濟權利之部分，又分為「向監督機關申訴之權」（第 77 條）、「透過司法救濟對抗監督機關之權利」（第 78 條）以及「透過司法救濟對抗資料處理者或受託者之權利」（第 79 條）：

首先，歐盟個資規則保障所有當事人在無損其他行政或司法救濟途徑之情況下，若當事人認其個人資料之處理有違反歐盟個資規則之情形，皆得向監督機關提請申訴，該監督機關以設立於當事人之所在地、工作地或可能事發地之會員國所設立者為主（歐盟個資規則第 77 條第 1 項）。受理申訴之監督機關，應通知申訴人關於申訴之情況及結果，包括依據第 78 條提起司法救濟之可能性。（歐盟個資規則第 77 條第 2 項）

其次，歐盟個資規則第 78 條賦予所有人，在無損其他行政或非司法救濟途徑之情況下，對於監督機關之行為提請救濟之權利；其中第 2 項則針對當事人的司法救濟權利再次強調，並特別指出監督機關不作為之情形，包括監督機關怠於依據歐盟個資規則第 55 條及第 56 條處理申訴，或是當事人依據本規則第 77 條提出申訴，而在 3 個月內未接獲其處理狀態或結果通知之情形，明訂所有當事人皆享有主張有效司法救濟的權利，但其他行政或非司法之法律救濟不因此受影響。但上述規定僅課予監督機關於 3 個月內開始處理申訴案件之義務，對於申訴決定之作成，卻未訂有明確之時限。

最後，歐盟個資規則第 79 條賦予所有人皆得透過司法救濟對抗資料處理者或受託者之權利，一旦其主張依據歐盟個資規則所享有之權利，因與歐盟個資規則不合致之個人資料處理程序而致生損害。但該權利之行使並不影響其得採行之其他行政或非司法救濟途徑，包括第 77 條所定向監督機關提請申訴之權利。

歐盟個資規則為確保其規範得以落實，在歐盟個資規則第 83 條及第 84 條中，針對違反歐盟個資規則之行為，訂定了處罰與制裁之規定。對於違反規定者，最高得處以 2 千萬歐元或其年度國際總營收 4%之罰鍰，但其適用之對象僅限於設立在歐盟之企業；以及蒐集、處理及利用歐盟境內人民之個人資料，且其業務主要以歐盟為範圍之企業，而未針對自然人作為資料資料管理者違反行為之處罰予以規範，且亦欠缺處罰應遵循之程序。而針對未適用罰鍰者，歐盟個資規則要求各會員國訂定相關規範，擬定得以落實歐盟個資規則之必要措施，且其所採行之制裁，應「有效、合於比例並具有遏阻的效果」。[70]

[70] 就此，德國除一致認為應援用其既有之規定予以補充外，其亦針對歐盟個資保護規則之公布與施行，訂有因應與轉化歐盟個資法草案（Entwurf des Datenschutz-Anpassungs-und Umsetzungsgesetz EU，DSAnpUG-EU），目前預計制定聯邦一般個人資料保護法（Allgemeines Bundesdatenschutzgesetz，ABDSG），將歐盟個資規則第 84 條第 1 項之適用範圍擴及於與涉及違反個資保護企業有所關聯之自然人，例如：經營者、企業之個人資料保護監察人等，使其亦必須負擔罰鍰，但罰鍰額度有別於企業，將其上限限定於 30 萬歐元（聯邦一般個人資料保護法第 42 條第 1 項）。

# 第三章　日本個人資料保護法制介紹與分析

## 第一節　法制構造與特色

在討論本節之法律規定前，須先對日本「個人資訊」、「個人資料」之用語意涵有所了解，始能正確理解相關條文之規定。日本「個人資訊[1]」譯自「personal information」，自 1975 年社會黨提出「個人資訊保護基本法案」及「利用電子計算機處理個人資訊規制法[2]」時，即使用「個人資訊」一詞；之後前述 1988 年立法之「行政機關保有電子計算機處理個人資訊保護法」則仍沿用「個人資訊」一詞；而實務上法院判決亦使用「個人資訊[3]」一詞，故日本法律上、實務上一貫採用「個人資訊」之用語。而日本個人資訊保護法中尚有「個人デ-タ」一詞，而デ-タ一詞為英文「data」音譯，依法第 2 條第 6 項是指構成個人資料庫（data–base）之個人資訊；為忠於日本條文用詞，故本文將「個人情報」譯為「個人資訊」、「個人デ-タ」譯為「個人資料」，在此先予說明。

### 第一項　立法沿革

#### 第一款　1988 年～2005 年

日本最初個資保護法制之建立，除為因應資訊社會之快速發展外，主要之推動力為 1980 年 9 月經濟合作及開發組織（Organization for Economic Co-operation and Development，下稱 OECD）理事會決議通過有關個人資料保護及流通之八大準則[4]；為加盟國之一日本顧及經濟、社會發展上個資之傳遞與

---

[1] 日本將「information」翻譯成「情報」，故其「政府資訊公開法」亦為「政府情報公開法」。本文中為忠於日本立法之原意，將原文「情報」用詞均譯為「資訊」。

[2] 堀部政男，個人情報，プうイバシー保護の世界潮流と日本，法學セミナー404 號，頁 32。

[3] 如橫濱地院，平成元年（1989 年）5 月 23 日判決，判例タイムズ 700 號，1998 年 9 月，頁 144。東京高院，平成三年（1991 年）5 月 31 日判決，判例時報 1388 號，平成 3 年（1991 年）9 月，頁 22。

[4] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data；其宣示各加盟國處理個人資料時，最低限度應遵守之八大原則為：1、收集限制原則（Collection Limitation Principle）；2、資料內容原則（Data Quality Principle）；3、目的特定原則（Purpose Specification Principle）；4、利用限制原則（Use Limitation Principle）；5、安全保護原則（Security Safeguards Principle）；6、公開原則（Openness Principle）；

保護確有與國際接軌之必要性，為符合此八大準則之要求，於 1988 年先針對處理個資量較大之公部門，依據 OECD 八大原則，完成「行政機關保有電子計算機處理個人資訊保護法」（下簡稱：行政機關個資保護法）之立法並施行[5]。而民間部門則未立法規範，先由該當目的事業主管機關訂出該領域業者處理個資應遵循之指導原則（Guide-Line，下簡稱 GL），再由各業界以之為範本，訂出自律規範[6]。

前述行政機關個資保護法所規範者僅限於行政機關，受保護客體則為電子計算機所處理之個資，而未及於人工處理者。且對於保有個人資料檔案之事前通知及公告等，訂有大量且廣泛之例外事由；另對於錯誤資料之訂正請求權亦未予以明定，對資料當事人之保護顯不周全，備受學者批判[7]。之後，日本又陸續發生多起企業、銀行等洩漏、盜賣大量顧客資料事件，個資之保護成為社會關注問題[8]。其間日本政府準備立法建立居民基本戶籍網路系統[9]，為防止被民間業者不當利用，降低人民疑慮，當時執政黨乃於 1999 年 7 月邀集各相關單位，開始進行「個人資訊保護法（以下稱個資法）」之立法作業。

### 第二款　2005 年～2013 年

承上，立法之目的為將民間業者納入規範，並擴及適用範至人工處理之個資，於 2003 年 5 月由國會通過完成個資法立法[10]，2005 年 4 月全部施行。在完

---

7、個人參加原則（Individual Participation Principle）；8、責任原則（Accountability Principle）。

[5] 岡村久道，「個人情報保護法」，商事法務，平成 17 年（2005 年），頁 22。

[6] 例如 1987 年日本舊大藏省（現改稱財務省，相當於我國財政部）公佈金融事業者個資處理指針。1991 年舊郵政省（現改稱總務省，相當於我國交通部）公佈電信通信事業者個資處理指針。

[7] 佐藤幸治，「憲法」（3 版），青林書院，平成 9 年（1997 年），頁 445。田島泰彥、三宅弘編、「個人情報保護法」，明石書店，2003 年，頁 14。

[8] 高芝利仁，個人情報保護法施行に向けての意義と課題，ジュリスト No.1287，2005 年 4 月，頁 17。京王百貨店顧客名簿被竊事件，東京地方法院昭和 62 年（1987 年）9 月 30 日判決，判例時報（下稱判時）1250 號，頁 144。さくら銀行顧客資訊不當洩漏事件，東京地方法院平成 10 年（1998 年）7 月 7 日判決，判時 1683 號，頁 160。

[9] 日本稱為「住民基本台帳ネットワークシステム（簡稱住基ネット）」，為跨越市町村全國性規模之網路系統，將住民之姓名、生年月日及住民証字號等資料存檔上傳，供行政機關確認當事人之用。

[10] 平成 15 年（2003 年）5 月 30 日法律第 57 號。

成本法立法時，同步配合將上述「行政機關個資保護法」修訂為「行政機關保有個人資訊保護法[11]」，並新訂立「獨立行政法人等保有個人資訊保護法[12]」。

因近年資訊通信技術（ICT）快速進步，資料儲存、傳送巨量化、廉價化，人們運用自各處電子終端裝置或機器，如個人電腦、智慧型手機，監視攝影機、各種電子感應器等，大量蒐集個人行動履歷、網路上閱覽紀錄、位置資料（GPS）、乘車紀錄、購物紀錄、通訊紀錄、健康狀態等資料，並利用 Hadoop 開放式 source 軟體程式，將龐大數量資料分散於複數之機器或雲端作有效率之分析、處理之大數據（big一data）運算，已為世界潮流。各國政府均高度重視大數據之利用價值，期待能活用以提升國家產業競爭能力，進行有效率之行政管理、或預防災害，流行疾病之發生，擬定人口、交通等國家發展政策等；民間產業界則希望利用來更正確掌握市場需求、流行趨勢，以開發新產品或提供消費者新服務，達到產業之創新之目的。

**第三款　2013 年~**

在此趨勢下，亦以經濟再生為名之國家大計畫下，日本在內閣府成立 IT 統合戰略本部[13]，並於 2013 年 6 月 16 日發布「世界最先端 IT 國家創造宣言」，其中針對大數據中利用價值特別高之「パーソナル　データ（personal data）」[14]之活用，與個人資訊、隱私之保護間之兩立併存之可能性為目標，進行現行法修法研究，且特別成立「パーソナル　データ」檢討會，自 2013 年 9 月開始，由東京大學教授宇賀克也為座長，帶領由法律學者、律師、消費者代表、經濟界之領導人所組成之團隊，經歷一年共十二次之討論會議，研擬出「有関パー

[11] 平成 15 年（2003 年）5 月 30 日法律第 58 號。
[12] 平成 15 年（2003 年）5 月 30 日法律第 59 號。
[13] 正式名稱為「高速情報通信ネットワーク社会推進戦略本部」。
[14] 所謂「パーソナル　データ」，是自英文「personal data」音譯而來，而日本個資法中稱個資為「個人情報」，故用此一詞藉與自來使用之「個人情報」作區分。「パーソナル　データ」是指：有關個人資料全體之泛稱，不問其是否屬法所稱之個人，或是有關隱私之資料，個人之移動履歷、購買履歷、抑或已匿名化之資料，甚至統計資料，全包含在此概念內。參閱森亮二，実務解説，平成 27 年改正個人情報保護法，NBL NO.1059，2015 年 10 月 1 日，頁 5 之註 3。

ソナル　データ之活用制度修正大綱」，先確立以下四個修法方向：1、消除現行法個資定義不明之問題；2、促進個資活用與加強隱私之保護；3、建立因應全球化趨勢所需之個資法制；4、統一執行監督機關之設立。此大綱交由 IT 統合戰略本部再於 2014 年 12 月 19 日正式對外公布「個人情報保護法部分修正法案概要」。依此修正法案概要為藍本，正式進行修法作業，並擬出具體法條經日本內閣會議通過後，向國會正式提出法律修正案請求審議。再經過國會一連串之審議與答詢後，終於 2015 年 9 月 3 日決議通過法律修正案，完成個資法之修法。

新修正之法將分兩階段施行，關於個資法執行監督機關個人情報保護委員會（下稱保護委員會）先行組成，於 2016 年 1 月開始運作，先對新修個資法所必要之細則性規則進行訂定。而新修正條文之施行，因須由保護委員會定立如個人符號之指定、匿名加工資料之基準、申報、公告程序等規則後始能運作，故定於兩年內再開始施行。

### 第二項　法制之構造與特色

#### 第一款　立法方式與定位

日本個資法之第一章至第三章規定有關保護個資公部門與民間業者必須遵守之基本原則，一般稱為「基本法」；第四章至第六章則完全針對民間業者處理個資所定之通用原則，此部分被稱為「一般法」，定位為規範民間業者處理、利用個資之總則性規定；換言之，日本以一統一法典確立官民雙方處理個資之基本原則及國家基本政策，又於同法中再針對民間業者明定處理個資之總則性規範，而關於國家行政機關、獨立行政法人及地方自治團體之處理、利用個資則另立特別法以違規範，為獨樹一格之日本式立法[15]。

究其採如此立法方式之理由為：1、有關個資之保護，不問公部門或民間業

[15] 宇賀克也，「個人情報保護法の逐条解説」（4 版），2016 年，頁 18。岡村久道，同前註 5，頁 24-25。藤原靜雄，「逐条個人情報保護法」，弘文堂，平成 15 年（2003 年），頁 17-18。

者均應依 OECD 八大原則，在尊重個人人格之前提下為個資之處理、利用。因此個資法應先對個資保護之基本原則予以明白揭示；再者，為建構國家保護個資之法制度基盤，國家與地方自治團體有關個資保護之政策、實現方法及分擔之責任應有明確一貫之策略方向。2、公部門如行政機關因行政管理之需或為提供正確之行政服務，有效率執行行政事務，常依公權力在強制下或半強制下蒐集、儲存、利用大量個資，若有濫用個資或洩漏個資，將嚴重危害人民之權利、利益，甚至形成監視社會；又行政機關原對人民負有公開資訊讓行政過程透明化之義務，因此蒐集、利用個資之程序人民亦應有權參與、監督。故對行政機關處理、利用個資，應以特別法予以規範。3、相對而言，民間企業等多因事業活動之需，基於契約或準契約關係而蒐集、利用個資，原屬於私法自治之領域，性質上常為組織內部處理個資之問題，如對之予以過度干涉將涉及營業自由之問題，亦可能牴觸表現自由（例如傳播業、出版業等）；因此日本立法時首先以基本法確立公部門與民間業者處理個資之共同基本理念，再立於此基礎上，分別針對行政機關與民間業者訂立不同之規範[16]。

## 第二款　主務大臣制之轉換

### 第一目　修法前之主務大臣制

如上述民間業者因其包含各種不同事業領域，且蒐集、處理之個資性質亦差異甚大，難採如規範行政機關之統一立法方式；加諸如前述個資之利用、處理涉及業者之營業自由等，為避免給予業者過多限制，造成業者不必要負擔，降低個資之有用性，對民間業者之規範應以尊重各業者之自律、自主為原則[17]。故個資法之第四章以下對民間業者處理、利用個資，亦僅於必要最小限度內作總則性之規範，確立各業界處理、利用個資之共通最低標準[18]；細節部分再委

[16] 田島泰彦、三宅弘，同註 7，19 頁。宇賀克也，同前註，頁 18。
[17] 藤原靜雄，同前註 15，頁 18。見平成 16 年（2004 年）4 月 2 日內閣會議決議公佈之「個人情報の保護に関する基本方針」1、(2) ②。
[18] 田島泰彦，「個人情報保護法と人権」，明石書店，2002 年，頁 136。藤原靜雄，個人情報保

由各業界以此為基本框架，依其處理個資之性質及利用方法等，在各目的事業中央主管機關（下稱事業主管機關）輔導下，自主性訂出較高密度之自律規則（Guide Line，下稱 GL）。此係為防止同業間之業者等訂出寬嚴落差過大之規則造成混亂與困擾，故由對該當業界處理、利用個資之內容、方法之實際狀況最為熟知之事業主管機關，出面輔導協助業者共同訂出合理適用之規範[19]，應最為妥當。從而個資法第 8 條明定：國家為支援民間業者確保其適當處理個資，應訂立指導原則。另同法第 7 條第 2 項第 6 款及第 3 項亦規定：政府為綜合、一體的推進有關個資保護之施政，必須明定保護個資應採取之有關措施事項；由首相在聽取國民生活審議會相關意見後[20]，作成「基本方針」交由內閣會議通過並公佈之。依上開等規定，首相於 2004 年 4 月公佈基本方針，其 2、(3)之①即明示，各種事業主管機關針對該管業者，應依其事業領域之實際所需制定或修正有關其處理個資之指導原則即前述 GL，或對已自行訂立自律規則之事業團體等為資訊之提供及建議。同方針 6 更進一步對各事業中央主管機關制定 GL 時應包含之重要事項一一列明。據此各事業中央主管機關陸續訂出各領域業者處理個資之 GL，作為個資法適用、解釋之基準，以督促、指導民間業者合法適當處理、利用個資；在此運作模式下，至 2015 年 9 月日本各省廳合計共有二七個業種領域四十個 GL[21]被制定公佈，一般稱此為「主務大臣制」。

然因有關個資保護須具備專業技術與法律知識，而擔任主管之大臣卻未具如此專業，往往致使法之執行遲疑且效果不彰；另外現行個資法之主管機關為消費者廳，但法施行之監督機關則為各目的事業主管機關，各司其事，隨資訊通信技術進步，許多新興事業為橫跨數業界領域經營，形成須受複數主管機關之監督，不僅在監督上責任不清，更讓業者負擔過重。尤以主管機關不明確之

---

護法に関する制度の整備ーその成果と課題，ジュリスト No.1287，2005 年 1 月，頁 2。

[19] 宇賀克也，同前註 15，頁 56。

[20] 日本國民審議會為設置於內閣府之首相諮詢機關，主要為對一般消費者保護，國民生活安全之保護與提升等相關重要事項，進行調查、審議，並向首相提出報告。

[21] 個人情報保護委員會，網址：http://ww.ppc.go.jp/personal/legal/，2016 年 6 月 10 日造訪。

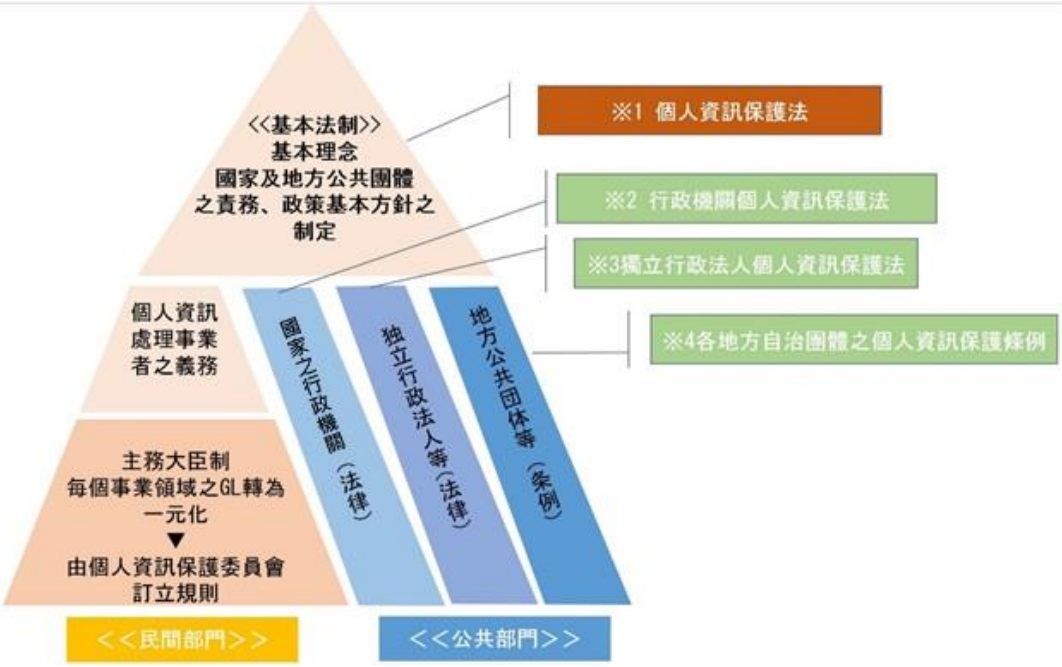
業者處理個資發生問題時，為確認主管機關，往往即耗時日，無法即時處理以阻止損害擴大。故而有必要修法建立一具有專業知識，且能橫跨機關、各業界一元化之監督個資法施行之體制[22]。

## 第二目　法施行、監督之一元化之修正

基於上開主務大臣制之缺失，此次修法即立法新設一專門且獨立於政府機關外之中立機關:「個人情報保護委員會（下稱保護委員會）」，對不問營利或非營利事業之全體民間事業，進行監督確保其遵守法令及定立適當之自律規範等，並統一法之解釋與適用。因此修法後第 7 條 1 規定：政府為綜合、一體的推進有關個資保護之施政，應明定保護個資保之基本方針。上開基本方針依第 61 條係由保護委員會定立後，依第 7 條第 3 項第 4 項規定，由內閣總理大臣送請內閣會議決議後，並予以公告。基此，保護委員會立於個資法中央主管機關之地位，原由各事業主務大臣各自定立之 GL，今後由保護委員會將之統一定出基本規則，在有必要時再考慮定立專門領域之個別 GL。如因規範專業領域之法律亦有關於個資處理之問題時，其 GL 之定立則由保護委員會提出意見，與該當事業主管機關共管之[23]。

有關個資法之全體法制構造以下以附圖一表示之：

[22] 宇賀克也，個人情報保護法改正について(1)，情報公開·個人情報保護，Vol.59，2015 年，頁 55。
[23] 日置巴美、板倉陽一郎，平成 27 年改正個人情報保護法のしくみ，商事法務，2015 年 12 月，頁 52~54。




此圖為參考日本消費者廳平成 26 年度說明會資料繪製

綜上，日本個資法制為自最上層個資法之基本理念，包含保護委員會定立之基本方針其次為民間業者應遵守之總則法與規範行政機關之個別法，而民間則由保護委員會定立之適用於各業界之規則或特別業種之 GL 之法制構造。

因本研究計畫受委託執行後，有關公務機關之行政機關個人資訊保護法及獨立行政法人等個人資訊情報保護法，於 2016 年 5 月 20 日，始經國會修正通過，故此部分不在本研究計畫範圍內，於此合先說明之。

## 第三款　特色

如前所述，個資法第一章至第三章為宣示包括規範公部門與民間業者處理、利用個資之基本理念、名詞定義、國家或地方自治團體有關個資法實行應有之責任及政策措施；第四章明定民間業者處理個資之總則性規範，為日本獨特折衷式之立法；本文依其構造及內容深入分析，同法實具有下列之特色：

### 第一目　基本法

在日本所謂基本法，為關於國家施政上佔有重要地位之制度、政策、理念，

明定其基本方針、原則、準則、大綱之法律；位階介於憲法與法律間，連結憲法與個別法之關係，具有具體化憲法理念之功能，用以補充憲法之完整性。因其常為揭示有關國家制度、政策之理念，基本方針及施政上應採之措施，內容通常為抽象性質之訓示或綱要性規定，對該當行政領域，提示施政之目標，及基本項目，並同時指示立法方向及法制之架構，而具有統合相關法律解釋、適用基準之機能[24]。按個資法於其第 3 條定明：個資應於尊重個人人格之理念下慎重處理，並必須謀求適當之處理方法及規範；揭示有關個資之保護及處理，均應遵循上述憲法理念建立法制予以規範。而所謂「尊重個人人格」，源自於憲法第 13 條之全體國民均為個人而應被尊重之理念;本法立法宗旨係為實現憲法上述理念，其為基本法之性質彰之甚明[25]。再查個資法第 1 條立法目的亦揭示：本法為確立有關適當處理個資之基本理念，及由政府制定基本方針及其他有關個資保護政策、措施之基本事項，揭示國家及地方自治團體對本法施行應負之職務，亦為本於其基本法之定位所作之宣示。更具體就個資法之構造而言，除前述第一章第 3 條為基本理念之規定外；接續之第二章章名為國家及地方自治團體之責任與義務，揭示國家及地方自治團體為確保個資被適當處理應有制定綜合性政策、建構法制及實施之義務；第三章章名為保護個資之策略與措施，明定內閣總理大臣應公告由保護委員會定立，並經內閣會議決議通過推動保護個資政策之基本方針等事項，國家應支援地方自治團體、國民或民間業者進行確保適當處理個資之活動；國家、地方自治團體應對民間業者與資訊當事人間因處理個資所發生之申訴事件，建置處理機制；地方自治團體或其設立之獨立行政法人保有個資之適當處理，應努力採取必要政策及措施等。對落實保護個資合法、適當處理之事宜，揭示國家及地方自治機關之具體政策、應採之措施，

[24] 參閱小早川光郎，行政政策過程と基本法，載於成田頼明先生退官記念，「国際化時代の行政と法」，良書普及会，1993 年，頁 59。日本類此之立法尚有教育基本法、土地基本法、環境基本法等，小野寺理，立法と調査，No.209，1999 年 1 月，揭載於參議院法制局 HP，http://houseikyoku.sangiin.go.jp/column/column023.htm。鈴木正朝，個人情報保護とコンプラインス•プログラム」，商事法務，2005 年，頁 16。

[25] 宇賀克也，同前註 15，頁 18。鈴木正朝，同前註，頁 17。藤原靜雄，個人情報保護制度の課題について，季報情報公開・個人情報保護，Vol.30，2008 年 9 月，頁 4。

均充分反映其基本法之特質。

## 第二目　總則法

本法第四章（第 15 條至第 39 條）包括第一節將 OECD 八大原則具體濃縮轉化為民間業者處理個資時應遵守之義務規定，及當事人請求公開、訂正、停止利用時，處理個資業者之對應處理方法，第二節匿名加工資料處理業者等之義務，第三節為保護委員會執行檢查、監督處理個資業者等權限之方法，及第四節依民間團體推動個人資料保護規定，包含認證個人情報保護團體取得認證之等資格、要件及其對團體成員之輔導等。而第五章則為監督民間業者適當處理、利用個人情報之第三人獨立機關「個人情報保護委員會」之設置方法、任務、職權及組織等規定。第六章雜則，規定法之適用範圍等。第七章主要為規定民間業者違反本法之罰則。

依本法第 76 條第 1 項規定，本法適用範圍除新聞、傳播媒體事業、著述業、宗教團體等為報導、著述、宗教活動等特定目的時得不受第四章適用外（本文將另行討論），包含所有業界領域之業者在內；而保護之客體則為得以識別生存之特定個人資訊；故而就本法第四章規定而言，為不問處理個人情報之業種、處理個資種類性質，一律納入規範對象，並揭示業者處理個資時所應遵守最低限度之義務；就本法性質上，為全體處理個資民間業者所應遵守之總則性規範，故其具有總則法之特質。

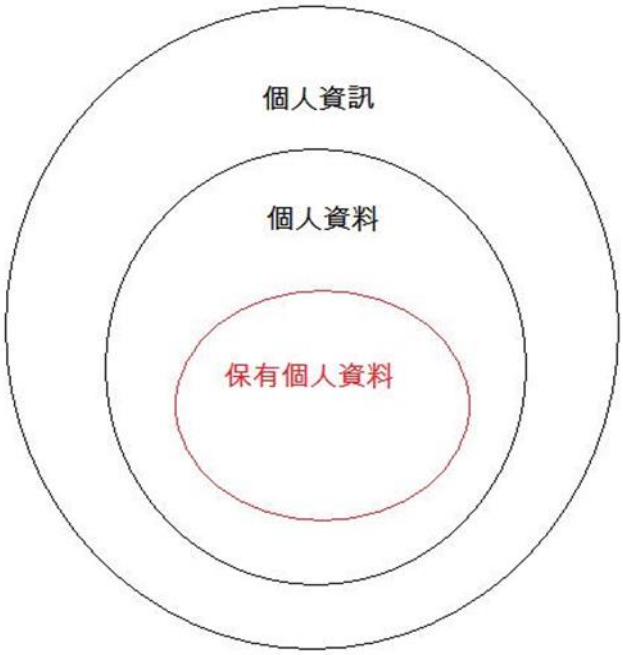
## 第二節　保護之客體

日本個資法，將其保護之個人資訊，依其保護之必要性或業者義務履行之可能性，分為以下三種範圍：涵蓋面最廣之個人資訊、其次為構成個人資訊資料庫（data-base）中之個人資料（data）、涵蓋面最小之業者「保有個人資料」，其關係圖如下（附圖二）。據此，個人資訊為最廣泛之概念，而個人資料則為包含在個人資訊範圍內，構成個人資訊之基本元素，個人資料與保有個人資料之

區分，係著眼於業者對該當資料有無公開或訂正之權限與保有處理期間之長短。

又日本此次修法主要之項目之一，即針對以下個資法關於「個資」定義及範圍，被指摘不明確而存在有灰色地帶（grace zoom）部分，進行更周詳立法，以解決問題並建構更有利於活用個資之法制基盤[26]。

附圖二：參照岡村久道，個人情報保護法，頁 60 之圖(2009 年版)




## 第一項　個人資訊之定義與檢討

### 第一款　個人資訊之定義

依現行個資法第 2 條第 1 項規定為：有關生存個人資訊，依包含於其中之姓名、生年月日及其他記述等，而得以識別特定個人者（包含藉由有容易組合、比對性之其他資訊，而形成得識別特定個人者。）。基此，一般學者均將個資概

[26] 森亮二，同前註 14，2015 年 10 月 1 日，頁 5 之註 3。宍戸常寿，個人情報保護法制，特集憲法の現況，Quarterly Jurist/2015spring/Number13，頁 39。

念解為：包含自然人有關聯之個人屬性、行動、評價、個人創作表現等資訊，不問其是否已為眾所周知；且該資訊存在形式並不限於文字，尚包含聲音、指紋、肖像等;亦不問該個人是否為本國人,公眾人物、公務員均屬此所稱個人[27]。

## 第二款　特定個人識別性

因個資法立法目的在保障個人對自己資訊自主權，避免被他人濫行蒐集、利用而致其權利、利益受損，若該當資訊無法辨識為某特定個人之資訊時，其被蒐集、處理或利用不致使當事人受損，即無保護之必要。故受個資法保護個資，尚須具有「特定個人識別性」者始足當之，特定個人識別性為個資該當性之要件，資料是否受個資法保護之分水嶺[28]。而個資法立法當時即考量，世上完全不涉及任何個人之資訊恐不存在，為避免個資保護範圍無限擴張，特意設置此一要件[29]。而所謂「特定個人識別性」係指自該當資訊包含之內容，依社會一般人之判斷或理解力，得認定生存之特定個人與該當資訊間之同一性，最典型即為姓名及顏面相貌，一般人依此單一資訊內容即可與其他人區分而直接識別出特定個人，除此之外，如該當資訊中因包含有身分證編號、住所、生年月日、職業、性別等記述，經組合、比對後，一般人亦得識別出特定個人時，亦為具有特定個人識別性之個資，至於該當個人具體姓名知悉與否，並非判斷有無特定個人識別性所必要者。在此所謂特定個人識別性係以一般人為基準以進行判斷[30],因直接特定個人識別性之判斷,不應被容許有相對化之問題存在，以避免主觀介入造成法適用之不安定性。

然另有一類型資訊，即單依該資訊本身無法識別出特定個人，但如得有其他資訊進行組合、比對後,得識別出特定個人者,此稱為具有間接識別性個資。

---

[27] 宇賀克也，個人情報保護法の逐条解説（第三版），有斐閣，2009 年 4 月，頁 32。藤原靜雄，同前註 15，頁 25。

[28] 岡村久道，ビッグデータの法的処理―個人識別性と非識別化の問題を中心に，法とコンピュータ学会研究会報告 no32，2014 年 7 月，頁 4。

[29] 園部逸夫編集，個人情報保護法の解説，ぎょうせい，平成 15 年 9 月，頁 49。

[30] 日置巴美、板倉陽一郎，同前註 23，頁 90-91。鈴木正朝，同前註 24，頁 91-92。

此時得與其為組合、比對資訊之範圍亦不能毫無限制，否則個資範圍又將無限制擴張，故日本於個資法立法時設置「容易得有他資料與之為組合、比對」為要件，一般此稱為「組合、比對容易性」[31]要件。乃指該當個資處理業者無須進行特別調查、運用特別軟體程式，或花費龐大費用、手續，即能獲該當個人其他資訊以為組合、比對，進得識別出特定個人[32]。典型之例為單一之電話號碼、信用卡號、IC 卡號、車牌號碼等，表彰特定個人之屬性或其所有物、行動事實等之資訊[33]。然如此立法因下列之問題而在解釋上、運用上留下曖昧模糊之空間，形成前所述之灰色地帶。

## 第三款　問題

### 第一目　「特定個人識別性」判斷之相對化

本條項之規定中並未明定間接特定個人識別性之有無係立於何人之立場為基準進行判斷？亦即該當個資是否容易得有其他資訊進行組合、比對，應以何人為對象進行判斷？係採依蒐集、處理個資者為基準之「個資處理者基準說」，或依一般大眾為判斷對象之「一般人基準說」？事實上因每個個人、各類業者，擁有之技術、所處理資訊之性質，及其與該當資訊當事人之親疏關係、獲得其他資訊能力均有不同，對特定個人識別能力原即有高低、難易之相對化特性[34]。造成間接識別性個資判斷上難以建立統一基準。而對此一問題，日本之學者[35]及實務[36]，則採個資處理業者基準說，如若將此類型個資提供給他人時，依同理採提供人基準說（即原個資處理業者），亦即仍以原蒐集、處理個資之業者為判斷對象；換言之，該當個資是否容易得有其他資訊為比對組合而具有間接識別

[31] 岡村久道，個人情報保護法（新訂版），2009 年 2 月，頁 43。
[32] 園部逸夫編，同前註 29，頁 73。
[33] 岡村久道，同前註 31，頁 73。
[34] 宍戸常寿，同前註 26，頁 39。岡村久道，同前註 28，頁 5。
[35] 新保史生，パーソナルデータの利活用を促進するための枠組みの導入等，自由と正義，65 巻，12 号，2014 年，頁 20。岡村久道，同前註 31，頁 76。森亮二，パーソナルデータの匿名化をめぐる議論，ジュリスト，March 2014/No.1464，頁 26。
[36] 參閱平成 16 年厚生勞動省、經濟產業省告示第 41 號「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」。

性，係依原蒐集、處理個資業者所具備之條件、技術處理狀況作基準進行判斷，於是因各業者事業規模不同、處理個資性質各異，資訊技術能力有高低差異，間接識別性判斷仍無可避免存有相對化之問題[37]。然因此係較能保護當事人權利之判斷基準，立於蒐集、處理個資人之條件、背景，只要該當資訊符合容易比對、組合之要件，即為具有間接識別性之個資，則其蒐集、處理須受個資法之規範；且此一基準亦可防止搜集處理個資業者，以分割、分次提供同一人個資之方式，規避法之規範，自屬較有利於當事人之保護。

### 第二目　特定個人識別性判斷之流動化

因資訊科技之進步，利用搜尋引擎（search engine）蒐集資訊越發便捷，原無識別可能之資訊，隨科技進步，轉成為容易獲得其他資訊以為組合、比對，而為具有特定個人識別性；另一方面近年民眾對自己個資保護意識提高，要求應受保護之個資範圍越發擴大，然因特定個人識別性之判斷涉及技術層面、主觀意識，原難以確立全面一致性之判斷基準，又與個人期待難免存有落差，造成個資保護範圍落實在立法上與人民理想上之期待未能一致[38]。

因如上「特定個人識別性」判斷基準之「相對化」與「流動化」，致使被保護個資範圍不明確，業者在蒐集、利用個資時因存有不可預測之風險，而有所顧慮或保留，降低個資得被合理利用之價值。

### 第三目　數位化符號個資之利用

如前所述，因資訊科技大量運用，利用電腦終端裝置 或感應器材蒐集儲存個人「以符號或電子紀錄顯示」之生活履歷（life log）、上網紀錄、位置資訊等業者非常普遍，此類資訊為單一符號時雖有「個人」識別性，卻未有「特定」個人識別性，本身原無法特定當事人為何人，但如被大量蒐集儲存後，再透過

[37] 岡村久道，同前註 31，頁 5。
[38] 岡村久道，同前註 31，頁 4。久保田正志，パーソナルデータの利活用と個人情報保護法改正，法と調査，No360，2015 年 1 月，頁 8。

電腦網路與其他資料庫資訊組合比對，可能分析出該當個人之生活習慣、嗜好，甚至財務狀況及信用度，亦可能因此識別出特定個人，造成其權利利益受損，故此種個人識別之符號，是否應視為個資而受到保護，為本次修法檢討個資保護範圍時檢討之重要課題[39]。

## 第四目　匿名加工資料新設之必要

如前所述個資法保護之個資須具備「特定個人識別性」，且依同法第 16 條第 1 項規定，如欲將蒐集、處理之個資為特定目的外之利用，原則上事先應得到當事人之同意，又或為原特定目的外將個資提供給第三人時，依同法第 23 條第 1 項規定，原則上亦應事先得當事人同意。然現今，各種事業往往運用資訊技術大量蒐集、儲存個資並建置為資料庫，如欲藉大數據運算分析在蒐集時原特定目的外，活用於產業創新、市場分析、流行疾病預測上等時，在現行個資法規範下須面臨下列問題：1、因屬目的外利用，依法須得到數以千萬計之當事人個別同意，對業者而言其成本、時間上負擔將過於沉重。2、如將蒐集所得個資予以加工匿名等使之除去個人識別性後，因該資訊已不具特定個人識別性非屬個資，而得不受個資法規範再予利用（包括提供給第三人），確實為一可考慮之方式；然現因電腦搜尋引擎網站之廣泛運用，資料之蒐集組合、比對，容易且便捷，所謂去個人識別性之「匿名化」，究竟應要求至如何之程度始得謂為完全無識別之可能？又匿名化之程序、及業者應遵守之義務及其監督機制等，現行法上均未確立。鑒於 JR 東日本 suica 事件之發生[40]，則已顯示一般民眾對

[39] 宇賀克也，同前註 22，頁 57。總務省「パーソナルデータの利用、流通に関する研究会報告書」，2013 年 6 月。

[40] Japan Railway 東日本公司，其發行販賣類似我國悠遊卡之電子乘車票證，稱之「suica」卡，被發現將約 4300 萬乘客之 suica 上錄存之乘降履歷資料，包括上下車站名、乘車日時、車資、生年月日、性別及卡號，於隱匿姓名、聯絡地址替代以其他代碼後，提供給第三人「日立製作所」，作統計、分析，後並將其結果作為市場、行銷資料（marketing information），再提供車站周邊之事業者利用。JR 東日本公司於事先未對 suica 之持有人說明此事，其提供之乘降履歷則是以秒為單位，歷經 2 年半之時間所蒐集之同一 ID 之資料。事發後，JR 東日本公司辯稱其所提供之個資，為已隱匿持卡人姓名、聯絡地址之乘降履歷資料，因無特定個人識別性而非個資法所保護之個資。但許多持卡人仍覺得自己個資未經同意被出賣給第三人利用而覺得不安，紛紛提出抗議，輿論界亦一片撻伐之聲。結果在同年 9 月 20 日 JR 東日本公司在社會壓力下決定

事先未經其同意，號稱已「匿名化」個資之提供給第三人利用，心存極大疑慮與不安，而引發社會爭議，亦造成業者對利用大數據有所猶豫與顧慮。從而明確匿名化個資之定義、要件及整備利用上應遵守之義務規範，亦為日本此次修法之重點之一[41]。

綜上，為消除上開現行個資法第 2 條第 1 項不明確之定義規定，所造成灰色地帶，建構大數據時代下更能合法活用個資之法制基盤，日本於本次修法中修正第 2 條第 1 項，並於同條新增第 9 項對加工匿名個資予以定義，再於第 36 條、37 條、38 條，確立匿名加工資料作成、利用時應遵守之義務。

## 第二項　修法後個資範圍之再確認

以下就日本於 2015 年 9 月修正通過之個資法，有關個資定義部分之修正介紹如下：

### 第一款　定義及範圍

依法第 2 條第 1 項，本法所稱「個人資訊」為該當於以下各號所揭示之一有關生存個人之資訊。

一、藉由包含於該當資訊中之姓名、生、年、月、日及其他記述（被記載或記載於文書、圖畫或電磁紀錄（使用電磁方式（電子方式、磁氣方式及其他依人之知覺無法辨識之方式）所作成之紀錄。第 18 條第 2 項亦同）上，或使用聲音、動作及其他方法所表示之一切事項（個人識別符號，除外）以下同。）而得以識別特定個人者（包含與其他資訊容易為組合、比對，因而得識別特定個人者）。

二、個人識別符號所包含者。

---

停止對外販賣系爭資料，並對已被蒐集乘降履歷當事人，採取 opt-out 制（得選擇退出個資被利用）。

[41] 久保田正志，同前註 38，頁 6。宇賀克也，個人情報保護法改正案について(2)，季報情報公開・個人情報保護，Vol.58，2015 年，頁 39、58。

第 2 項，本法所稱「個人識別符號」為，該當於以下各號之一之文字、編號、記號、其他符號，而依政令所指定者。

一、特定個人之身體一部分特徵為供電子計算機使用而變換之文字、編號、記號、其他符號，而得識別該當特定個人者。

二、對提供個人勞務或對個人購入其所販賣商品上分配或發給之卡片及其他書類上，記載或依電磁方式所記錄之文字、編號、記號、其他符號，其係依每個利用人或購買人或受發給人為不重覆之分配、記載或記錄，而藉之得以識別特定利用人或購買人或受發給人者。

上該規定事實上與現行法規定差異不大，僅加上個人識別符號之新類型個資規定，個資仍須具有特定個人識別性。

**第一目　個資範圍及類型**

依上開規定個資範圍及類型得分析如下：

1、個資之類型化：

如前述以電腦連線終端裝置或各種感應裝置所蒐集、儲存之個資，如係在同一 ID 號碼下大量儲存同一人網路閱覽履歷、手機下載應用軟體紀錄、位置資料之生活履歷資料，因為大量長期被蒐集累積者，再經電腦網路連線搜尋各網頁資料進行比對、組合後，仍有辨識出特定個人之可能，故此類型個資，實有納入個資法保護之必要。又為消除現行法定義不完全及因特定個人識別性「相對化」、「流動化」所產生之灰色地帶，本次修法於第 2 條第 1 項將個資分為二類型分別予以定義。第一類:記述型個資，依其第 1 款為包含姓名、生年月日、其它記述等以文書、圖畫、電子等方式記錄之得以識別特定個人之記述型資料，基本上與現行法第 2 條第 1 項定義與要件差異不大。第二類:個人識別符號型個資，依增訂之第 2 款，藉由個人「識別符號」而得識別特定個人者，亦屬個資。

所謂個人識別符號則又得分為兩類，(1)：為供電子計算機利用而將個人身體一部分特徵所變換成之符號、編碼、記號等，而得藉之識別該當特定當事人者，例如數位化之指紋資料或顏面特徵辨識資料。(2)：提供給個人利用之服務或販賣給個人商品上所分配、或發給個人之卡片、其他書類上，所記載或依電子方式記錄之文字、編號、記號，而用以識別特定利用人、購買人或持卡人者；例如護照號碼、身分編號、保險證號碼等，上開兩類型個資若依政令而被指定為「個人符號」者即屬個資法保護之個資。換言之，上開「個人識別符號」單其本身即被認定為個資，無須考量其是否具備「比對、組合容易性」。依提案修法政府機關之說明，如此修法與現行法比較下，並未變更或擴大個資之範圍，單只是將個資之定義及範圍予以更明確化[42]。

2、個人識別符號之指定：

應注意者為政府依政令指定個人識別符號時，並非得任意為之，而須依一定之判斷基準為之；判斷基準定立考量之重點在於該當個資係被反覆、大量蒐集或分屬各種資料庫而被各領域業者間共用者，具有識別出特定個人之高蓋然率[43]，致使該當個人權利、利益受損，立於事先預防損害發生之觀點有必要指定者。又因個人識別符號之運用涉及技術層面，故個資檢討會（パーソナルデータ検討会）委由所設置之技術工作小組（ウォーキンググループ　working group），依其電腦資訊專業知識及技術深入檢討及研究後，於其報告書中提出以下 4 個指定個人識別符號之判斷基準[44]：(1) 到達性：即該當符號與當事人或其所有物之間有密切關連性，基於此符號編號等即可直接到達至(approach)當事人，亦有稱此為「當事人到達性」。如：當事人與生俱來或後天形成之顏面

[42] 參閱眾議院內閣委員會 4 号，平成 27 年（2016 年）5 月 8 日，山口國務大臣，在答覆質詢時之說明。
[43] 宇賀克也，同前註 22，頁 51。
[44] 森亮二，同前註 35，頁 43。參酌技術檢討ウォーキンググループ報告書，「(仮称) 準個人情報」及び 「(仮称) 個人特定性低減データ」に関する 技術的観点からの考察について」，平成 26 年 5 月。

特徵資訊、手掌靜脈數、聲紋、筆跡、舉止行走之特徵或當事人社會生活中被配賦之編號、符號，如身分證字號、護照編號、健康保險卡號碼、駕照執照號碼等，均可直接連結至當事人。（2）一意性：或稱為「唯一無二性」，亦即該當識別符號具有一對一之特性，對同一對象不為重覆配賦之獨有識別因子，如不同對象有可能配賦相同識別因子之符號或編號即不屬之。例如指紋資料國民身分證編號即屬之，而身高、血型資料等即不具此特性。（3）不變性：即被配賦之編號或符號等，不因當事人之意思有頻繁、任意變更之可能。（4）共用性：亦即為識別因子之符號、編號等，係被複數之業者、提供服務之機關、團體間所共用，或跨越數個不同領域被利用，而得產生特定個人識別性者[45]。在國會審議本項時，並未討論及（4）之判斷基準[46]。其原因可能是工作小組當時是以擴充個資範圍為前提，而考量判斷基準之定立，並未以明確化個資概念為主要之目標，且未遭受外界壓力下，提出上開 4 個基準，然至報告書提出給政府並公諸於世後，即遭受民間業者之強力反對，批評如此修法會擴大個資範圍而限制個資之利用範圍。故在國會審議草案時，主管修法之大臣轉向強調此次修法是不變個資範圍，僅更明確化其定義[47]，對（4）之基準避而未進行說明，之後學者在討論時，亦未再提及[48]，此部分今後之發展仍須注意。

## 第二目　檢討

事實上，日本在開始研議修法時，基於 2013 年 6 月內閣會議決議之「世界最先端 IT 國家創造宣言」，係將建置大數據時代得安心合法活用個資之法制環

[45] 関啓一郎，個人情報保護法とその 10 年ぶりの改正について，知的資產創造，2015 年 10 月号，頁 10-11。森亮二，個人情報の保護と利用，法律時報 88 卷一号，2016 年 1 月，頁 82。宇賀克也，同前註 22，頁 51。

[46] 參同前註 42，山口國務大臣之說明。

[47] 宍戸常寿，同前註 26，頁 39-40，對修法過程之轉折有說明。參閱森亮二，實務解說平成 27 年改正個人情報保護法，第 2 回，NBL，No.1601，頁 43，及其註 6 之說明。宇賀克也、大谷和子、寺田眞治、長田三紀、向井治紀、森亮二，座談会，個人情報保護法・マイナンバー法改正の意義と課題，ジュリスト，No.1489，2016 年 2 月，頁 16，森亮二之發言。

[48] 如宇賀克也，個人情報匿名加工情報，個人情報取扱事業者，同前註，ジュリスト，No.1489，頁 37。

境，以有利於產業創新、活化經濟等，作為國家發展目標之一，此於修法後之第 1 條目的的規定[49]，亦得窺知。而個資檢討會及其下設置之工作小組在討論個資定義時，原先朝向擴張其範圍方向檢討，於 2014 年 5 月提出報告書中將為未能識別「特定」個人，因被大量或多方蒐集下而產生識別特定個人之虞之資訊，稱作「準個人資訊」，建議納入法保護範圍內。後報告書中同時提出前述 4 個判斷基準，除將前述之身體特徵顏面識別資訊等列入「準個人資訊」外，個人手機之端末、個人電腦端末 ID 等，亦被納入[50]。而再經檢討會繼續討論之結果，因所謂「準個人資訊」被批評概念不明確[51]，且有關應被保護之範圍為何？各方見解始終無法取得共識，最終於 2014 年 6 月 IT 總合戰略本部提出之「個人資訊利活用制度修正大綱」，終究未將「準個人資訊」之概念納入。

為何修法過程會有如此轉折，事實上是因為日本修正個資法時，一方面參考歐盟一般資料保護規則[52]4 條（1）之規定已將個人識別符號、位置資訊、線上識別元素等納入為個資之新規定，一方面須顧慮國內 IT 產業希望放寬規制之意見，加上有來自民間消費者要求提升個資保護之聲浪，在此議題激烈論戰中，很難面面顧全，個資保護與活用兩相顧全之政策實現有高度之困難度[53]。此外自現實面考量，因資訊科技日新月異，新興產業、服務業不斷登場，新的識別個人符號於可預見之將來，亦將推陳出新，單以前述工作小組所提議之四項基準進行判斷，是否仍有未盡之處？甚或因事前作過度規範，而對產業創新造成不利之影響[54]。故現階段修法僅先將已經普及被社會利用之個人識別符號，由

[49] 第一條目的規定為：有鑑於伴隨高度資訊通信社會之進展下，個人資料之利用明顯擴大，本法以關於個人資料適當處理，定出其基本理念及政府基本方針作成、其他關於個人資料得保護施政之基本事項，明示國家及地方自治團體之責任之同時，並藉由規定處理個人資料事業者應遵守之義務，在考量個人資料之適當且有效活用，有助於產業創新及活力化社會經濟並實現豐裕國民生活，及其他個人資料之有用性下，並保護個人之權利利益，為立法之目的。

[50] 此段經過得參酌宇賀克也，パーソナルデータの利活用に関する制度改正大綱について，季報情報公開・個人情報保護，Vol.55，頁 66-67。

[51] 新保史生，同前註 35，頁 20。

[52] General Data Protection Regulation（GDPR），（Regulation（EU）2016/679）。

[53] 宍戸常寿，同前註 26，頁 36。

[54] 同前註 47，座談會，頁 17，寺田真治之發言。

政府機關與各產業、經濟界協議後，再依政令指定納入個資保護範圍。

在現時點依政令被明確指定為「個人識別符號」者有：個人編號（マイナンバー，類似我國之身分證字號）、駕駛執照號碼、護照號碼、基礎年金號碼、保險證號碼。另一方面，單只是以機器賦以編號之手機通信端末 ID，則不被認定為個人識別符號；而手機電話號碼、信用卡卡號、電子郵箱號碼（e-mail address）、及為提供服務之會員證號碼，亦不被認定為個人識別符號[55]。對此論者間有不同之見解；批評派，認為國會對判斷基準（4）未作詳細討論，且端末 ID 雖為機器所分配之符號識別，如該機器與其所有人關係緊密相連時，實質上應被視為有特定個人識別性；又自「法的安定性」觀點來看，委由政令在「判斷基準」未十分明確下，指定「個人識別符號」似有未妥[56]。另有主張依據情報通信網路產業協會之「2015 年手機利用實態調查」結果顯示，手機使用 2 年以上未變動電話號碼之用戶中智慧型手機約占 90％，而手機持有人日常生活行動之各種個資多已被儲存在手機中，卻未納入個資被保護似有疑義[57]。贊成派論者則主張:手機及電話號碼有許多情形是工作單位供用且員工輪流持有使用，與當事人之關聯性薄弱;再實際上許多機器端末設有讓利用人得任意變更帳號、密碼之方法，例如金融提款卡密碼、電子郵箱號碼等，故而未具有不變性，似乎無須納入個資保護範圍內。更何況本次修法將現行法原未納入規範對象之中小企業全包含進來[58]，如將手機電話號碼等亦納入為個資，將會使中小企業增加負擔，故目前仍不宜將之指定為個人識別符號[59]。

綜上，一般而言，日本此次修法，有關特定個人識別性之要件並未作任何更動，仍維持與現行法相同，不問是敘述類型還是識別符號型個資，仍以有「特

[55] 請參閱眾議院內閣委員會 4 号，向井治紀政府參考人對質詢之答覆，平成 27 年 5 月 8 日。
[56] 森亮二，同前註 45，頁 82-83，同作者，同前註 47，頁 43-44。
[57] 同前註 46，座談會記錄，頁 17，長田真治之發言。
[58] 日本現行法第 2 條第 3 項規定,「以個人資料庫等供事業者之用者,如其所處理之個資數量，在過去 6 個月內之任何一天均未超過五千人之個資者」，不受本法規範。
[59] 同前註 47，座談會記錄，頁 16，大谷和子之發言。

定個人識別性」為要件。而個人識別符號，則除須有特定個人識別性外，尚須屬政令所指定者，自目前被指定為個人識別符號之個資觀之，實多為在社會上已有共識被認定應為個資所保護者，因此修正後「個資」之範圍，正如政府官員於國會所言並未擴大，僅將其範圍更「明確化」而已，有學者稱此乃為本次修法之特徵[60]。

## 第二款　匿名加工資料

### 第一目　構想與設計

此亦為本次修法重點之一，被認為是促進大數據利用之重要催化劑[61]。基本之出發點即在解除業者依現行法第 16 條第 1 項及第 23 條第 1 項規定，對個資之利用須受原特定目的之限制、對第三人提供時，原則上亦應得到當事人同意之義務。能將蒐集所得大量個資依大數據運算、分析之結果，用於原定目的外或提供給第三人以創新產業、開發新藥、預知市場趨勢等，而在法律上建置得活用大數據之基盤[62]。然另一方面亦為消除消費者對匿名個資被業者利用之不信任與權利受損之疑慮，日本本次修法特別增設一新類型之「匿名加工資訊」之規定，亦即將個資予以加工處理去除「特定個人識別性」，成為無法識別「特定」個人之資訊，並免除其為原特定目的外第二次利用、或提供第三人時須得到當事人同意之義務。

而在此部分修法之過程中，原係參考美國聯邦交易委員會（Federal Trade commission，FTC），於 2013 年公布之報告書中所提出有關網路上消費者個資匿名化之建議（idea）[63]，日本一般稱此為 FTC 三原則[64]，亦即如果業者滿足 1、

---

[60] 宍戸常寿，同前註 26，頁 40。
[61] 小林慎太郎，「匿名加工情報」によるビッグデータビジネス活性化への期待と課題，知的資產創造，2015 年 10 月号，頁 31。
[62] 宇賀克也，同前註 41，頁 39。
[63] Protecting consumer privacy in an Era of Rapid Change：Recommendations For Businesses and Policymakers, *available at* https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers (last visited: May. 30,2015).

已對該當資料採取適當去個人識別性措施；2、對社會大眾公開聲明，該已去個人識別性資訊，不再回復其識別性；3、將該去個人識別性資訊提供給第三人時，以契約禁止受提供之第三人進行回復其識別性，三要件時，即得認定該當資訊已喪失與特定個人之合理關連性，而為匿名化之個資。

復經研究會再三討論之結果，認為：1、之匿名化措施，在現實適用上，因各種事業蒐集、處理或利用之個資性質、種類均有不同，所謂「去個人識別性」之方法，及究竟至何種程度始得稱為安全？恐須依個案判斷，且在資訊科技不斷進步下，沒有任何一去特定個人識別性方法得稱為完全安全（即永遠絕無人得回復其識別性），亦無法以立法之方式具體訂出得泛用於各企業之去個人識別性措施。2、之不再回復識別性之宣示，在美國如企業之後有違反者，得依 FTC 法第 5 條予以制裁[65]；而相對在日本並無類似之制度，則此要件即無任何法律之實效性。3、之由提供人與受提供人間以契約約定禁止受提供人回復個人識別性，在日本能否期待提供人自發性訂立如此契約實有疑慮，故似以「法定義務」替代「契約義務」較為可行[66]。基於上開理由，日本最終未採納 FTC 三原則，而自技術面及法制面考量，將兩者組合朝向自己創設規範方式進行修法[67]。

按匿名加工資料是立於為顧全個人權益之保護及個資能被合理利用而設計者，但因各業者所處理之個資種類、性質及利用方法差異性甚大，加之匿名化之程度自完全無法回復原狀至加入新資訊即有復原可能者，其間幅度相當大；一般而言內容越詳細之個資，其有用性越高但相對的其被復原之可能性亦越高，在此二者間如何取得平衡，是制度成敗關鍵。因此匿名加工之方法如採統一固定方式規範，反而無法取得衡平，亦不符合現實之所需[68]。從而須將各業界處

---

[64] 森亮二，同前註 35，頁 27。宇賀克也，同前註 41，頁 39。

[65] Federal Trade Commission Act, 15U.S.C, §41et seq.(2012)，其第 5 條規定，如事業者以不公正、欺瞞之行為或慣行（unfair or deceptive act or practices）侵害消費者隱私時，FTC 得依第 5 條(a)(2)命令扣押、(b)排除，(m)(1)(A)或科以制裁金。

[66] 森亮二，同前註 35，頁 30。宇賀克也，同前註 41，頁 40。宍戸常寿，同前註 26，頁 43。

[67] 小林慎太郎，同前註 61，頁 32。関啓一郎，同前註 45，頁 62。

[68] 同前註 47，座談會記錄，頁 20，寺田真治之發言。

理、利用個資業者之實際狀況、資料管理體制、採取之匿名加工方法等要素納入考慮，始能完整建構一結合技術面及法制面之匿名加工規範，並能兼顧個資之有用性與當事人權利之保護。

## 第二目　匿名加工之方法

依修正後法第 2 條第 9 項，所謂匿名加工資料為：係對應本法第 2 條第 1 款與第 2 款二種不同類型個資，依法定措施加工後，所得之無法識別特定個人且無法回復資訊。故 1、同條第 1 項第 1 款之記述型個資：其加工方法為削除包含該當個資中一部分記述（包含藉由無法得有規則性方法，以復原該當部分記述，而替換為其他之記述等）。例如將組合於資訊中之姓名刪除，或將住址之市區以下之路、巷、號等刪除；又或者將生年月日替換為 20 歲年齡層、30 歲年齡層等抽象表記。2、同條項第 2 款之個人識別符號：其加工方法為刪除包含於該當個資中所有個人識別符號（包含藉由無法得有規則性方法，以復原該當個人識別符號，而替換為其他之記述等）。此乃因個人識別符號常是跨越各業界而被共同利用，須儘可能讓特定個人被識別之危險性降低，故須將個人識別符號全部刪除[69]。又此處所稱無法回復特定個人識別性，並未要求至嘗試任何手法均不可能復原之程度，亦即自技術面而言，並未要求全面排除回復可能性[70]。

上開第 2 條第 9 項「匿名加工」規定僅作原則性規定，而適用於各事業實務操作上具體方法，依法第 36 條第 1 項規定，應再依個人情報保護委員會[71]（下稱保護委員會）所訂規則揭示之基準以為進行。然保護委員會規則所定基準亦僅止於任何業者均能適用之一般性最小限度加工方法[72]，更具體之加工方法，因須考量該當個資之內容，預定之利用方法，及適合於各事業實務上資訊管理系統操作之匿名加工方法。故法修正後第 53 條規定，將各業界具體之匿名加工

[69] 宇賀克也，同前註 41，頁 41-42。
[70] 參閱眾議院內閣委員會 2015 年 5 月 15 日，及參議院內閣委員會，2015 年 5 月 28 日之答詢。
[71] 此為本次修法依內閣府設置法第 49 條第 3 項所設置之獨立委員會，用以監督個資法施行之專責機關。
[72] 宇賀克也，個人情報の保護と利用，法律時報 88 卷 1 号，2016 年 1 月，頁 72。

方法委由民間認定個人情報保護團體[73]制定之「個人情報保護指針」以自律性規範方式定立。且為避免認定個人情報保護團體基於業界立場，所定方法過度重視資料利用之方便性，不利於當事人權利保護。因此該條中規定相關保護指針作成之際，應努力與消費者代表，及關係人等交換意見以達成協議後再定立。此乃採取日本近年在行政規則制定時所導入之多方利害關係人參與程序（multi-stakeholder process）[74]之理念，即由處理個資業者及消費者間協議後，再訂出匿名加工之規則，讓消費者安心，而建立被信賴之匿名加工制度，以開啟活用大數據之路[75]。

### 第三項　敏感性特種資訊之新設

#### 第一款　原因

日本在修法之現行個資法並未對敏感性特種資訊（日本稱為「要配慮個人資訊」）作任何特別保護之規定，當時之主要之理由為：何謂敏感性特種資訊，要得到社會上共識是很困難；個資法本身應不問資訊性質、內容，僅須規定其蒐集、處理或利用上最低限度應有之規範即可，敏感性特種資訊則由其他個別法或指針作更嚴格之規範予以保護[76]。但地方自治團體制訂之個人資訊保護條例之半數均將有關思想、信仰等成為社會差別待遇之個資，較嚴格限制其蒐集、利用之要件[77]。其次，現行法之主務大臣由事業主管機關制訂之有關個資保護指導方針（Guide

[73] 認定個人情報保護團體，為日本為推動民間事業者能自律性遵守個資法之規範，而設計由個人情報保護委員會（未修法前為由各事業主管大臣），依個資法所定之條件，對申請符合條件之法人，給予認定為「認定個人情報保護團體」，而受此認定之保護團體，得依法處理其團體成員之個資處理事業者有關個資處理上之申訴，或對其團體成員進行有關確保個資適當處理之必要輔導。故而為遂行上述業務，認定個人情報保護團體依法應致力作成「個人情報保護指針」，此指針中包括「匿名加工資料作成方法」。

[74]「multi-stakeholder process」是指有對等代表性之三方以上利害關係人間，為解決某一課題，而為之意思決定、合意形成、或類此意見溝通之程序。其特徵為：1、依此程序得在利害衝突之關係人間，藉由平等對話，以增進互相理解而提高彼此信賴關係；2、因為由各方之利害關係人參加下，得反應各種不同意見，容易得到社會之正當性，及民眾之理解；3、因係透過各方以對話方式解決難題，故得找出由全部利害關係人一起行動以為解決之可能。

[75] 宇賀克也，同前註 72，頁 72。宍戸常寿，同前註 26，頁 43。

[76] 宇賀克也，同前註 41，頁 40~41。

[77] 例如東京都個人情報保護條例第 4 條第 2 項。

line）中，亦多訂有特別保護敏感性特種資訊之條款[78]。再加上EU個資保護指令第8條第1項至第4項亦有針對敏感性資訊特別保護規定。因日本個資法因未針對敏感性特種資訊設置特別規定予以保護，亦被認為是日本對個資保護不完全之處，而無法得到歐盟依EU個資保護指令第25條規定，得到十分性（adequate）認定之原因之一[79]。故於本次修法亦增定條文，對敏感性特種資訊加強其保護要件。

## 第二款　定義及種類

修正後法第2條第3項所謂敏感性特種資訊為：當事人之人種、信仰、社會身分、病歷、犯罪經歷、因犯罪被害事實、及其他為不對當事人產生不當之差別待遇、偏見、其他不利益者，其處理上須要特別注意，而為政令所指定之人資訊。以下分別說明其概念[80]。

一、 人種：指個人出生之世系、民族、種族，但不含膚色及國籍。

二、 信仰：指個人內心基本之想法，包含個人思想及信仰，但不包含得推知思想或信仰事實本身，例如購買某宗教團體之書刊等。

三、 社會的身分：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[81]，或是被歧視之賤民部落出身等。

四、 病歷：指罹患疾病之經歷，因曾罹患特定疾病將使其他人對當事人產生差別待遇或偏見。日本著名之例為痲瘋病及後天免疫不全症候群等疾病。另外引起較大討論者為身心障礙之資訊，然依學者之見解，認為如此之個資被

[78] 例如：金融領域有關個人資料保護 GL 之第 4 條第 2 項；電氣通信事業有關個人資料保護 GL 之第 4 條第 2 項。
[79] 宇賀克也，同前註 41。日本本次修法之目的之一，事實上亦為希望能得到歐盟十分性之認定，除去其與歐盟加盟國傳遞個資之障礙。
[80] 宇賀克也，同前註 41。日置巴美、板倉陽一郎，同前註 23，頁 67。
[81] 參見東京高等法院判決，平成 5 年 6 月 23 日，高民 46 卷 2 號，頁 43。

蒐集或利用仍有引起差別待遇之可能，應被認為為敏感性特種資訊[82]。

五、 犯罪之經歷：指受法院有罪判決之前科，即當事人受確定判決為刑罰宣告之事實。

六、 因犯罪被害事實：指受到一定犯罪行為侵害之事實，不問身體之被害、精神之被害或金錢之被害。此是為避免當事人因事實揭露受到第二次傷害，或被犯罪集團所定為犯罪之標的。

七、 其他為避免當事人受到不當之差別待遇、偏見及其他不利益，而在處理上須特別注意者：此款具體之個資項目，則由政府機關依政令指定，目前討論之項目為，遺傳資料、性的偏好、違反社會秩序前科、信用資料。

### 第三款　蒐集、利用之限制

#### 第一目　原則

現行法，有關敏感性特種資訊之蒐集或利用與一般個資相同並無區別；而修法後則於第17條第2項規定其取得，除有下列例外之事由，亦即相較當事人之權利、利益有應優先被保護者，或限制其取得不具有合理性者外，原則上均應事先得到當事人同意。

#### 第二目　例外事由

1、法令有規定者。

2、為保護人之生命、身體或財產而有必要，於得到當事人同意為有困難時。

3、為提升公眾衛生或推廣兒童之健全育成特別必要時，於得到當事人同意為有困難者。

[82] 宇賀克也，同前註 41，頁 48。

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，因得到當事人同意，有對該當事務之遂行造成障礙之虞時。

5、敏感性特種資訊，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（例如新聞媒體或宗教團體等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。

6、其他準用上開各款所揭示之情形，而為政令所規定者。

因此處對當事人同意之方式並未限制，故亦得以口頭同意，然搜集者仍應儘量明確化同意之有無；至於默示同意雖未被限制，學者仍主張以明示同意為原則[83]。

再者，前開例外事由第2款中所謂「得到當事人同意為有困難」，乃指①、得到當事人之同意在物理上為不可能或有困難者(如當事人死亡、或行蹤不明者)；②、請求當事人同意而被拒絕者；③、因請求當事人同意，而有助長違法或不當行為之虞者。而第3款之「公眾衛生之提昇」，例如癌症或疫學之研究，依不同人種之特定藥物藥效研究，為特定疾病之預防、治療等目的，而取得有關人種之資料。

## 第四款　個人資料與保有個人資料之定義與區分之意義

個資法保護之客體原則上為「個人資訊」，但為避免處理個資業者負擔過重，在現實上法施行之可能及考慮對公益之影響[84]，日本立法時將其保護客體再畫分範圍為「個人資訊」、「個人資料（データ（data））」及「保有人資料」，然後對應保護範圍之不同，課予業者義務亦由輕至重層疊構成。

上述被分為三種範圍之保護客體，「個人資訊」為最廣義之概念，「個人資料」及「保有個人資料」包含在其中；「個人資料」為廣義之概念，「保有個人

[83] 宇賀克也，同前註 41，頁 48。
[84] 宇賀克也，個人情報保護法の逐條解說（第二版），有斐閣，2005 年，頁 42。

資料」包含在其中，其關係如附圖二（詳參第 42 頁）。

按業者處理個人資訊之流程得分為三個階段：於蒐集、取得階段，稱為「個人資訊」；於進行鍵入、儲存而建構成個人資訊資料庫者，稱為「個人資料」；之後被保存於資料庫六個月以上者，稱為「保有個人資料」；本法對每個階段課予業者本文以下所述由輕至重不同層次之義務[85]，此為本法立法之特色之一。

在此先說明「個人資料」與「保有個人資料」之定義。

## 第一目　個人資料

所謂個人資料依本法第 2 條第 4 項，係指構成個人資訊集合物－data base 等之個人資訊而言；其範圍較個人資訊為限縮，限定於得依電腦檢索、或被有體系編存於資料庫中之個人資訊；或其他依一定方法處理儲存，為有體系構成且容易檢索之個人資訊；如僅為散存於各媒介物上，未被有體系整理儲存之個人資訊，即非本法所稱之個人資料。蓋使用電腦自動處理系統或以人工有體系整理儲存之個人資訊，具有完整性及利用便利性，且可快速、大量傳遞。其被洩漏、竊取或為不當之利用致使個人權利、利益受侵害之危險性相對提高[86]。著眼於業者上述處理利用個資方式，個資存在形態上可能包含之風險，本法第四章對處理個資業者再加重課以確保個資之安全性、正確性之義務、對第三人提供之限制等；故為避免對民間業者造成不必要之負擔，將受保護之個人資訊範圍予以限縮；因此處理個資業者除對「個人資訊」有利用目的特定等義務外，依本法第四章對「個人資料」進一步負有確保其內容正確性、最新性（第 19 條）、採取安全管理措施（第 20 條、第 21 條、第 22 條）、限制對第三人提供（第 23 條、第 24 條、第 25 條、第 26）等義務。

## 第二目　保有個人資料

[85] 北原宗彥，「個人情報保護基本法」の問題点，慶應法律學，公法Ⅱ，慶應義塾創立 150 年紀念論文集，2008 年 12 月，頁 118。
[86] 宇賀克也，同前註 15，頁 38。

依本法第四章規定，處理個資業者關於其所保有個人資料，有對資訊當事人公布相關事項、提供閱覽、訂正、停止利用等義務。此所謂「保有個人資料」依本法第 2 條第 5 項：為處理個資業者具有權限得提供閱覽、訂正、追加或刪除內容，停止利用、消去、停止對第三人提供之個人資料；在此又進一步將受保護之「個人資料」限縮其範圍為「保有個人資料」；其理由係因考慮該當業者等履行前述提供閱覽訂正等義務，必須先保有該當個人資料，且事實上有上開義務履行之可能性者[87]。

其次，同項後段規定：因該當個人資料存在與否之事實如被公開，將有損害公益或其他利益，且為政令所規定者，不適用本項之「保有個人資料」有關義務之規定。日本政府資訊公開法第 8 條亦有類似「拒絕回答」之規定[88]。換言之，適用本項「保有個人資料」之義務規定者，需為無公益、其他利益保護必要性之個人資料，此乃因業者對保有個人資料有提供當事人閱覽之義務，如公開該當個人資料存在與否之事實而所損害之公共利益等，相較於將資料提供當事人閱覽、利用等所保護之個人利益，被認定應優先受到保護時，被請求提供閱覽之該當業者，得不告知該當個人資料存在與否。又本項另一要件為「政令所規定者」,依本法施行細則第3條規定為:因該當個人資料之存否被公開時，1、將有損害於當事人或第三人之生命、身體或財產之虞者；例如家暴、兒童虐待事件，對被害人進行救助之民間機關保有被害人當事人之個人資料，而加害人又正為被害人之法定代理人者，加害人以被害人法定代理人身分請求閱覽被害人當事人之個人資料時，一旦為拒絕或未保有該當個人資料之回答時，加害人即能知悉被害人現今所在或狀況;2、將有助長或引誘違法或不當行為之虞者;例如該當業者保有職業股東之個人資料，或反覆為惡意申訴之顧客個人資料，如被當事人知悉有如此個資之存在，即可能招來報復；3、將有損害國家安全或

[87] 藤原靜雄，同前註 15，頁 33。宇賀克也，同註 15，頁 42。
[88] 請參閱范姜真媺，日本資訊公開救濟程序之探討，東吳法律學報，17 卷 1 期，2005 年 8 月，頁 50，註 45 之說明。

與他國或國際機關間信賴關係之虞，或使與他國或國際機關間交涉蒙受不利益之虞者；例如飯店或保全警備業者保有記錄外國政要等活動之個人資料；軍火製造業者保有記錄擔任武器設計、開發者之個人資料，其保有之事實一旦公開，將有損於國家安全或與他國間之信賴關係；4、將有對犯罪預防、鎮壓或搜索，或其他公共安全與秩序之維持形成障礙之虞者；例如回應檢警機關搜查事件，業者因照會所作成回報中，犯罪者個人資料存否之事實，將使進行犯罪偵查活動之有無曝光。故本項特別將上開個人資料自業者保有個人資料中除外，有關業者所被課予之義務得被免除。

再者，如僅為業者短期間保有之個人資料，其對個人權利、利益侵害之危險性相對較低；且業者自蒐集個資至提供當事人閱覽，或訂正、刪除其內容，往往需要時間及成本；又如在提供閱覽前資料已被消除者，實亦無規範之實益；基於上述之考慮，本項亦將業者保有個人資料，依一年以內政令所定期內被消去者，排除於本項之「保有個人資料」範圍外；換言之，適用本法第四章應提供閱覽、訂正之保有個人資料，需為業者繼續一定期間處理利用之個人資料始足當之。之後本法施行細則第 4 條將前述期間定為六個月；在本法施行前已保有之個人資料者，此六個月之期間則自本法施行日開始起算[89]；如個別法本身定有資料保存期間，則優先適用個別法。而其問題在於如有業者為規避本法之適用，刻意將該當個人資料於六個月期間內先行消去，然後立刻復原再繼續保有時，是否有本法第四章之適用，恐有爭議[90]。

## 第三節　法適用範圍－受規範對象

現今 IT 社會中，個資之處理已為許多業者日常業務之一部分，是否所有業者均無例外一律納入規範？在立法政策上應如何界定受規範之業者？為另一重要課題。而本法第四章有關處理個資規範之義務，其適用對象則定為「處理個

[89] 宇賀克也，同前註 15，頁 43。
[90] 宇賀克也，同前註 15，頁 41。藤原靜雄，同前註 15，頁 34。

資業者」，依本法第 2 條第 3 項規定，「處理個資業者」係指將個人資訊資料庫供事業之用者，原則上將所有業者納為規範之對象，例外再將其處理個資之數量及利用方法侵害個人權利、利益之虞低微，且依「政令所規定」者，排除本法之適用。當然此項適用對象不包含國家機關、地方自治團體、獨立行政法人等、地方獨立行政法人在內。

### 第一項　以個人資訊資料庫等供事業之用者

所謂「個人資訊資料庫等」，其具體之意涵，依經產省 GLⅡ1、(2)之解釋為：使用電腦將特定個人資料以得檢索有體系構成之個人資訊集合物；或雖未使用電腦，如病歷、學生指導紀錄等以書面檔案處理之個人資料，為依一定規則（如五十音順、生年月日等）作整理、分類，並附以目次、索引、關鍵字等成為易於檢索特定個人資訊之集合物。換言之，「個人資訊資料庫」包含二種類型，一為以電腦處理之資料庫，另一為以人工處理之資料庫；但二者均需具備「檢索容易性」及被「有體系性」整理之要件。

所謂「事業」係指具一定目的反覆繼續從事之同種活動，且為社會一般通念上所認定之事業[91]。上述解釋有二個應注意之重點，一為此處之事業不限以營利為目的，法人、非法人團體，甚至個人所進行者均有該當之可能性。蓋儲存、處理利用包含大量個人資訊資料庫所可能帶來對個人權利、利益之侵害，不因其是否為營利事業而有本質上之不同，故均納入為本法規範之對象[92]。惟於現今電腦普及之社會，一般人用電腦按拼音順序、筆畫等儲存大量親友、生活周遭關係人之姓名、電話、住址等個資以為連絡發送信使用者，不在少數；有無必要將如此日常生活行為亦納入本法之適用應再商榷。為避免本法適用範圍不當擴張，造成人民生活上之困擾，因此本項以「供事業用」之要件劃定其

[91] 參議院會議記錄平成 15 年（2003 年）5 月 13 日（第三號），政府參考人藤井昭夫之回答。宇賀克也，同前註 15，頁 31。
[92] 園部逸夫，同前註 29，頁 88。

適用範圍;另一為所謂事業須有「社會一般通念上被認為係事業」之「社會性[93]」，如非為社會上通認為事業,而為一般日常生活利用行為者,亦不受本法之規範。上述二個重點為本法所稱「事業」之判斷基準，藉以有效限縮本法第四章適用範圍。此外，如業者本身對資料庫內容未有任何行為涉入或認知，單只是進行運送、保管、販賣行為者，如運送業者、倉庫業者、書店等，亦非此處所謂「供事業使用者」。

### 第二項　適用除外之對象

現行法於立法時最大爭議的是，總則法為對民間業者團體全面性之適用規範，故新聞媒體業者，宗教、政治團體亦為法適用對象，一旦被課予個資法之義務將對其新聞取材、報導、宗教、政治活動造成極大障礙。尤以新聞媒體之報導自由、採訪自由為憲法所保障表現自由之重要內容，又為防止行政機關得藉本法進行行政指導而不當干涉新聞媒體之報導活動；本法立法時曾將新聞媒體納為規範對象，被強烈質疑有違憲之虞，於日本國內引發爭論[94]；日本新聞協會、日本民間放送聯盟與日本放送協會，並於法案審議中聯手發表聲明強力反對將新聞業者納入法之適用對象。其他又如宗教、政治團體在從事相關活動時，或大學等研究機構等在進行研究時，均可能處理、利用大量個資；基於憲法保障之宗教自由、學問之自由等考量,能否與一般業者同歸於本法適用對象，亦備受爭論。為平息爭議，除去眾人之疑慮，最終在本法完成立法時，特別於現行法（本次修法未修正）第 50 條第 1 項將下列處理個資業者等，其處理利用個資之目的全部或一部，有該當於各款所定之目的時，排除於本法第四章之適用範圍外。換言之，該當本法適用除外之要件有二，一為業者須為本項揭示之事業類型，另一為，其利用個資目的亦須該當於本項各款規定之目的。如該當業者進行與該當款項所定目的無關之活動時，即不能豁免於本法之適用；例如

[93] 岡村久道，同前註 5，頁 88。藤原靜雄，同前註 15，頁 31。
[94] 藤原靜雄，同前註 15，頁 136。岡村久道，同前註 31，頁 30。田島泰彥、三宅弘編，同前註 7，頁 19。

報導機關經營文化事業，開辦寫作研習班等與報導自由完全無關之活動，即為其適例。但如同一個人資訊資料庫，同時為報導目的及文化事業營業目的利用時，或業者之利用目的只有一部分該當於適用除外條款之目的而非全部時，仍得不受本法之適用；顯示立法者對新聞報導、政治活動、研究活動等自由賦予相當程度尊重[95]。

（一）廣播機關、新聞社，通訊社及其他報導機關（以報導為業之個人亦包含在內）供報導之用：

所謂報導，依同條 2 項之解釋為：「對不特定之多數人讓其知悉客觀事實」之傳達活動，及「基於客觀事實為意見或見解之陳述」。此處廣播機關、新聞社、通訊社等僅為例示；舉凡進行事件報導之出版社、雜誌社、電子出版業等大眾傳播業者均包含在內。

（二）著述業者，供著述之用：

於現今 IT 社會中，從事著述者可能亦容易處理大量個資，有鑒於表現自由之重要性，特別將其與報導分離而為獨立一款予以揭示。所謂「著述」，依立法者說明：不問其範疇，將人之思想或感情、智能活動以文藝作品、評論、學術論文撰寫方式等為創作性表現者均屬之。其表現方法、手段亦不侷限於書本之刊行，網路文章等亦包含之[96]。且基於著述之目的，凡參與採訪、執筆、校正、印刷、製本、刊行等與著述之完成程序有關者，均包含於本款所稱之「以著述為業者[97]」之範圍內。

（三）大學或其他以學術研究為目的之機關或團體或其所屬人員：

本款係基於憲法所保障學問自由之考量；此所稱之大學或學術研究機關團

[95] 宇賀克也，同前註 27，頁 196。
[96] 參閱平成 15 年（2003 年）4 月 8 日第 156 次國會院會議事錄 21 號。
[97] 宇賀克也，同前註 27，頁 199。

體，包括私立大學、民間研究所、學會等以學術研究為目的之機關或團體。不問是否有法人資格；而其所屬人員，則包括私立大學教師、民間研究所之研究員、會員等。因進行學術研究不只限於上述機關、團體，由其構成員之各個個人自行進行者不在少數，因此本款特別揭示其構成員亦為本款適用對象。問題則在於，不屬於大學或任何學術研究機構之個人，以學術研究為目的而為處理個資時，即無本款之適用，須回歸受本法第四章之規範；同樣為學術研究，僅因是否屬於大學或學術研究機構之成員，而課予不同之法律義務，是否公平、合理，尚有商榷餘地。

（四）宗教團體為供宗教活動（包含其附隨活動）目的之用：

所謂「宗教團體」為依宗教法第二條之定義為：在推廣特定宗教教義而進行宗教儀式，及教化養成信徒為主要目的下，具備有禮拜設施之神社、寺院、教會、修道院等同性質之團體；及包含此等團體之教派、宗教、教團、教會、修道院、司教區、其他同類之團體。

所謂宗教活動，依前述宗教法第 2 條解為，推廣教義、舉行宗教儀式及教化養成信徒等活動；其問題則在附隨宗教活動究竟如何界定範圍？例如宗教團體經營之墓園、靈骨塔或是葬儀社等，雖非以宗教活動為主要目的，但事實上亦有解為內含普及教義目的之餘地，是否能納入此處之「附隨宗教活動」不無疑問。有學者主張鑒於宗教自由為憲法保障之基本人權，為防止行政過度介入宗教活動，所謂「為宗教活動目的之用」不應作限縮之解釋，故上開活動亦應解為宗教附隨活動而排除本法第四章之適用[98]。

（五）政治團體為政治活動（包含其附隨活動）之目的者：

所謂「政治團體」，依政治資金規制法第 3 條規定解為：1、以支持、推展或反對特定政治主義或政策為其基本目的之團體；2、以支持、推薦或反對特定

[98] 宇賀克也，同前註 27，頁 201。

公職候選人為其基本目的之團體；3、及其他繼續性、有組織的以推動上述 1、2、活動為其主要活動目的之團體。再依同法第 5 條：以研究政治主義或政策為目的之團體，而由國會議員所組織者或其主要成員為國會議員之團體，及對特定政黨提供資金援助為目的之「政治資金團體」，均為本款之政治團體。

而「供政治活動用」之個資處理，最典型者即為政黨後援會參加者名簿之編輯，或政黨發行刊物之購讀者名單資料。當然此款與前款相同，關於政黨附隨活動之範圍界定，亦有相當程度之困難度。學者對此則主張：政黨為實現憲法確立之議會民主政治制度所不可或缺之要素，故應保障政黨之高度自主性及自律性讓其自由組織營運，為避免對政黨政治活動作過度之干涉，故仍不宜將供政治活動用之目的作限縮解釋[99]。

### 第三項　外國個資處理業者之適用

現行法因日本有關法律之適用，一貫採取「屬地主義」，以在日本領土內發生之行為或事件為適用對象，從而對於在國外收集、處理日本國內居住者之個資之業者，並無本法之適用。

然近年來因企業活動及物流全球化，且電子商務等網路經濟活動極速普及，國外之業者透過網路跨國對居住於日本之住民販售商品或提供服務者日益增多，並因此而取得日本住民之個資，如有違法不當之利用者，因無本法之適用無法採取有效之對策，對個資之保護形成一大缺口，故本次修法採標的規準（例如新聞媒體或宗教團體等），亦即外國之行為者以本國人為標的而施行特定行為時，亦應受法之規範，特別於第75條增訂對境外之外國個資處理業者適用規定[100]。

#### 第一款　要件

須為關連於對在日本居住之人販售物品或提供服務等，而直接取得該當當事

[99] 宇賀克也，同前註 27，頁 203。
[100] 日置巴美、板倉陽一郎，同前註 23，頁 134~135。

人之個資。所謂販售物品等，係指如販賣或借貸給有體物之商品；而提供服務，則係指提供如音樂、影像或資訊等之服務，例如外國之旅館飯店因來自日本客人預訂住宿旅行而取得個資者[101]。

### 第二款　應遵守之義務

依第75條規定該當外國事業負有：第15條利用目的特定義務、第16條特定目的之利用限制、第18條利用目之通知，及第19條至第25條有關資料內容之確保正確、安全維護、對第三人提供之限制等義務，另第27條至第36條有關對當事人保有個人資料之公開、訂正、停止利用、提供閱覽等義務，第四章第一節個資處理業者應遵守之義務幾乎均有適用。而第17條則未包含在內，乃因其蒐集個資之主要行為，為在日本領域內所進行者，直接適用該條即可，無須再迂迴適用第75條之規定。又因本條所規範者為直接自當事人蒐集該當個資，非由第三人提供者，故第26條亦無適用之餘地[102]。

### 第三款　保護委員之監督

因此部分法之執行，涉及其他國家之司法、行政主權，故而保護委員會得行使之權限，僅限於依第41條進行指導或建議、或第42條之勸告。若認為外國事業有違反本法之義務，經進行上述之指導、建議或勸告後，仍未予以改善時，應依本法第78條，請求該當外國之主管機關依該國法令協助執行。

## 第四節　民間處理個人資料業者之義務

### 第一項　層疊式之義務構造

依本報告第二章第四節所述個資法保護之客體，分為個人資訊、個人資料及保有個人資料三範圍，分別課予個資處理業者輕重不同之義務，以下即依此三者分別說明業者應遵守之義務。

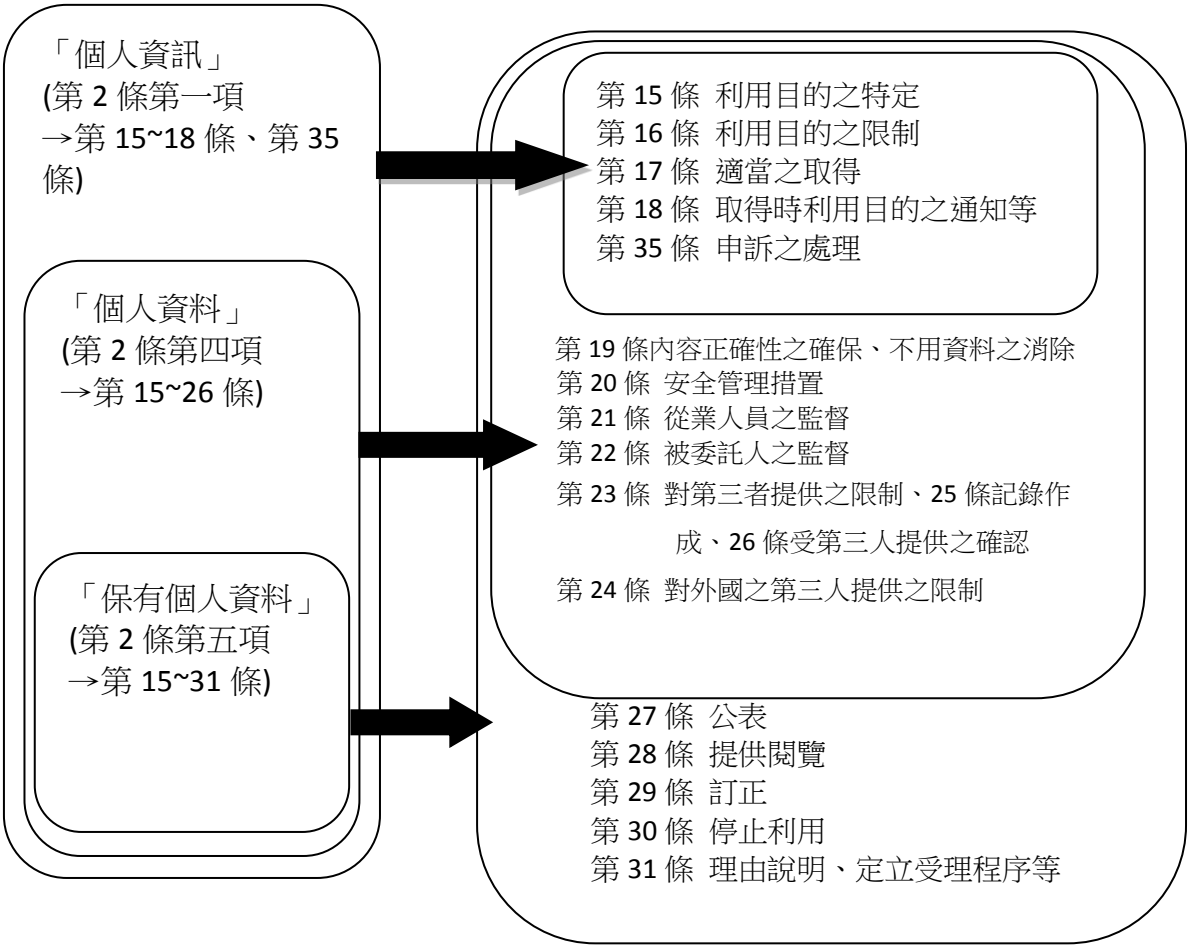
---

[101] 瓜生和久，平成 27 年改正個人情報保護法，商事法務，2015 年 12 月，頁 144。
[102] 日置巴美、板倉陽一郎，同前註 23，頁 136。

業者第一階段最基本之義務為自蒐集個人資訊時起應負之特定利用目的等義務;業者第二階段如將個人資訊鍵入或建構成個人資訊資料庫之「個人資料」,則須進一步負擔其安全管理等義務；業者第三階段對其繼續一定期間所保有之個人資料，須再進一步負對當事人提供閱覽、訂正等義務，學者稱此為「層疊式義務[103]」構造參見如附圖二。 如此立法之理由，係考量業者之負擔及其履行義務之可能性；申言之，處理個資業者如不欲負擔本法之義務，開始應先避免不必要個人資訊之蒐集，自無任何義務可言；又即便業務上需要而蒐集個人資訊後，亦盡可能不建構為資料庫以為利用，則此時即無須負加重之第二階段義務；對已建構之個人資訊資料庫已無利用之必要時，應儘快將其消去不做長期留存，自無第三階段義務之負擔。以此為誘因期望業者在衡量實際所需與其被課予義務之輕重，將個人資訊之蒐集、處理及利用自發性降至必要最小限度，對業者為浮濫之個人資訊蒐集、處理產生抑制作用，相對提高對個人之保護。

[103] 岡村久道，個人情報保護法，商事法務，平成 17 年，頁 133。鈴木正朝，個人情報保護のための企業法務，法律ひろば，2003 年 9 月，頁 51。

附圖三：層疊式義務表[104]




[104] 修改自岡村久道，同前註，144 頁圖。

## 第二項　關於個人資訊之義務

關於本節之重要之法修正部分為：緩和特定目的變更之限制，主要之目的即為符合大數據時代下，業者對蒐集所得大量個資在不損害當事人權益下，得因應事業之所需靈活運用於原特定目的外，以增加個資之合理利用範圍，其餘部分予現行法差異不大。

### 第一款　適當取得之義務

為建立當事人與業者間之信賴關係及自開始處理個人資訊之始即能確保其合法、適當性，預防個人權益受損，本法第 17 條規定：業者不得以欺騙及其他不正當手段取得個人資訊。所謂不正當是否須至違法程度？抑或在通念上被認為有違背公序良俗者，即足當之，似乎有討論空間。查經產省 GLⅡ.2.(2).①則特別舉例說明：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訊」、「強迫他人違法提供第三人資訊」、「明知其他業者以不正當手段蒐集個人資訊後，再轉交自己」，等均屬不正當蒐集個人資訊事例，採較寬鬆之見解。其次較有爭議者為，該當業者並非第一手蒐集個人資訊者，而是受讓他人不當取得時，因本條並無「善意」、「惡意」之要件，是否有本條之適用[105]？為避免業者脫法行為，並周全保障個人權益，通說多以：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[106]。

又違反本條規定所取得之個人資訊中，如為業者所保有之個人資料時，當事人得依本法第 30 條 1 項請求停止利用或刪除。

### 第二款　特定利用目的

#### 第一目　利用目的之特定

[105] 宇賀克也，同前註 27，頁 97。
[106] 宇賀克也，同前註 27，頁 97。藤原靜雄，同前註 15，頁 76。園部逸夫，同前註 29，頁 120。

依本法第15條第1項:業者等於處理個人資訊時應盡可能特定其利用目的;特定利用目的為本法第 16 條第 1 項限制業者個人資訊處理範圍，及第 18 條公告、通知利用目的之前提；藉此防止業者之濫行或為不必要之個人資訊處理，同時亦透明化個人資料之處理,讓當事人得預見自己之個人資訊將如何被利用,評估其風險及利益以決定是否提供，且亦得據為判斷蒐集處理個資事業是否為目的外之利用行為。又利用目的須盡可能具體敘述不得過度抽象概括，以避免傷及本項立法意旨，並避免紛爭發生。但應具體化至何種程度?且因處理個資之事業種類、性質不同,所處理之個資類型亦不同,原難以法訂出一致性之標準；但為避免同種類業者之間，產生不合理之差距，學者及經產省（經濟產業省）GLII.2.(1).①均主張:如業者係為法人、團體時，至少得要求對照其章程所訂事業目的，當事人得合理預測其個資將被利用於何處程度之具體性[107]。

此所謂「利用目的」並非指蒐集、處理、利用等各階段之目的，而是業者依一連串個人資訊處理程序後最終所欲達到之目的[108]，因此存在於每個處理該當個人資訊之業者，或連續性處理個人資訊之每一階段，而當然此利用目的不得有悖於公序良俗。

### 第二目　利用目的變更限制之緩和

於蒐集個人資訊時雖已特定其利用目的，而於後處理過程中，如得任意變更利用目的，無疑使本項特定利用目的失去意義；但如果完全不容許變更，在現今資訊科技發達時代,業者將無法靈活運用大數據以創新產業或開發新商機,大大降低合理利用個資之可能性。因此本次修法，即將現行法本項原規定允許「於被認為與變更前利用目的有相當合理關連性」之目的變更要件，修正去除「相當」之用詞，一定程度緩和利用目的變更之限制[109]。但問題是「合理之範

[107] 宇賀克也，同前註 15，頁 79。
[108] 園部逸夫，同前註 29，頁 109。
[109] 日置巴美、板倉陽一郎，同前註 23，頁 122。宇賀克也，同前註 22，頁 47。

圍」應如何判斷？學者之見解有所歧異：一說為其變更至少必須依通常人之判斷，是當事人得預見之限度之變更[110]；另一說則以係客觀上被社會通念認為合理之限度內[111]；另有學者主張，為當事人通常得預見程度之限度內[112]。上述三種不同之主張，最主要之差別在於，對利用目的變更之「預見可能性」是以「當事人」之主觀認知為準，抑或以社會一般人之客觀認知為準？一般而言，於現今電腦網路發達之時代，許多事業處理大量之個人資訊，顧及成本及效率，採對眾多當事人一併將其利用目的於公佈於其網頁上最為普遍，故應以社會一般通念上認為合理得預見之範圍，作為判斷基準，較客觀並容易解決爭議。又如該當業者超過此得預見之範圍而為該當個資之利用時，則應視為目的外之利用，依本法第 16 條原則上應事先得到當事人同意。

### 第三款　利用目的之告知

#### 第一目　原則：

本法第 18 條 1 項規定：業者於蒐集個人資訊時，除已事先公告其利用目的者外，應儘快將其利用目的通知當事人或公告之。立於保護個人權益之觀點而言，業者於蒐集個人資訊時，能事先公告或通知利用目的最為理想，但如此一來業者必須早先於蒐集前即特定其利用目的，始能履行此一義務；然如前述，利用目的之特定本法僅規定為努力義務，本條未強制性規定業者於蒐集個人資訊時即須告知當事人利用目的；於瞬息萬變之商場上業者常須靈活運用經營策略，機動改變行銷方法，強制性要求必須於蒐集個人資訊當下或之前履行告知義務，恐造成業者過重負擔；且本規定目的在於讓當事人有機會預知其個人資訊可能被處理或利用之範圍或方法，如業者於蒐集後迅速通知或公告其利用目的，當事人仍有機會要求停止利用，尚不致過度損及當事人權益[113]，從而本法

[110] 岡村久道，同前註 5，頁 147。瓜生和久，同前註 101，頁 60。
[111] 宇賀克也，同前註 15，頁 80。
[112] 関啓一郎，同前註 45，頁 13。
[113] 宇賀克也，同前註 15，頁 89。

以較緩和立法方式規範業者。

依前述本條之規定，其告知方式係以預先公告為主，通知當事人僅為未預先公告時得為之選項；換言之，業者僅需將利用目的公開置於當事人得知之狀態即可，非必須「直接通知」當事人；立於保護當事人之立場應以確保當事人知悉之通知方式為原則較佳；其立法理由仍為考量大量蒐集、利用各種個人資訊已為現今社會之常態，如均須一一直接通知當事人，對業者可能造成過重負擔，甚至對當事人亦有造成不必要困擾之虞，因而採取以公告為主，通知為輔之立法方式。又此「通知」方法不限於書面，得以電子郵件（e-mail）或傳真方式，甚至口頭、電話等均可[114]。「公告」則可揭載於公報、報紙、網站上，或發送手冊，或於營業處所窗口、櫃台等處以海報張貼或放置傳單等方式為之。對業者而言得選擇其成本負擔低之方式為之，但對當事人而言，如其個人資訊保護意識不高，或較為忙碌疏忽者，僅為利用目的之公告，其錯漏之可能性極高，對當事人之保護不能謂為周全。

### 第二目　例外

本條第 2 項規定，業者因與當事人締結契約而以契約書或其他書面（包含以電子方式、磁氣方式，其他人無法知覺方式所作成記錄），自當事人依書面記載方式取得個人資訊者，因其可信度及明確性遠較其他依口頭方式取得者為高，且更容易編輯為資料庫，存檔後利用之機會大增；故特別課予業者事先告知之義務，以確保當事人在提供自己資訊前有慎重考慮之機會[115]。

常見之例為，業者與當事人訂立契約時，各種契約書上所記載當事人個人資訊，其他如各種申請書、問卷調查表、懸賞應徵用紙等，舉凡蒐集由當事人記載於書面之個人資訊者均應有本項之適用；此「書面」並不限於當事人自己

[114] 宇賀克也，同前註 15，頁 90。但由金融廳所揭示有關金融領域之 GL 第八條一項則規定，則以書面之通知為原則。金融分野における個人情報保護に関するガイドライソ，網址：http://www.tsa.go.jp/public/public.html，2016 年 6 月 10 日造訪。

[115] 宇賀克也，同前註 15，頁 92。藤原靜雄，同前註 15，頁 76。

填寫者，包含直接由當事人遞交而取得身分證、戶口名簿、駕照等影本者；甚至包括為確認當事人身分而暫時保管之健保卡等。又因本項包括以電子郵件方式、磁氣方式等所作記錄，故使用電腦網路接收來自當事人之電子郵件而取得個人資訊，在網頁（web）畫面登載欄直接鍵入而取得個人資訊者，均有本項之適用。

本項規定為「事先」對當事人「明示」，故業者應於該當個人資訊取得前即明示利用目的。「明示」之方法，例如將利用目的項目於書面上特別標示、特別另以其他書面表明利用目的交付給當事人；依其事業性質及處理個人資訊性質之不同，得採不同之方法，重點在以合理及適當之方法讓當事人能確實認識其內容[116]。如僅將利用目的夾雜記載於契約一般條款中，當事人不易辨識其存在或不易了解其內容者，即難被認為符合於本項之明示之義務[117]。

本項但書規定：為保護當事人之生命、身體或財產而於緊急必要時得免除事先告知義務。例如將病重昏迷患者病歷告知急救之醫護人員，如要求事先明示利用目的，事實上不可能、亦不合理，故例外免除業者本項事先告知義務。

### 第三目　適用除外事由

業者利用目的之告知係為保障當事人之權益所必要者，但如利用目的告知將使應優先於當事人權益而受保護之他人權益或公共利益受損害時，基於利益比較衡量原則，業者應得豁免於本條之適用，基此本條第 4 項訂有下列四項適用除外事由：

1、將利用目的通知當事人或公告時，將有損害當事人或第三人之生命、身體及其權益之虞者。例如蒐集不治之重症患者病歷，以進行治療方法之研究，如告知當事人真實病名將打擊其求生意志者。或學校機關將虐待兒童、家暴事

[116] 金融領域 GL3 條 3 項。
[117] 園部逸夫，同前註 29，頁 124。宇賀克也，同前註 15，頁 92。

件有關加害人個人資訊提供給社會福利機關進行介入、處理者，若告知可能引起報復或藏匿時。

2、公告或通知利用目的將有害於業者之權利、正當利益之虞者。例如因通知或公告利用目的，可能使該當業者新商品開發之訊息、營業「know-how」等有關營業秘密事項被公開，而損及其競爭上地位[118]。

3、業者對國家機關或地方自治團體所遂行之法令所定事務有協助之必要，將利用目的通知當事人或公告，將對該當事務遂行有產生障礙之虞者；例如為協助犯罪偵查，業者提供檢警機關客戶可疑資金往來資料。

4. 自該當個人資訊蒐集狀況觀之，得認為利用目的已明確之場合。例如提領郵件貨物之核對身分證件，當事人原已確知利用之目的者。前述三款均以通知、公告利用目的將生損害、障礙為理由，而豁免於本條之適用；惟本款係以進行通知等並無實益為由而免除，其立法理由仍在於減輕業者之負擔[119]。

**第四目　利用目的限制原則**

**1、原則：**

依前述本法第 15 條規定業者盡可能特定其個人資訊之利用目的，再依第 18 條將其公告或通知當事人，並遵守第 17 條以正當手段蒐集個人資訊，均為事先預防業者不當或違法蒐集個人資訊，致使當事人受損為其立法目的；而業者蒐集取得個人資訊後，其處理、利用仍應限制於特定利用目的範圍內，如此才能一以貫之保障當事人之權益不受未預期之損害。基此本法第 16 條第 1 項規定：於未事先得到當事人同意下，不得超越達成特定利用目的之必要範圍為個人資訊之處理。所謂「處理」，包含處理之手段、方法、被處理個人資訊之內容、

[118] 岡村久道，同前註 5，頁 169。鈴木正朝，同前註 24，頁 162。宇賀克也，同前註 15，頁 94。
[119] 宇賀克也，同前註 15，頁 95。

數量等，均不得超過必要之範圍[120]。

設業者因事業合併、經營權讓與等事由，而繼受取得他業者處理之個人資訊時，如繼受者得不受拘束自由改變原定利用目的時，將有使當事人於不知情下權益受損之危險，亦架空前述特定利用目的之規定。因此本條第 2 項規定：因事業合併等事由而繼受其他業者所蒐集取得之個人資訊者，於未事先得到當事人之同意時，不得超越達成繼受前該當個人資訊被特定之利用目的，而為該當個人資訊之處理、利用。亦即，事業繼受者於事先未得到當事人同意時，亦僅能於達成被繼受業者原定利用目的範圍內繼續為該當個人資訊之處理、利用。

再者，依本條 1 項與 2 項均以「事先得到當事人之同意」為目的外利用之條件，此乃當事人與業者間既有合意，即應由當事人間自治，本法無須加以限制，僅於得到當事人同意之方法上，應注意不得以例如「同意將來被本公司認為有必要之利用目的」等「概括式事前同意方式」，以避免類似空白授權而不利於當事人；依經產省 GLⅡ.1.(10)之解釋，業者必須對應其事業之性質及處理個人資訊狀況，依資訊當事人在作同意之判斷上被認為合理且適當方法為之。

**2、適用除外事由：**

限制業者目的外利用個人資訊，係為事後保障當事人權益不受未預期之損害，但目的外利用個人資訊不必然侵害當事人之權益，且目的外利用亦有為保護應優先受保障之公益，或他人之權利、利益者，完全禁止目的外利用，即不合理[121]；因此本條於第 3 項明定四項例外事由，業者於有該當於其中之一者，即得於未得到當事人同意下為目的外之利用。

(1)、基於法令者；所謂法令，包括法律、命令及條例，但不包括行政規則

[120] 宇賀克也，同前註 15，頁 82。藤原靜雄，同前註 15，頁 71。
[121] 岡村久道，同前註 5，頁 161。

[122]；因既為法令明文規定之利用目的，即可認定立法已認為係為合法之利用，或有應優先保護之利益存在，故得不受本法利用目的之限制。例如依刑事訴訟法第 218 條因法官發出強制處分狀為個人資訊之搜索、扣押等而提供者；或依組織犯罪防制法第 54 條申報客戶可疑之金融交易紀錄等。

(2)、為保護人之生命、身體或財產而有必要時，且得到當事人之同意為困難者；此處之人包含自然人、法人及其它團體，亦不限他人，包括當事人在內。此款適用除外事由第一個要件為，人之生命、身體或財產等權利、利益有受侵害之危險性，而該當個人資訊之目的外利用對上該權益之保護被合理認為有必要性。第二要件為，取得當事人之同意有困難者，例如已為請求而當事人不同意，或因當事人為意識不明或身分不明之患者，物理上不可能取得同意者，為查詢病歷或身分而照會相關機關。或者取得當事人之同意，反有助長當事人違法或不當行為之發生等[123]，例如將蒐集所得之職業股東、犯罪組織成員、恐怖份子名單等資訊於相關業者間交換、通知等，即可能引發當事人報復等行動。本款事由該當性之有無，應依各個個案為全面之利益比較衡量後，以為決定。

(3)、因公共衛生、兒童之健全育成而特別有必要者：前者例如為疫學調查、傳染疾病之防治等，由醫療診所依法通報病患資料；後者例如兒童虐待、賣春問題之防止、救助，由學校、醫院或社福團體通報主管機關被害人之個人資訊等。

(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，且如須得到當事人同意將使協助或受託業務之遂行產生困難者。本款乃為協助行政機關遂行法定事務，而業者提供其所蒐集之個人資訊為不可或缺者，然業者如須取得當事人之同意，可能因當事人之人數眾多或者事實上有困難無法取得全數之同意者；例如，業者於自己營業店舖內設置監視攝影機，為協助犯罪

[122] 園部逸夫，同前註 29，頁 116。
[123] 園部逸夫，同前註 29，頁 117。

案件之調查而將所錄存進出顧客之影像提供檢警調查案件之用[124]。

凡該當上開四款適用除用事由任何之一者，業者即使未事先得到當事人同意，亦得為特定利用目的範圍外之個人資訊處理、利用。

### 第三項　關於個人資料之義務

業者進行個人資訊蒐集處理時，僅須依適當之方法蒐集，盡可能特定利用目的，並通知當事人或公告，基本上對當事人已有一定程度之保護，而此時個人資訊可能散存於各媒介物，未經整理、分析或編輯為容易檢索有體系之個人資料庫中。若業者為利用之便又進一步將其合法蒐集之個人資訊再經分析整理並編輯入個人資料庫，其可信度及有用性已大幅提高，又若業者所處理個人資料內容有誤、任意提供給第三人或未為適當管理以致於遺失或洩漏者，將使當事人權益受損；職是之故，本法自第 19 條至第 26 條即進一步關於構成個人資料庫之個人資料內容正確性及其安全管理措施等課予業者相關義務。

本次修法關於本節最主要重點在：對將資料提供給第三人時義務之增訂、確認請求資料之公開、訂正、停止利用等當事人之權利、不用資料之刪除及匿名加工業者之義務。其目的在消除個資法自來被批評之未充分重視當事人隱私權保護之缺失,故藉本次修法將個資法更明確定位在防止隱私權侵害之發生上,對有關個資處理業者，盡可能採取防止其侵害當事人權利之規範[125]。

#### 第一款　正確性確保義務

個人資訊經完成整理分析並編輯至個人資料庫後，因檢索容易，便於與其他個人資料比對、組合，利用性可能性增大，如內容不正確時，可能造成個人形象被扭曲或誤解，致其個人權益侵害，故本法第 19 條規定：於達成利用目的

[124] 岡村久道，同前註 5，頁 167。
[125] 森亮二，實務解說平成 27 年改正個人情報保護法（第 1 回），NBL，No.1059，2015 年 10 月，頁 6。

必要範圍內，業者應努力於保持個人資料正確且最新之內容。所謂「正確且最新」之內容，指資料內容與最新「事實」相符，如為對個人之評價、鑑定、意見等即無本條之適用[126]。又本條義務僅及「達成利用目的必要範圍內」;換言之，是否應為最新內容之個人資料，須依其利用目的決定之，並非所有個人資料均必須隨時更新為最新內容，例如已畢業學生在學紀錄，即無更新以符合當事人現況之必要。

又本條義務為「應努力」，為強制力弱之努力義務，其立法之理由為，所謂正確且最新內容之資料，通常只有當事人得知，一般業者常無確認之方法或手段，在判斷上多有困難，為避免造成業者過重之負擔，故本條僅為「努力義務[127]」。

另外，在本次修法於本條後段加入：已無利用必要之個人資料，應不得遲延努力予以刪除。原本個資處理業者蒐集所得之個資，於其所定之利用目的完成時，或已無利用必要時，如仍為將來可能有利用之必要而繼續漫然保存，實質上是違反本法第 16 條之超越特定目的範圍之違法處理行為,原應得要求其迅速刪除該當資料;然業者是否已達成利用目的或該當資料確已無必要?並未被課予應告知當事人之義務。且在現今雲端運算（cloud computing）普及、資通訊技術之發達，得廉價、簡單儲存並持續保有大量資料，而當事人對自己之資料可能被持續保有，存有高度之不安感，尤以消費者團體最在意此事[128]，因此本次修法特別增修本條。

### 第二款　安全管理義務

業者於處理、利用個人資料之過程中，最常發生之事故為資料之遺失、被竊或遭受入侵破壞，造成當事人損失，因此課予業者安全管理義務，係為防止

[126] 藤原靜雄，同前註 15，頁 79。宇賀克也，同前註 15，頁 97。
[127] 園部逸夫，同前註 29，頁 128。
[128] 宇賀克也，同前註 22，頁 47。日置巴美、板倉陽一郎，同前註 23，頁 71。

當事人權益受損所必要者；而所謂資訊安全（Information security）即為保護資訊之機密性（Confidentiality），確立只有被授權者得以獲取（Access）資訊；安全性（Integrity），保護資訊及其處理方法完全且確實；可用性（Availability），確保被許可利用之人，於必要時得獲取資訊及其關連資產，此為一般稱之「CIA」概念[129]。OECD 於 1992 年亦依此概念，針對資訊安全通過資訊安全指導原則[130]，因此本法自第 20 條至第 22 條課予業者下列保護個人資料安全管理等義務。本次修法此部分未作修正。

1、安全管理措施之確立：本法第 20 條規定：業者為防止所處理個人資料洩漏、滅失或毀損，應採取必要且適當之管理措施。然因處理個人資訊業者分屬不同業界，處理之個人資料性質亦千差萬別，故無法以法律統一訂出「安全管理措施」之具體內容，而僅能籠統以「必要且適當」之方式規範。學者據此解為應以：所處理個人資料之「重要性」，其安全管理上之「被威脅性」，對威脅性該當管理系統呈現之「脆弱性」，及防止外來侵害之「難易度」等要素作綜合考量，以判斷業者是否確立「必要且適當」之安全管理措施[131]。再查內閣會議通過施行本法之基本方針（下稱基本方針六），所定業者保護個人資料應採措施之基本事項(1)、②[132]揭示：業者應建構有防止來自外部不當獲取個人資料之防禦措施、設置個人資料保護管理人、管理內部員工接近及防止資料被擅自攜出之對策等內部安全管理體制；並於發生洩漏事件時，為防止損害擴大及迴避類似事件再發生，應儘可能公佈事件之事實經過。此外，對安全管理措施是否完善應作定期檢測，如有可能應請外部第三人對其進行安全管理之監督。

2、對從業人員之監督：業者固得建構並施行良好之安全管理體制及措施，

[129] 岡村久道，情報セキュリティ・マネジメントと法，関西情報産業活性化センタ情報セキュリティ・マネジメント研究会編「企業活動と情報セキュリティ」，2003 年，頁 93。
[130] 1992 OECD Guidelines for the Security of Information systems。
[131] 岡村久道，同前註 31，頁 219。名和小太郎，情報セキュリティ，みすず書房，2005 年，頁 16。
[132] 2004 年 4 月 2 日內閣會議議決。

但實際上之運作仍須依賴人；且自歷年洩漏個人資料事件觀之，行為人多即為業者內部之從業人員[133]；因此本法第 21 條規定：業者為謀求該當個人資料管理上安全，對處理個人資料之從業人員，應進行必要且適當之監督；揭示業者負有監督員工之義務，讓業者之安全管理義務得以落實。

本條所稱「從業人員」，係指於該當業者組織內部，受其指揮監督從事業務之人員；不問其與業者間是否有雇用關係，包括正職、兼職人員、派遣人員等[134]。

又本條所謂「監督」義務，除設置硬體上必要措施，另與從業人員訂立保密契約，於員工守則揭示保密義務，並定期對從業人員進行相關之教育研習等，以強化從業人員保護個資意識，慎重其職務之執行，均能有效防止或降低個人資料外洩事件發生。

3、對受託人之監督：於分工細密之今日，業者為降低成本及提高效率等，往往將蒐集所得之個人資訊以承攬契約委託給外部科技公司進行鍵入、編輯、製成資料庫、建立查詢系統等。而因承攬業務之承攬人故意或過失致使個人資料洩漏或毀損之事件亦時有所聞[135]；故業者之安全管理措施亦應包含其對承攬人之監督在內，安全管理措施始能稱為完備。故本法第 22 條規定業者將個人資料處理之全部或一部為外部委託時，對受託者應進行必要且適當之監督。

本條所稱「委託」係指業者將個人資料處理事務之全部或一部分以契約方交付他人進行，契約種類不限，可以為承攬、委任等；而所謂對受託者進行「必要且適切」之監督義務，一般而言自選任受委託人開始即應善盡注意義務，選擇適當之受託人或承攬人；其次，該當契約之內容必須具體載明應遵守之安全管理措施及責任分擔；查經產省 GLⅡ.2.(3)有關契約中應載明安全管理措施揭示如下列事項：(1)、防止個人資料之洩漏、禁止盜用；(2)、禁止為契約範圍外

[133] 參閱宇賀克也，同前註 15，頁 100 之資料。
[134] 園部逸夫，同前註 29，頁 131。經產省 GLⅡ，2，(3)。
[135] 青木耕一，企業による個人情報保護と流出対應，法律のひろば，2008 年 9 月，頁 37。

之加工、利用；(3)、禁止契約外之影印、複製；(4)、契約期間；(5)、契約終止後之個人資料之返還、消去、廢棄等事項。再實際上應採之措施，同 GL 則明定：關於個人資料處理狀況，受託人應向委託業者報告之內容及次數；確認遵守契約內容，如未遵守契約時之處置；發生安全管理事故時之報告、聯繫等事項，均為業者於委託時，應對受託人等進行之監督義務。

又因本條並未禁止「再委託」，故理論上受委託人可以再委託第三人處理被委託事務；但在此場合，可能使原委託之業者對再受委託人無法進行本條之監督，讓本條形同虛設；因此學者主張業者應於契約中禁止或限制再委託；縱使得再委託，業者對再受託人之選任及處理業務進行必要且適當之監督，亦應包含在業者依本條應負之監督義務內[136]。加之，轉委託之原受託人亦該當於本法之「處理個人資訊業者」，對受其委託之再受託人，仍應依本條負監督之義務；而再受託人實質上亦為「處理個資業者」，同樣應依前開第 20 條負安全管理義務，對其從業人員進行監督；從而形成連鎖義務[137]，故無強制禁止再委託之必要。

### 第三款　對第三人提供之限制

業者如得將蒐集處理之個人資料於未得當事人同意下任意提供給第三人，對當事人而言，其將不知自己資料之流向，無法掌握其利用方法，容易遭受不可預測之損害；且被提供之個人資料可能有被第三人予以違法加工利用之危險性，故原則上禁止業者將個人資料任意提供給第三人；究此行為之本質乃屬前述第 16 條「目的外利用」行為，亦為業者最常見之違法行為，為更周全保護當事人法特別再以第 23 條規範之[138]。但業者將個人資料提供給第三人者，常係基於不同之原因，有時是營業上有需要，有時為公益上之必要，不必然造成當事

[136] 園部逸夫，同前註 29，頁 134。宇賀克也，同前註 15，頁 103。
[137] 岡村久道，同前註 31，頁 231。
[138] 岡村久直，同前註 31，頁 241，園部逸夫，同前註 29，頁 136。

人權益受損；又若完全禁止提供給第三人可能減損個人資料之有用性，又與現在資訊社會廣泛流通運用資訊之實態未盡一致；再者，所謂「第三人」之規範為何易生爭議。從而第 22 條即針對「個人資料提供給第三人」要件之合理範圍予以明確之界定[139]。

## 第一目　原則

選擇加入－opt-in 制：本條第 1 項規定：業者除有該當為本項所揭示之例外事由外，如事前未得到當事人同意，不得將個人資料提供給第三人；一般稱此事前「選擇加入」－opt-in 制度，基本上事前當事人對資料之被蒐集、利用或消費者對受取業者發送資訊未予同意時，即不得為蒐集或送付之制度。換言之，對業者能否合法將個人資料提供給第三人，係以事前得當事人同意為原則。

本項之「提供」，指將該當個人資料置於第三人可能利用之狀態，雖僅供閱覽或置於電腦網站供下載者，亦應包含在內。而所謂「事先」係以何時點為基準？「提供第三人」如係業者原定之利用目的，又屬前述第 18 條 2 項所規定，以書面記載方式直接自當事人蒐集時，當然在蒐集時即應對當事人明示之，並在該當書面設置同意欄，以確認當事人同意。如依其他方式蒐集者，則以開始對第三人提供時為基準點[140]；換言之，只要在提供第三人前得到當事人同意即可，而經產省 GLⅡ.2.(4)亦為相同之解釋。

又本項列舉四款例外事由，業者如有該當其一者，即得不受本項之限制。1、基於法令者；2、為保護人之生命、身體或財產而有必要者；3、為提升公眾衛生或推展兒童健全育成而有特別必要時，且於得到當事人同意有困難者；4、對國家機關或地方公共團體或受其委託者遂行法定事務有協助之必要時，且得到當事人同意，將對該當事務之遂行有造成障礙之虞者。上述四款與前述第 16 條 3 項所定「目的外利用限制」之適用除外事由內容完全一致；因將個人資料

[139] 宇賀克也，同前註 15，頁 106。藤原靜雄，同前註 15，頁 88。
[140] 宇賀克也，同前註 15，頁 106。岡村久道，同前註 31，頁 214。

提供給第三人，本質上多屬目的外利用之形態，如依本項容許對第三人提供之例外事由與容許目的外利用之例外事由不相符或相互齟齬時，將使本法適用上發生錯亂。而有關本項四款例外事由之說明，請參酌本章第二節「四、(二)」之說明，在此不贅述。

### 第二目　加強要件之事後選擇退出－opt-out 制

只要當事人對自己資料之被蒐集或利用未行使拒絕權，即視為同意之制度，而一旦當事人表示拒絕即須停止蒐集或利用。此為日本特別之制度，有其社會及歷史背景。因日本係自 2005 年立法後開始規範民間部門處理利用個人資料，但事實上當時業者處理利用個人資料之狀況已非常普遍且行之有年，如此時再依本條 1 項要求在事先一律須得到資訊當事人同意，有其現實面之困難；且日本長久以來即有名簿業者、住宅地圖業者等以販賣個人資料為業之業者存在對增進個人資料之有用性、社會經濟之發展有一定貢獻[141]；為顧及渠等之生存，故作為第 1 項規定之例外，替代當事人同意之得合法提供第三人資料之要件，依本條第 2 項規定：業者對其提供給第三人之個人資料，依當事人請求停止對第三人提供；並事先將 1、提供給第三人之利用目的，2、被提供給第三人之個人資料項目，3、提供手段或方法，4、依當事人請求而停止對第三人提供，四項事項通知當事人或置於其容易得知之狀態者，即不受本條前項限制得將該當個人資料提供給第三人。換言之，業者於符合上述要件時，即使事先未得到當事人同意，仍得將個人資料提供給第三人；惟一旦當事人要求停止提供時，不問請求停止理由為何，必須無條件停止提供給第三人[142]；上述之選擇加入，係業者於事前先取得當事人同意後提供個人資料給第三人，如事後當事人要求停止提供時，因業者與當事人有契約、或準契約關係，除非業者違法，並不當然

[141] 園部逸夫，同前註 29，頁 150。例如日本各省廳職員名簿、國會議員名簿、紳士名錄等均在市面上公開販售。日本現行法律中有明文規定採 opt-out 制者，如特定電子郵件送信適當化法第四條(特定電子メール送信適正化法)；以及特定商取引法第十二條之 2(特定商業交易法)，有關廣告宣傳電子郵件之規定。

[142] 藤原静雄，同前註 15，頁 92。園部逸夫，同前註 29，頁 147。

有停止義務。故當事人一旦同意，日後反悔較難以補救，但至少是當事人預見之利用；而選擇退出制則是在建立事後當事人得有機會反映其意見之必要條件下，容許業者雖未於事先得到當事人同意，而得對第三人提供個人資料之制度；對當事人而言，雖得事後表示反對，但卻承擔未預見之風險，事實上較不利於當事人。

而上述「置於當事人容易得知之狀態」，之要件，法未規定其方法，業者得繼續揭載於自己網站上或事務所，事實上無法保障當事人充分理解其內容[143]。

且日本在 2014 年發生有名兒童教育出版事業(ベネッセ)之大量顧客資料，被維修電腦之派遣公司工程師以隨身碟下載後攜出，販賣給名簿業者再輾轉賣給其他業者利用之事件。突顯出雖形式上名簿業者已依法建置 opt-out 程序，但因其取得之資料原係來自於不法時所取得者，而又再轉賣他人者，實際上造成當事人無法行使其選擇退出之權利[144]。

故本次修法於 23 條第 2 項，特別對採 opt-out 制之業者加重其要件及建立由保護委員會監督之機制。亦即業者必須依保護委員會所定規則，將上述應通知當事人或置於當事人容易得知之四項事項，再加上第⑤之受理當事人請求之方法，成為五項事項，並須向保護委員會申報之。又於同條第 4 項規定，保護委員會於業者為前第 2 項之申報時，應將其申報事項連同業者之名稱，一併於委員會之官方網站公告之。如此之設計可以讓社會大眾得以掌握依 opt-out 制進行將資料提供給第三人之業者為何人，確認其實際運用狀況，而提高 opt-out 權利之實效性[145]。

### 第三目　第三人範圍之界定

所謂「第三人」如何界定？一般指原處理個人資料之業者及當事人以外之

[143] 瓜生和久，同前註 101，頁 75。
[144] 日置巴美、板倉陽一郎，同前註 23，頁 76。
[145] 日置巴美、板倉陽一郎，同前註 23，頁 77。宇賀克也，同前註 22，頁 52。

人，包括自然人、法人或其他團體；原則上總公司與分公司、加盟連鎖店相互間，屬同一事業集團之企業成員間，均被解為屬第三人[146]。立法限制業者將個人資料提供給第三人，係為防止當事人遭受不測之損害，但如業者與受提供之第三人得視為一體，或者該第三人及其利用目的為當事人得預知或掌握時，當事人不致蒙受不可預見之損害，且其相互間共有個人資料將有益於個人資料有用性之提高，增進企業經營之效率，故本條第 5 項特別明定下列三款非屬本條所稱「第三人」。

1、受託人：業者於達成利用目的之必要範圍內，將個人資料之全部或一部委託他人處理者，此受委託人非本項所稱之第三人，業者無須另行得到當事人同意。因高度資訊化之現今社會，企業往往大量收集、積存顧客資訊，為有效率將蒐集所得個人資訊整編成資料庫以供利用，而委託給專業之業者作鍵入、編輯等處理業務者十分普遍，如仍須一一再得到當事人個別同意，自時間及成本上考量，極不合理；另一方面依前述本法第 22 條規定，於委託外部處理個人資料時，業者必須負安全管理上之監督責任，以保護當事人，故本款將利用目的範圍內事務委託，視為業者處理個人資料業務之一部，其受託人非屬於第三人。

2、事業繼受人：現今企業常有事業之合併、分割、轉讓等事情，伴隨營業之移轉或繼受，被視為資產之顧客個人資料常也一併被移轉給合併或分割後新設或存立之業者，此時該當業者如被認定為「第三人」，即必須重新一一取得當事人之同意，將形成重大負擔，減損個人資料之有用性；再者，繼受事業之業者因隨事業移轉所受讓之個人資料，依本法第 16 條第 2 項，其利用仍被限制於繼受前該當個人資料利用目的範圍內，當事人受損害之危險性不致於提高，故本款明定繼受事業之業者，非屬本條所稱之第三人。

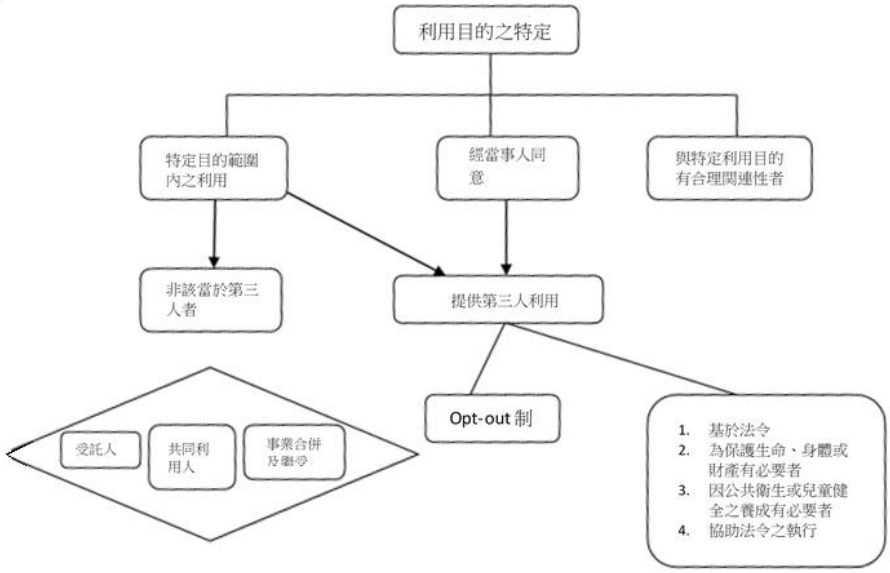
[146] 宇賀克也，同前註 15，頁 114。

3、集團間共同利用者：個人資料為特定人間所共同利用，並預先將此要旨、被共同利用個人資料之項目、共同利用者範圍、利用者利用目的及安全管理者責任之姓名等通知當事人，或置於當事人容易得知之狀態時，該當共同利用人亦非本條所稱「第三人」。常見之事例為金融、保險業者間為防止多重貸款或重複保險而交換彼此之客戶資訊；或與旅行業連鎖經營之餐飲、旅館、遊覽車業者間共有旅客資料；容許集團內之業者間共同利用顧客資訊，一方面有助於企業經營效率化得降低成本，一方面亦提升業界服務品質；且因事先已將「共同利用者範圍」、「利用目的」及「負安全管理責任人」之重要事項告知當事人，當事人仍得掌握自己資訊之流向及被利用狀況，尚不致遭受不能預見之損害，故本款亦將此類共同利用人排除於第三人之範圍外。

而上開「共同利用者範圍」，業者雖無須一一列舉，但仍須為客觀上可確定者，不得以「本事業集團」等籠統方式記載[147]。如事後有「利用者之利用目的」及「安全管理責任人」變更之事情時，依本條 5 項亦應於事先將變更內容通知當事人或置於當事人容易得知之狀態。但應注意本項不包含「共同利用要旨」、「被利用個人資料項目」及「共同利用者之範圍」之變更，其理由為：「共同利用要旨」之變更，本質上為解除共同利用關係之一種，此時該當業者間已非共同利用者，其為個人資料之提供時，應還原適用本條第 1 項須事前得到當事人同意，而無本項之適用；再「被利用個人資料項目」及「共同利用者之範圍」之變更，實質上已動搖前項容許「共同利用」不損害當事人為前提之信賴基礎，此時如僅為變更之通知或置於當事人容易得知之狀態顯有不足，仍應以再得到當事人同意較為妥當[148]。有關於個人資料之合法利用，以附圖四示之。

[147] 藤原靜雄，同前註 15，頁 97。宇賀克也，同前註 15，頁 115。岡村久道，同前註 31，頁 259。

[148] 夏井高人，個人情報保護第 50 条に関する要件事実論，判例タイムズ 1131 号，頁 68；鈴木正朝，同前註 24，頁 53。




## 第四款　資料追蹤履歷（トレーサビリティ **traceability**）之作成與確認

在現今資通訊科技發達之時代，個資流通管道多且快速方便，個資處理事業可自多方取得個資，再提供給他人，個資往往由數個業者經手利用，在資料流通之過程中如發生洩漏、或遺失之事故時，常很難確認問題出在哪一環節，以追究責任。又於未修法前，對不法流通之個資之規範，僅得依法第 17 條第 1 項適當取得資訊之規定規範之，如有違反者僅能依事業主管機關之監督及當事人請求停止利用以為救濟。且此時尚須取得個資之業者對自己取得之資料係不法之來源已有認知，否則亦難以課予任何法律責任。如前所述之ベネッセ事件，名簿業者即否認對該當資料為不法流出者有所認知，形成難以追究責任[149]。因此本次修法即針對如何抑止個資不法流通，及發生洩漏等不法事故時，能迅速掌握該當資料取得之通路以追究責任，特別增設第 25 條、26 條規定個人資料提供者及受提供者之記錄作成義務。

### 第一目　提供個人資料者

[149] 日置巴美、板倉陽一郎，同前註 23，頁 80~81。

依法第 25 條第 1 項，個人資料處理業者將個人資料提供給第三人時，應依保護委員會所定規則，將該當個人資料提供之年、月、日，該當第三人之姓名或名稱、及其他規則所定事項作成記錄。

1、適用主體：負有本項之義務者限於個資處理事業，「個人」並不包含在內，故個人不問提供或受取他人個資，均無本項之適用，但如個資處理事業受「個人」提供其當事人以外他人之資料時，則仍應負本項義務[150]；此處之第三人不包含第 2 條第 5 項之國家機關、地方自治團體及獨立行政法人等。

2、記錄之內容：除該當個人資料提供之年、月、日，該當第三人之姓名或名稱外，雖保護委員會之規則尚未明確定出其他事項，但應是包含所提供個資之類型、包含之項目等[151]。

3、記錄之保存：依本條第 2 項，自前開記錄作成之日起，應依保護委員會規則所定期限保存之。

**第二目　受個人資料提供業者之義務**

接受第三人提供個資之業者，於接受時依法第 26 條，應負有下列義務。次處「第三人」包括個人在內，如該當資料之提供人如為第 2 條第 5 項之國家機關、地方自治團體等，則無本條之適用[152]。

1、確認義務：依本條第 1 項，受資料提供業者應依保護委員會規則進行 下列事項之確認：(1)、該當提供人之姓名或名稱及住所，如為法人時，其代表人或非法人團體時之代表人或管理人。(2)、該當提供人取得該當個資之經過。所謂取得該當個資之經過，是指提供人自何人、以如何方法取得被提供個資之事實；確認之範圍則僅限於自己之前手，並非該當個資全部之轉手紀錄，因提供

[150] 瓜生和久，同前註 101，頁 93。
[151] 日置巴美、板倉陽一郎，同前註 23，頁 82。
[152] 宇賀克也，同前註 22，頁 53。

人通常僅知自己取得該當個資之經過，且如各個受提供之業者均已如實確認時，亦得掌握該當個資之轉手經過，不致造成業者過重之負擔[153]。

2、記錄作成：依本條第 3 項，受個人資料提供業者於依本條第 1 項進行 確認時，應依保護委員會規則作成取得該當資料之年月日、所進行之確認事項及保護委員會規則訂其他事項等記錄。

3、記錄保存：依本條第 4 項，自前開記錄作成之日起，應依保護委員會規則所定期限保存之。

如上述，本次修法已建立業者自搜集個資至提供個資之全程記錄制度，依此完整記錄，得追蹤個資流通之每一個階段，一旦有洩漏遺失之事故時，得容易查知何階段出問題，亦得抑止個資之不法散布。但如此立法被指摘之問題為是否會造成處理個資業者之過重之負擔[154]？依本法案於國會審議時內閣委員會之答詢，說明以：如為同一事案、當事人間，反覆、繼續為同種類個資之提供者，例如信用卡、水電費等支付扣款之提供利用，僅需為包括性之記錄，無需對各個供取行為作詳細記錄。又記錄之方法，如該當個資供取行為為於網路線上進行者，則無需另行作成記錄[155]。關於此部分之具體對應作法，尚有待保護委員會進行討論後在決定之。

### 第五款　對國外之第三人提供資料

原未修正前個資法並無相關之規定，但因日本企業活動已地球村化，又伴隨資訊科技發展電腦網路之普及，個資之跨國傳遞日益頻繁，必須建立法制以為規範；再者歐盟指令第 25 條對加盟國對其他非加盟國傳遞個資時，需符合其「十分性（adequate）」之要件，日本因欠缺此部分之規範，被認為係被歐盟認定不符合十分性要件之原因之一。因此本次修法即於第 24 條新增跨國傳遞個資

[153] 瓜生和久，同前註 101，頁 95。日置巴美、板倉陽一郎，同前註 23，頁 83~84。
[154] 関啟一郎，前揭 45，頁 13。日置巴美、板倉陽一郎，同前註 23，頁 83。
[155] 日置巴美、板倉陽一郎，同前註 23，頁 83。関啟一郎，同前註 45，頁 13。

之限制[156]。依第 24 條規定之要件，跨國傳遞個資須符合下列兩種情況之一者，始得為之。

（一）外國第三人之條件：此部分又須滿足二個要件：

1、該當外國之個人資料保護法制，被認定為與日本有同等水準，而為保護委員會所指定者。此被稱為「同等性認定」國要件，為由保護委員會定立規則，負責對該當外國之個人資料保護法制水準進行判斷。

2、受資料傳遞之外國第三人，須符合本法第四章第一節，對個資處理業者所規範之處理個資時，為符合保護委員會定立之基準，所應具備之採繼續性措施體制，此稱為「基準符合體制」要件[157]。

（二）事先得到當事人之同意：但如依前述同法第 23 條第 1 項，因基於法令之規定等事由提供時，得不經當事人之同意。

### 第四項　匿名加工業者之義務

#### 第一款　匿名加工業者等之義務

如前第二章第二節第二項所述，對於業者匿名加工之規範，已在技術面訂出除去特定個人識別性之基準外，因加工匿名之業者手中仍握有原始個資，如單只依其內部規程禁止再組合比對回復特定個人識別性，實難以防止弊端。又即使匿名加工業者已依基準所定方法進行匿名加工，然如其將匿名加工資料提供給第三人利用時，如前述此時對個資之識別性為採「提供人基準說」，故對該第三人所具有之資訊技術，及其手中是否有其它得組合、比對之消費者其它資料，事實上均為提供者所無法預知之事；尤其現在因社群網站及智慧型手機利用普及，在網路留存有大量個資，加上搜尋引擎網站資料搜索功能強大，形成

[156] 日置巴美、板倉陽一郎，同前註 23，頁 140。関啟一郎，同前註 45，頁 15。
[157] 日置巴美、板倉陽一郎，同前註 23，頁 141。関啟一郎，同前註 45，頁 15。

即便是匿名資料仍留存有與他資料得為組合、比對而被還原之危險性[158]。因此為更周全保護資料當事人，且為建立社會大眾之信賴度，故除對匿名加工方法在技術面予以規範外，尚須以法律定明如下匿名加工業者及受匿名加工資料提供者應負擔之法律義務，並要求匿名加工資料利用過程之透明化。

### 第一目　禁止再識別義務

依修正後法第 36 條第 5 項:個資處理業者作成匿名加工資料而自己為該當資料之利用時，不得為識別出該當匿名加工資料之當事人，而將該當匿名加工資料與其它資料為組合、比對。而受匿名加工資料提供之業者，依同法第 38 條亦不得為識別出特定個人，而取得自該當個資中被刪除之記述等，或個人識別符號，或是作成匿名加工資料之方法等資料，換言之，進匿名加工之個資處理業者與接受匿名加工資料之業者，均不得進行回復該當資料個人識別性之行為。

### 第二目　公開義務

為取得消費者之信賴及讓社會大眾安心，匿名加工業者尚必須將其作成匿名加工資料之事情透明化。依修正後第 36 條第 3 項其必須公開下列事項為,1、個資項目：匿名加工業者應依保護委員會規則規定，公開包含該當匿名加工資料中個資項目（如利用日時、年齡、性別、居住都、道、府、縣、購入商品項目等）。2、提供第三人之個資項目及方法：依同條第 4 項規定，個資處理業者作成匿名加工資料，並將其提供給第三人時，應依保護委員會規則規定，預先將包含於匿名加工資料中之個資項目及提供方法公開之。3、再提供之公開義務:接受匿名加工資料提供之業者，又將該匿名加工資料提供給第三人時，應負與前 2 項相同之義務。建構一套將匿名加工資料之內容、加工方法、流向、全部予以透明化之完整規範；一方面當事人可掌握自己個資被蒐集、處理及利用之

[158] 小林慎太郎,「匿名加工情報」によるビッグデータビジネス活性化への期待と課題，知的資產創造，2015 年 10 月号，頁 31。

全部過程，另一方面社會大眾亦得知該匿名加工資料之作成與運用，應較能防止弊端發生。

### 第三目　明示義務

依同條第 4 項，個資處理業者作成匿名加工資料且將之提供給第三人時，應依保護委員會規則規定，事先對該當第三人明示所提供之資料為屬匿名加工資料；若受提供者又將該當資料再提供給其他業者時，亦負相同之義務。此乃考量後提供資料業者若不知受領之該當資料為匿名加工資料時，恐有不遵守有關匿名加工資料法定義務之虞。而此處之「提供」不僅止於對特定人之交付，即便公開於網頁供人利用者亦同[159]。

### 第四目　安全維護義務

原本匿名加工資料，其經加工後個人識別性已去除，且不得回復為原個資，如洩漏或被違法利用，並不致於直接使用個人權利利益受損；但如前所述其仍有與其他資料組合、比對之可能性，或加工方法可能被破解之危險存在，故依第 36 條第 6 項個資處理業者對該當匿名加工資料之安全管理，有致力於採取必要且適當措施並公告該措施內容之義務；而依第 39 條，接受匿名加工資料之業者，亦負相同之義務。

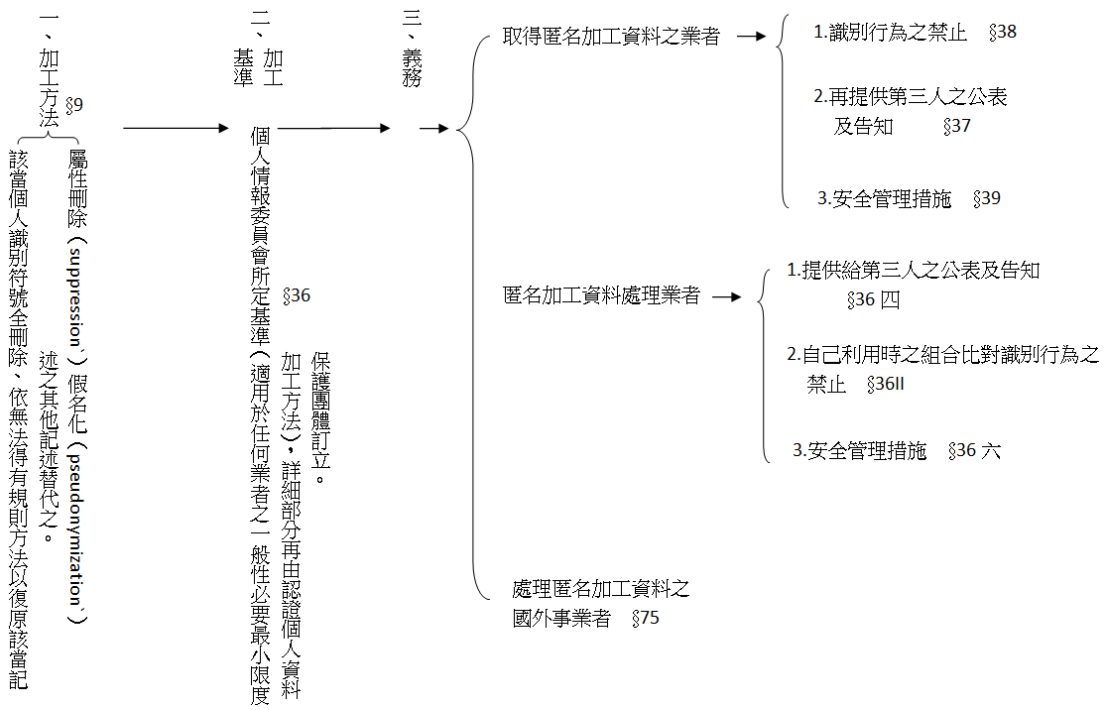
## 第二款　國外處理匿名加工資料業者之義務

因修正法第 75 條所規定法之施行範圍，於對國內之人提供物品或服務，而取得當事人個資之個人資料處理業者，即使是在國外處理該當個資或利用該當個資所作成之匿名加工資料，亦有前述第 35 條、36 條適用；故直接自當事人取得個資者，即使在國外所為之利用或進行匿名加工，因考量關連日本國內人民權利利益之保護，故亦應受本法之規範。另一方面如此國外之業者非為

[159] 宇賀克也，同前註 72，頁 43。

自當事人，而係從其他之業者取得匿名加工資料者，則無本法之適用。

下附圖五為匿名加工時，業者所應遵守之法定義務：




如前所述匿名加工資料為依個人情報保護委員會規則所定方法，加工於個資使其失去特定個人識別性，且無法復原者，因此匿名加工資料原已不屬於個資法中之個資，從而對匿名加工資料為蒐集、處理及利用者，除負有前述第 36、37、38、39 條之義務外其餘個資法規定即無適用之餘地。換言之，個資處理業者無須得到當事人同意即得將匿名加工資料提供給第三人，或得變更其原定之利用目的[160]利用於其他目的上，因此得開展匿名加工資料活用之途。

## 第三款　檢討

### 第一目　複雜之義務構造

日本個資法之立法方式將保護客體分成「個人資訊」、「個人資料」、「保有個人資料」，及匿名加工資料之等四種，前三者以層級漸進方式課予業者由輕至

[160] 森亮二，同前註 45，頁 82。

重之義務，雖然可緩和一部分業者之負擔，但一方面卻造成法律責任構成複雜，增加適用法律之困擾；尤其對一般人而言，造成理解上之困難。又所課予業者之義務中有具強制力之「作為義務」，亦有不具強制力之「努力義務」，當然其理由多說明為減輕業者之負擔，究其原因恐怕仍是意圖以一總則性規定，將處理個人資訊數量及性質可能相去甚遠之各種業者，均包括在法適用射程內實有困難，因此只能定最低義務標準，再由保護委員會訂出更具體嚴格之規則，並作為解釋及適用本法之準則，故吾人在研讀日本個資法時，除本法規定外，尚須查明保護委員會規則，甚至該當業界之自訂之自律性指針，始能得其業者義務規範之全貌；此亦增加日本保護個人資訊法制之不透明性，事實上降低人民對本法之信賴，不利於法之推行。

### 第二目　事件通知及揭露義務

雖前開意見書未提及，但亦應為現行法須增訂者，尚有業者之事件揭露通知義務；當處理個人資訊業者發生個人資訊被竊取或洩漏之事件時，該業者應負有立即向主管機關為事件之通告，通知當事人並揭露事件經過之義務；因發生事件之業者，唯恐自己商譽受損或遭受指責、求償，往往隱匿不揚，直至當事人或社會大眾知悉時常為時已晚，被竊取或洩漏之個人資料已被廣為傳遞、利用，使當事人損失擴大，尚有接受不法個人資料提供之善意第三人發生；因此業者於事件發生時應即時通告主管機關擬定防止損害擴大之對策；並通知當事人，讓其有應變之準備，避免二次受害；同時揭露真相讓大眾知悉，減少善意第三人之受害；且因事件經過之披露，讓其他業者記取教訓，避免類似事件重複發生。日本現行法僅於基本方針六(1)、①及金融業之 GL 第 22 條對此有相關規定[161]，本法則付之闕如；鑑於上述事件揭露及通知之效用，應負擔此義務之業者應係全體業者而非僅限於金融業者，且不僅止於公布事件之發生，更應

[161] 淺井弘章，個人情報保護法と金融実務（第三版），金融財政事情研究会，2006 年 6 月，頁 136。

通知當事人，現行法實應增訂該當之義務條款，以彌補不足。

## 第五節　當事人權利之確立

有關個人資料之處理，為確保其透明化，除業者應負通知、公告等義務外，尚應讓當事人有適當參與之權利，基此，本法自第 27 條至 33 條明定，業者持續六個月以上「保有個人資料」時，當事人得請求業者提供閱覽、訂正、停止利用等。

### 第一項　修法前之爭議

因本章章名為「個人資訊處理業者之義務」，係以業者之法定義務為主軸，而非以當事人為權利主體之立法方式，故其相關條文規定為：「有當事人請求閱覽、訂正得識別該當當事人之保有個人資料時…」；設該當業者不依當事人之請求履行法定之義務時，當事人是否得依本法逕行提起訴訟請求救濟？主張「權利肯定說」之學者以：本章立法雖以業者義務為主軸，但自保護當事人之立場而言，本法立法本旨亦為實現「自我資訊控制權」；且業者義務與當事人之權利原為一體之兩面，故當事人應得依本法對業者提起訴訟要求履行本章義務[162]。但採「權利否定說」者，則以現行法第 1 條立法目的規定中，並未明定保護個人之「自我資訊控制權」，且本法本章立法方式係以規範業者之義務為主軸，重點在於主管機關對業者之行政監督與規制，非為業者與當事人間權利、義務之規範；故當事人對業者處理利用個人資料有不服而申訴時，應先由業者自律性自行處理，未能解決或無結果後，始由事業主管機關以勸告、命令等行政處分介入，督促業者履行本章義務；且個人之「自我資訊控制權」其外延內涵至今學界尚未有定論，本法自不宜貿然承認之；因此當事人不得依本章之規定，逕行起訴請求該當業者履行義務[163]，實務上亦採否定說[164]。然此亦未符合歐盟指

[162] 藤原靜雄，同前註 15，頁 95。宇賀克也，同前註 15，頁 116。
[163] 岡村久道，同前註 31，頁 239。夏井高人，同前註 148，頁 68。
[164] 東京地院平成 19 年（2007 年）6 月 27 日判決，判例時報 1978 號，頁 27。東京高判平成 27 年（2015 年）5 月 20 判決，平成 20 年(2008 年)(ネ)第 5348 號。

令第 22 條，個資處理業者如未履行法定義務時，當事人得依司法程序請求救濟之規定，而被認定為日本不符合前述「十分性」之原因之一，故本次修法特別於第 28 條、29 條、30 條確立當事人之請求閱覽、訂正、停止利用之權利[165]。

## 第二項　相關事項之公告

為使當事人能有效參與個人資料處理過程，並保障業者處理過程之透明化、公正性，其前提為自始讓當事人知悉自己個人資料依何利用目的？由何人處理、其狀況為何？因此本法第 27 條第 1 項規定：業者關於保有個人資料，應將下列事項置於當事人得知悉之狀態（包含應當事人請求而迅速予以回答）：1、該當業者之姓名或名稱；2、所有保有個人資料之利用目的，但依同法第 18 條第 4 項第 1 款至第 3 款規定，豁免業者對當事人通知利用目的者，則不在此限；其豁免業者本項義務之理由，請參閱本文前述第四章第二節「三、(三)」，此不贅述。應注意者，本項並未將第 18 條第 4 項第 4 款之「自取得狀況觀之，其利用目的被認為係明確者」，列為適用除外事由；此乃因本項之義務為繼續一定期間保有個人資料業者義務，而非取得個人資訊時業者之義務，且「取得時」與其後之「保有時」之業者及其利用目的未必一致，故無法免除其公告義務[166]；3、當事人依本條第 2 項要求通知利用目的，依同法第 28 條第 1 項請求提供閱覽、依同法第 29 條第 1 項請求訂正、依同法第 30 條第 1 項要求停止利用或提供第三人時，其處理之程序；4、除前三款所揭示者外，依政令規定有關確保保有個人資料適當處理之必要事項；據此本法施行細則第 5 條規定之必要事項為：①、關於該當業者保有個人資料當事人不服時之申訴處理窗口；②、該當業者為認定個人資訊保護團體之成員時，該當認定個人資訊保護團體之名稱及申訴之提出窗口[167]。

---

[165] 宍戸常寿，同前註 26，頁 41。関啟一郎，同前註 45，頁 14。

[166] 宇賀克也，同前註 27，頁 136~137。日置巴美、板倉陽一郎，同前註 23，頁 88~89。

[167] 認定個人資訊保護團體為推動民間事業者自律性的遵守個資法，由民間事業者團體以個資法為基礎，自己訂立之處理個資規則，藉團體自治方式確保事業者適當的處理個資，同時因處

本項所謂「置於當事人得知之狀態」，依經產省 GLⅡ1.(2)，係指於網頁上揭載、散發手冊，應當事人要求之即時回應等，只要當事人欲知悉時即得有知悉之方法及管道。又因其規定為「狀態」，故僅曾於公報、新聞或網路上通知過仍有不足，應繼續經常性保持得獲取之狀態。至於包含「應當事人請求而迅速予以回答者」，係考慮對規模較小之企業，一律要求其在網頁上常時揭載，或在營業處所備置手冊等，可能形成過重之負擔，故變通得以個別通知當事人方式以履行本項義務。

### 第三項　應當事人請求之通知義務

前項利用目的之公告，主要是針對業者所保有之個人資料所定之義務，因業者為利用、檢索之便利性多將個人資料經整理編輯成一個資料庫，故常以資料庫為單位做複數利用目的之公告，而非針對特定個人資料之利用目的為告知，當事人可能無法確知自己個人資料之利用目的；為補前項之不足，本條二項規定，當事人要求業者通知其保有得識別該當當事人個人資料之利用目的時，應通知當事人不得遲延。但如業者所為前項之公告，已明確告知該當當事人利用目的時，即無須再依本項規定特別通知特定當事人。又如對特定當事人為利用目的之通知，而有本文第四章第二節「三、(三)」所說明之依本法第 18 條第 4 項第 1 至第 3 款之利用目的通知，有損害當事人或第三人生命、身體、財產，其他權利利益之虞者等之適用除外事由時，該當業者應當事人請求通知利用目的之義務亦得免除。

### 第四項　當事人之公開請求

依修正後法第 28 條第 1 項，當事人得對個資處理業者請求閱覽所保有得識別該當當事人個人資料。，應依政令所定方法公開（包括通知該當個人資料不

---

理個資與當事人發生紛爭時，亦由事業者自己本身建構處理機制；因此個資法設計「認定個人資訊保護團體」制度，以事業者自己組織民間團體，在取得事業主管機關之認定後，協助各成員事業者訂立處理個資之規則，提供資訊，舉辦個資保護之研修及處理成員事業者與資訊當事人之申訴案件，希望以團體自律自治方式，推展個資法之施行。

存在之說明），不得遲延。此處所謂「閱覽」，當然於被請求業者確實保有該當個人資料時，除有本項例外規定得不提供閱覽之事由外，自應迅速提供當事人閱覽；對當事人而言，該當業者是否保有自己個人資料亦為其保護權益所應知悉者，從而本項明定於業者如未保有或該當個人資料不存在時，業者應將此事實「告知」當事人。

又提供閱覽方法屬細節性、技術性之事項，且隨今後科技通訊技術之發展，將得以更迅速、靈活應對，故本項提供閱覽方法為依政令規定；而本法施行細則第六條則規定，原則上以交付書面方式為之；如得到請求者之同意時，亦得依雙方合意之方法進行。總言之，提供閱覽之方法不僅只考慮當事人之便利性，業者之成本負擔及技術上之安全性亦須納入考量[168]。

對當事人提供閱覽所保有之個人資料，固為保障當事人之權益，但對當事人公開與其它應保護之利益衝突時，則應有所調整；而本項以但書規定：1、「有危害當事人或第三人生命、身體、財產及其他權利利益之虞時」；例如被請求閱覽個人資料為當事人罹病之事實或痊癒之可能性，當事人知悉則可能造成精神上痛苦；或其中包含第三人資訊，其公開將使第三人（如器官捐贈人）隱私權受侵害時，業者即得不提供閱覽。2、為「對該當業者業務之適當施行造成顯著障礙之虞時」，例如該當個人資料中包含有人事考核等評價資訊時，一旦公開將使業者之正常人事管理事務運作發生顯著障礙者。或當事人對同一內容個人資料反覆請求公開，明顯為惡意濫用權利時，亦有本款之適用。3、「違反其他法令」者；例如請求閱覽當事人通話紀錄，而其發話對方為保密電話時，電信公司如公開其號碼時即違反電氣通訊事業法第四條祕密通訊保護之規定等三項事由，亦得拒絕提供當事人閱覽。

又依同條第 3 項：業者基於前項規定對其保有個人資料之全部或一部分為

[168] 園部逸夫，同前註 29，頁 159。

不提供閱覽之決定時，應將其決定內容通知當事人不得遲延。

### 第五項　當事人訂正之請求

當事人請求訂正個人資料內容與前述請求公開相同，均為有效確保資料內容正確所必要之手段。本法第 29 條第 1、2 項規定：當事人以該當業者所保有其個人資料內容與事實不符為理由，要求訂正、追加或刪除時；除其他法令有特別規定之程序外，業者應於達於利用目的之必要範圍，進行必要調查並依調查結果追加或刪除該當個人資料內容，不得遲延。該當業者決定為全部或一部之訂正等決定時，或決定不為訂正等決定時，均應通知當事人不得遲延。

本條規定當事人得要求訂正等「理由」為，該當個人資料內容「與事實不符」；換言之，得要求訂正等對象限於「事實」部分而不及於「評價」、「診斷」或「意見」。但評價或意見等通常係根據事實而來，常為一體難以區分，且事實更改連帶「意見」或「評價」必須隨之更改，但本條更改對象限定為「事實」，在今後法之適用產生爭議之可能性極高[169]。

本條所謂「訂正」係指改正錯誤資料；「追加」則指添加不足之資料；而「刪除」係指除去不要部分。而請求之當事人必須合理、客觀說明「內容與事實不符」之理由，如未說明時，業者得不予調查，亦無須回應請求人之請求。若業者於調查後仍為真偽不明之狀態時，雖無須依本條訂正內容，但應於該當個人資料上附記此一事實[170]。又調查後不問決定是否訂定，均應通知當事人，如為訂正決定等時，其訂正內容亦應一併通知當事人。

### 第六項　當事人請求利用停止及消去

依本法第 30 條第 1、第 2 項規定於業者 1、違反本法第 16 條為超越特定利用目的為個人資訊之處理時；2、違反第 17 條以詐欺、其他不正當方法蒐集個

[169] 藤原靜雄，同前註 15，頁 104。
[170] 多賀谷一照，個人情報保護法，頁 128，弘文堂，平成 17 年。藤原靜雄，同前註 16，頁 105。

人資訊時；3、違反第 23 條第 1 項或第 24 條規定，未得到當事人同意將個人資料提供給第三人時；當事人得請求該當業者停止利用或消去該當個人資料，或停止對第三人提供；而業者認為當事人請求有理由者，於改正違法行為之必要範圍內，應先行為該當保有個人資料之停止利用等，不得遲延。

上述三項請求停止利用等理由中，並未含違反本法有關安全管理措施義務（第 20 條至第 22 條），其理由為：有關資料安全措施之內容，如承認當事人亦得參與表達意見，反而對安全管理目的之達成造成困擾；且安全管理義務係業者整體處理保有個人資料之問題，亦不適合由特定個人參與[171]。

本條中所謂「利用停止」，學者認為只要對違反義務部分停止利用即可，並不須保有個人資料全部停止利用。而停止對第三人提供，亦於收到於當事人通知後停止即可，無須將過去之提供收回[172]。另所謂「消去」係指將保有個人資料之全部或一部進行物理上處理成為無法復原再使用之狀態。本條與前條請求訂正等不同，並未規定業者有調查義務，此乃因有無超越特定利用目的利用或是否違法蒐集個人資訊，係業者自身施行之事務，乃無須調查或容易調查即自明之事實。

如已出版上市個人資料（名簿或 DVD）中僅有少數一部分為不正當蒐集者，而必須消去或停止利用，或停止對第三人提供時，可能有事實上之困難，或是需要龐大費用，為解決此一問題，本條一、二項但書規定，業者得採保護當事人權益之替代措施而暫時免除利用停止等義務；例如以金錢賠償當事人心理上、經濟上損失，並約定於日後再出版、發行時定予以修正[173]。

### 第七項　理由之說明

業者依本法第 27 條拒絕通知當事人個人資料之利用目的，依第 28 條第 2

[171] 參酌參議院會議記錄平成 15 年(2003)5 月 13 日（第 3 號），細田博之國務大臣之答辯。
[172] 園部逸夫，同前註 29，頁 174。
[173] 多賀谷一照，同前註 164，頁 129。岡村久道，同前註 31，頁 271。

項拒絕公開保有個人資料，依第 29 條第 2 項拒絕為資料內容之訂正等，或依 30 條第 3 項拒絕停止對第三人提供個人資料時，均應依本法條規定對請求之當事人說明其理由。

## 第六節　監督與救濟機制

### 第一項　團體自律性監督

第一目 認定個人資訊保護團體（下稱個資保護團體）之推廣

日本個資法立法時，有關對民間規範之設計，立於 1、個資之蒐集處理原屬當事人與業者間之事務，依私法自治之原則，故希望依約定確保其適法性；2、民間事業蒐集處理個資，性質、目的不同、方式亦有異，故法原僅能作泛用性、最低限度之規範，為謀求法規範之義務能被適當、確實遵守，希望各業界以法所定義務為基礎，依據其蒐集處理個資，性質、目的、方式進一步自定出適合其實務上運用之細節性規範，藉團體自律方式自發性合法、適當處理個資[174]。本法特別設計「認定個人資訊保護團體」之制度，由各業界、業者自主組織之民間公益法人團體，於經中央事業主管機關，修法後之保護委員會認定後，得依其所屬業界處理個資之種類、方式，以保護委員會所頒佈之 GL 為藍本，訂立更具體、詳細之個資處理規則「個人資訊保護指針」供其團體成員共同遵守；此外於業者與當事人間為個資處理發生爭執時得介入斡旋，擔任裁判外紛爭處理之任務；因此現行法第四章第二節，修法後之第四章第四節，設置「以民間團體推進個人資訊保護」之規定，建構以同業團體力量確保其成員適當處理個資為業務目的之民間團體認定制度，期於建立社會對其信賴後，有助於民間團體之自律確實發揮作用。至 2016 年 1 月為止，自金融、醫療、資訊通訊至婚慶喪葬業等，受認定之團體共有 42 個[175]。

[174] 日置巴美、板倉陽一郎，前揭 23，頁 128。
[175] 參見個人情報保護委員會官方網頁 www.ppc.go.jp/files/pdf/personal_nintedantai.pdf，最後瀏覽日 2016 年 8 月 25 日。

第二目 資格之認定取得

一、資格：申請認定之個資保護團體依第四章第四節 51 條第 1 項，可分為二種類型之團體，一類為以處理個資業者所屬業界為單位(例如銀行業界)所設立之業界團體、連合會等(例如全國銀行個人情報保護協議會[176])，通常由原已存立業界團體本身提出申請受許可認定後成為「個資保護團體」，而其原構成會員業者即為其業務對象。另一類為橫跨各業界訂立出個資保護共同規則，並對符合其標準之業者授與隱私保護認證標章之團體(例如財團法人日本情報處理開發協會，一般稱為 JIPDEC)，其成員為同意成為其認定業務對象之個資處理業者。申請取得認定為個資保護團體，依本節第 47 條規定並不一定須具有法人資格，僅設有代表人或管理人之非法人團體亦得申請認定。

二、認定取得：欲設立認定個資保護團體者，應依保護委員會所定申請程序，向其提出申請；保護委員會應依第 49 條進行審查申請者符合第 47 條第 1 項所規定之：1、訂有適當且確實進行其業務所必要之施行方法；2、具有適當且確實進行其業務之足夠知識、能力與管理之基礎；3、於進行認定業務以外之其他業務時，不因此而造成認定業務有不公平之虞等三要件，如確認滿足上述三項要件時，且無該當於第 48 條所定之消極資格者[177]，即為許可之認定，並在保護委員會官方網站公告其名單。

三、業務：取得許可認定之個資保護團體，依本節第 47 條 1 項規定得進行下列三項業務:㈠處理有關其會員或構成員業者在處理個資上發生之申訴事件；

[176] 為平成 17 年（2005 年）4 月 15 日，以銀行、長期信用銀行、銀行控股公司、全國各地銀行協會及全國銀行協會為會員，受主管機關認定所成立之個人資訊保護團體。

[177]第 48 條 （失格條項）
有該當於下列任何一項者，不得為前條第 1 項之認定。
一、依本法規定被科處刑罰，其已執行完畢，或未受執行之日起，未經過二年者。
二、依第 58 條第 1 項規定被撤銷認定，自其撤銷之日起，未經過兩年者。
三、執行其業務之董、監事（包含非法人團體設有代表人或管理人者，其代表人或管理人。以下在本條亦同。），有該當於下任何一項事由者：
1.被處徒刑以上之刑罰，或依本法規定被科處刑罰，自其刑執行終了，或為受刑罰執行之日起，經過二年者。
2.依第 58 條第 1 項規定被撤銷認定之法人，自撤銷之日前三十日以內，為其董、監事者，自撤銷之日起未經過二年者。

㉡提供有助於會員業者適當處理個資之相關資訊；㉢其他協助會員業者適當處理個資之必要業務(例如提供研習、收集資料、辦理宣導活動等)。以下就其重要之兩項業務說明之。

1、申訴之處理：依第 52 條規定，資訊當事人或關係人對其會員業者處理個資有不滿而提出申訴時，該當個資保護團體須因應其訴求，提出必要之建議；並於調查申訴事實之同時，將申訴內容通知該當會員業者，要求其迅速解決。又個資保護團體為解決前述申訴事件於必要時，得對該當會員業者要求提出文書或口頭說明或資料；而該當業者對上開要求，如無正當理由不得拒絕。依此規定個資保護團體有義務受理申訴並迅速處理。又為確保其有效處理申訴事件，本條規定再賦予其對會員業者有要求說明之權及資料提出請求權。

2、個人資訊保護指針(下稱保護指針)之作成：為讓個資保護團體有效幫助其會員業者能確實遵守本法規範，適當處理利用個資，發揮其團體自律機能，法第 53 條規定：個資保護團體應依本法規定意旨，應努力作成並公表包含特定利用目的、安全管理措施、本人申訴處理程序、匿名加工資料作成方法等事項之「保護指針」；並對團體會員業者進行遵守指針所必要之指導、勸告及其他輔助措施。此指針之性質相當於該業者團體處理個資之 GL，讓同屬相同業界之業者有一具有明確性、一致性以適當處理個資之規範。又保護指針之作成，如本章第二節第二項第二款第二目所述，為採利害關係人參與程序之理念，故保護指針之作成依第 53 條之規定，須聽取消費者代表及其他關係人之意見，以確保指針作成之公正性與提升社會之信賴度[178]。

保護指針作成後，依第 53 條第 2 項規定，個資保護團體應依保護委員會規則，向其申報提出，不得遲延。再依同條第 3 項應將該當保護指針依保護委員會規則公告之。

[178] 日置巴美、板倉陽一郎，同前註 23，頁 131。宇賀克也，同前註 22，頁 42。

四、信賴度之提高與保護委員會之監督：又為提高國民對個資保護團體之信賴，充分發揮其功能，在消極面尚有第 54 條規定：個資保護團體於進行認定業務時所獲知之資訊，不得供認定業務以外之目的使用。如有違反者，保護委員會得撤銷其許可認定。第 55 條規定：其他非個資保護團體，不得使用個資保護團體名稱或可能使人誤認之名稱，以保護資訊當事人或消費者，並防止惡德業者冒用名義進行非公益活動。

在積極面上，保護委員會對個資保護團體有以下之監督權限，即依第 56 條規定：保護委員會於必要時，得對個資保護團體要求提出有關認定業務之報告；又為擔保此報告要求權之效力，本法於第 85 第 2 款條規定，如該當個資保護團體不為提出，或為虛偽報告者，將被處以三十萬元以下之罰金。除此之外，有必要時，得再依第 57 條命令個資保護團體，改善認定業務施行方法、變更個資保護指針及採取其他必要措施。且於該當個資保護團體不遵從上開命令時，得依第 58 條第 4 款撤銷其認定，以確保本條命令之效力。

綜上可見，日本個資法希望以團體自律、自治方式確保各個業界業者適當合法處理個資；因業者為維護自己商譽，在其所屬業界保有生存空間，就必須遵守團體之規則，否則難以獲得同業間支援，甚至受到排擠。以讓業界自律方式，彼此互相發揮監督力量，一方面可以讓各業界依其處理個資之性質及方式，自訂出符合實際需求之處理個資具體規範；一方面亦可避免公權力過度介入業者經營自由，主管機關退居於第二線進行監督即可。

## 第二項 他律之監督

### 第一目 原主務大臣制

一、立法之理由

如前述日本個資法考量業者之營業自由與為能符合各業界處理個資之多樣性，故以行政指導方式，輔助業者自主、自律合法處理個資為最終立法目的，

自始即未授權行政主管機關以公權力作強力之行政監督。

許多日本學者專家於立法時，曾建議應採歐洲各國方式，設置一具強制力之獨立機關，統一掌理監督各業界合法適當處理個資之事權，逐步讓國內所有業者保護個資之體制健全並達到國際水準[179]；但基於各中央事業主管機關較熟悉各業界業者實際處理個資之狀況，由各該當主管機關自行監督較易達到實效；正如新設機關其必須為包括中央政府、地方自治團體之大規模增設組織及人員之擴充，此又違反日本近年持續推動之行政改革精簡機關之既定目標[180]；最後決定採「主務大臣制」替代獨立機關擔負起監督業者之權責。

二、制度轉換之背景

在全世界超過 22 億人利用網路之今日，網路已成為人們工作、學習、社交、交易等生活上不可或缺之工具。更因企業經營國際化，以及雲端科技產業興起，國內外間跨國傳遞個資已為企業事業活動之一環，從而個資之保護須跨國合作執行始能落實，紛爭或違法事件之解決及救濟，更須國際間互相協助，始能發揮實際救濟效力。長年來如何在各個國家間取得一定共識，建立相同水準及有實效性之國際性保護個資公約，以保障個資得安全、自由於國際間傳送，為各個有關個資保護法之國際組織首要議題。從而個資法之執行已非僅為國內事務，乃須經常性與各國互動、協議之國際事務，政府實需設置有統一事權得代表國家參與國際會議，與各國進行國際協議、合作執法等之機關。

其次，行政機關為行政事務管理或行政任務之遂行，常蒐集處理大量人民個資，尤以隨近年電子化政府之發展，常將所保有個人資料檔案電子化，以電腦處理戶籍、稅務等申報事務或提供行政服務，減省行政成本，並有效提升行政效率。然卻衍生行政機關間得輕而易舉將所保有之個資，藉身分證號碼為連結樞紐，透過電腦網路進行比對或組合，鎖定特定個人全面性掌握其戶籍、財

[179] 新美育文，個人情報保護基本大綱-アメリカ、EU との対比，ジュリスト，No.1190，2000 年 12 月，頁 94。田島泰彦、三宅弘編，同前註 7，191 頁。
[180] 岡村久道，同前註 31，頁 310；田島泰彦、三宅弘編，同前註 7，頁 192。

產、醫療、保險等資料，隱私權因此被侵害之風險極高；若再被有心人濫用以監視或打擊特定個人，更將使自由民主社會之根基受威脅。尤其近年各國以防止恐怖組織活動、打擊犯罪維護治安為由，廣設監視攝影器或監視人民之電子通訊記錄等事件頻傳[181]，在大眾不自覺中政府正嚴重侵害人民之資訊自主權。因此對行政機關之蒐集處理或利用個資，必須設置獨立監督機制，以有效監督政府機關合法蒐集、處理或利用人民個資，防止弊端發生。

再者，非公務機關民間之蒐集、處理或利用個資，雖得由各目的事業主管機關或地方政府機關監督其遵守個資法，因關於當事人請求閱覽刪除、訂正等糾紛之處理程序，常涉及法律之解釋與適用，為避免執法者各自為政，造成法律執行上寬嚴不一，及個資安全體制(security system)之建立時，規格、技術水準須求統一，實有必要設一獨立機關提供諮詢及予以輔導。

此外，當事人與個資之蒐集、處理或利用者發生紛爭時，常係以單一個人力量對抗行政機關或企業、團體，有資力不對等，救濟程序費時，訟源增加之問題；如有一獨立機關得先介入當事人紛爭中調查、調解，對當事人之救濟較有利，亦可減少訴爭。故設一獨立機關，擔任各機關、團體或個人有關個資問題之諮詢，發現個資處理上有問題時，提供建議或調解糾紛，負責遵法之宣導、資訊安全、教育訓練等事宜，除監督個資法之施行外，更能主導個資法之落實與發展。

三、獨立監督機關－特定個人情報保護委員會之設置

事實上設置獨立機關監督個資法之施行，並非本次修法所首創者，於 2003 年 5 月立法完成並開始施行之個資法特別法「行政程序中為識別特定個人之編號利用法」(日本一般稱編號法)[182]，對利用個人編號蒐集、處理之特定個資屬

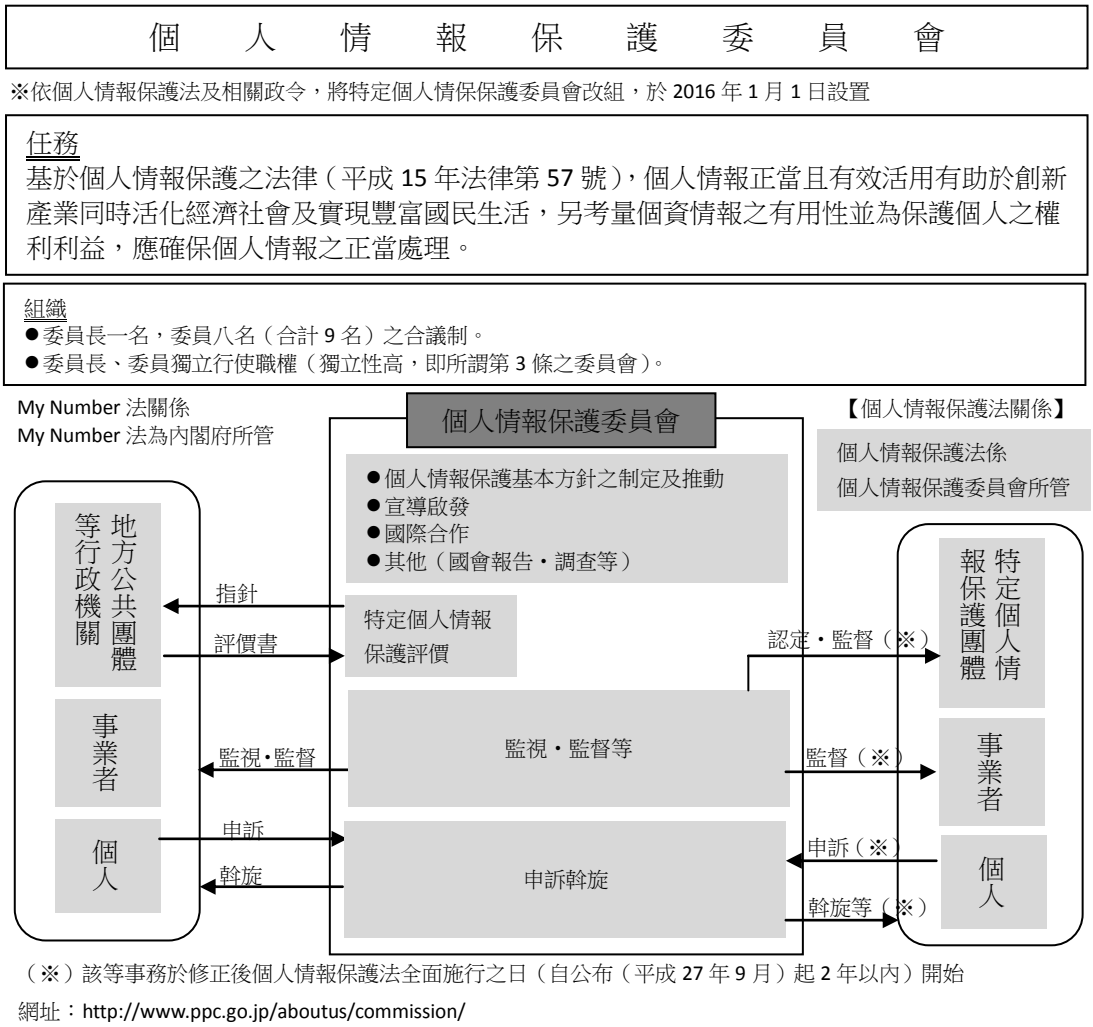
[181] 2013年6月16日曾任美國中央情報局之技術人員史諾登(Edword Snowden)於香港揭露美國國家安全局(NSA)用以監視網路平台之「稜鏡計畫(PRISM)」。

[182] 平成 25 年 5 月 31 日法律第 27 號，其詳細之立法經過及法制內容，得參閱范姜真媺，日本個人編號法對我國之借鏡，東吳法律學報，第二十六卷第二期，頁 14，2014 年 10 月。

社會保障、稅務及災難救助領域之個資，因具一定敏感性之個資，且以電腦網路作「人民→特定民間業者或團體→該管行政機關或行政機關間」之存取、傳遞，為確保其安全，且控管行政機關間以特設資訊處理系統作特定個資之比對、組合，不法利用於特定目的外嚴重侵害人權[183]，立法時於行政機關外設置獨立監督機關「特定個人情報保護委員會」自外部監視有關機關等合法運用特定個資。而此次修法即沿襲編號法第五章相關規定，設置保護委員會，並將「特定個人情報保護委員會」依法改組成個人情報保護委員會[184](即前所稱之保護委員會)。

[183]藤原靜雄，番号法と個人情報保護，法律のひろば，2013 年 9 月，頁 4。黛孝次，番号法における個人情報保護法の仕組み法律のひろば，2013 年 9 月，頁 20。
[184]日置巴美、板倉陽一郎，同前註 23，頁 52。宍戸常寿，個人情報保護委員會ジュリスト，2016，February，#1489，頁 43。

組織理念




（※）該等事務於修正後個人情報保護法全面施行之日（自公布（平成 27 年 9 月）起 2 年以內）開始

網址：http://www.ppc.go.jp/aboutus/commission/

第二目 個人情報保護委員會

一、定位、性質－內閣府外局之委員會

因保護委員會為監督對象包含全面業界個資之處理及利用，且必須具有獨立性，設置如會計檢查院(相當於我國審計部)為獨立於內閣外之機關，應最能達成任務，但如此則必須修改憲法始能設置，困難度極高。在參考如掌理警察行政之國家公安委員會及公正取引委員會(相當於我國公平交易委員會)等，同為須具有高度獨立性、位於各省(相當於我國二級機關之部會)之上，屬內閣府設置法第 64 條[185]所定之內閣府委員會設置方式；本法立法時，於第 59 條將保

[185] 平成 11 年 7 月 16 日法律第 39 號。

護委員會定位為依內閣府設置法第 49 條所設之內閣府外局機關，由內閣總理大臣(首相)管轄，以保障其不受外來行政機關等之干涉及壓力下，得以考量各業界活用個資之實際狀況與需要，且不偏頗獨立行使監督之權限。同時又因制度運用時，其得對監督對象行使指導、建議、勸告、命令、檢查等強力權限，須作高專業之法律及資安技術判斷，由委員會組織合議制方式進行各方意見之交換及討論係較理想可達成任務之運作方式。

二、組織

1、組成

依本法第 63 條規定，保護委員會由委員長 1 人及委員 7 人組成；其中 4 人為兼任委員；委員及委員長須經參、眾議院同意後，由總理大臣任命，以確保政治之中立性及受民主之統制。又因本法之立法目的是為規範業者適當並有效率活用個資，以創新產業、發展經濟，有助於豐裕人民生活，而建構必要之法律基盤，故委員須具有 ①對個資保護及利用之專門學識經驗者，②對消費者保護具有具有知識經驗者，③關於資訊處理技術具有學識經驗者，④對利用特定個資，亦即編號法中有關保險、稅務等行政領域個資之實務運用具有充分知識及經驗者，⑤對民間企業實務具有知識經驗者，⑥連合組織(為地方自治法第 263 條之三第 1 項所稱如律師公會、經濟連合會等)所推薦者。期能結合不同領域之學者或專家以進行會議，充分討論後依決議方式作出適當之決定。且上開①、②、④委員之加入組成，乃有助於透明化個資保護與活用調整過程[186]。

又依法第 70 條於委員會中設置事務局，以協助委員調查或處理行政事務，於 2016 年保護委員會成之初，先配置五十二位人員進行事務運作。

再因委員會委員不可能對個資保護之所有領域事務，均具有專業之知識與經驗，且委員會掌管之事務相當繁多，為避免對委員會造成過重之負擔，法第

[186] 宍戸常寿，同前註 184，頁 44。

69 條規定針對專門事項之調查，委員會得設專門委員，此專門委員係由委員會提出申請後，經內閣總理大人任命之，於專門事項之調查結束後即解任。例如有關匿名加工資料作成方法之規定，或跨國傳送個資時，對對象國家個資法制及運用是否達於與日本同等水準之調查事務，均為將來預定委任由專門委員進行之事務[187]。

2、任期與身分保障

委員及委員長任期，依本法第 64 條規定為 5 年，且得連任。為確保保護委員會持中立立場、獨立行使職權，法第 65 條規定在任期中，委員除有①受破產程序開始決定；②違反本法或編號法而被處以刑罰；③受有期徒刑宣告及④被委員會認定身心障礙無法執行職務，或有違反職務上義務及其他不適合為委員長或委員之行為者，不得違反本人意思予以免職；為避免前述④之免職被恣意濫用，以及保障委員會之獨立性，在該當性判斷上委由委員會自身進行，其決定依本法第 68 條第 4 項規定，必須經本人以外其他委員之全體同意。而委員之報酬依法第 75 條為由法律定之。

三、職權

依本法第 61 條明定委員會所掌事務如下：①基本方針之策定及推展，②有關個資及匿名加工資料處理之監督，及對當事人提出申訴進行必要之斡旋，並協助業者處理③有關認定個資保護團體之認定、監督事項等，④特定個資處理之監視、監督，或對當事人提出申訴進行必要之斡旋，並協助業者處理，⑤特定個資保護評價，⑥對個資之保護及適當、有效率活用，進行宣導，⑦對有關實施前六項事務，進行必要之調查及研究，⑧有關所掌職務之國際協助事項，⑨除前揭事項外之其他依法屬於委員會之事務。

依現行法規定原由各事業領域之主管大臣制定之 GL，於本次修法後亦轉由保護委員會擔任制定出全體業界共用之 GL，如遇有特殊之事業領域，則再

[187] 宇賀克也，同前註 22，頁 47。

由該事業主管大臣協助共同定立 。

四、監督權限

如前述日本向以個資或匿名加工資料之蒐集處理事務，為私領域之私法自治之問題，基本上應委由當事人間自行為第一次之協議處理，或透過個資法所定之當事人行使訂正、刪除等請求權，亦或經申訴程序要求個資處理業者履行其法定義務，以保障個資之合法、適當利用。但如遇惡質之個資處理業者，或當事人間就問題之解決無法達成協議時，最終仍需有第三人之監督機關保護委員會介入，作個資法被適當運用及保障當事人權益之最後手段。日本個資法賦予保護委員會如下之監督權限：

1、要求提出報告及進入檢查：依法第 40 條第 1 項規定，保護委員會對個資處理業者或匿名加工資料處理業者，關於個資法所規定義務之履行等上，有應予改善而進行檢討之問題時，得於必要範圍要求該當業者提出報告或相關資料；或進入該當事業之事務所或其他必要之處所，進行職員之詢問，或檢查帳冊、書類、其物件如電腦設施等。依同條第 3 項法規定上開進入檢查行為，並非為犯罪之調查,原依日本憲法第 35 條進入人民住所處等之檢查為犯罪之蒐查，為採令狀主亦須得到法院之許可,而本條特別明定本項之檢查非為犯罪之調查,故無須得到法院之許可,但其檢查所得之資料,並不完全排除在將來之訴訟上，作為證明犯罪之用[188]。

又進入檢查僅限於要求提出報告，仍無法正確掌握事實者或對必要資料之收集有困難者，使得進行之[189]。若個資處理業者或匿名加工資料處理業者拒絕提出報告、或進入檢查者，依法第 85 條得處三十萬元之罰金。

2、指導及建議：依本法第 41 條保護委員會得對個資處理業者或匿名加工資料處理業者，為有關個資匿名加工資料處理上必要之指導及建議。目的是希

[188] 宍戸常寿，同前註 184，頁 45。另得參考日本最高法院平成 16 年 1 月 20 日判決，刑集 58 卷 1 號，頁 26。
[189] 日置巴美、板倉陽一郎，同前註 23，頁 55。

望業者先能自主性解決問題，改善其處理個資之不當行為。但此指導及建議均非行政處分，故無法律之拘束力[190]。

3、勸告及命令：依本法第 42 條規定，保護委員會對違反法第 16 條至 18 條、第 20 條至第 22 條、第 23 條(不含第 4 項)、第 24 條至第 26 條(不含第 2 項)、第 27 條、第 28 條資處理業者、第 29 條第 2 項或第 3 項、第 30 條第 2 項、第 42 條、或第 52 條之資處理業者；或違反第 32 條第 2 項、第 36 條(不含第 6 項)、第 37 條、第 38 條之匿名加工資料處理業者，為確保正當處理個資或匿名加工資料，而認為有必要時，得勸告其採取改正或中止該當違法行為之必要措施。接受勸告者無正當理由而未採取勸告措施，且被認為對個人重大權益有迫切之侵害時，得命令其採取有關勸告之措施，原則上命令採勸告前置主義。但個資處理業者或匿名加工資料處理業者係違反法第 16 條、17 條、第 20 條至 22 條、第 23 條第 2 項、第 24 條，或 36 條第 1 項、第 2 項、或第 5 項、第 38 條，且被認為對個人重大權益有危害之事實，有必要採取緊急措施時，得直接得對該當事業者命令其採取中止或改正違法行為之必要措施。對違反本條命令之行為人，得依本法第 84 條處以 6 個月以下之拘役，或三十萬以下罰金。

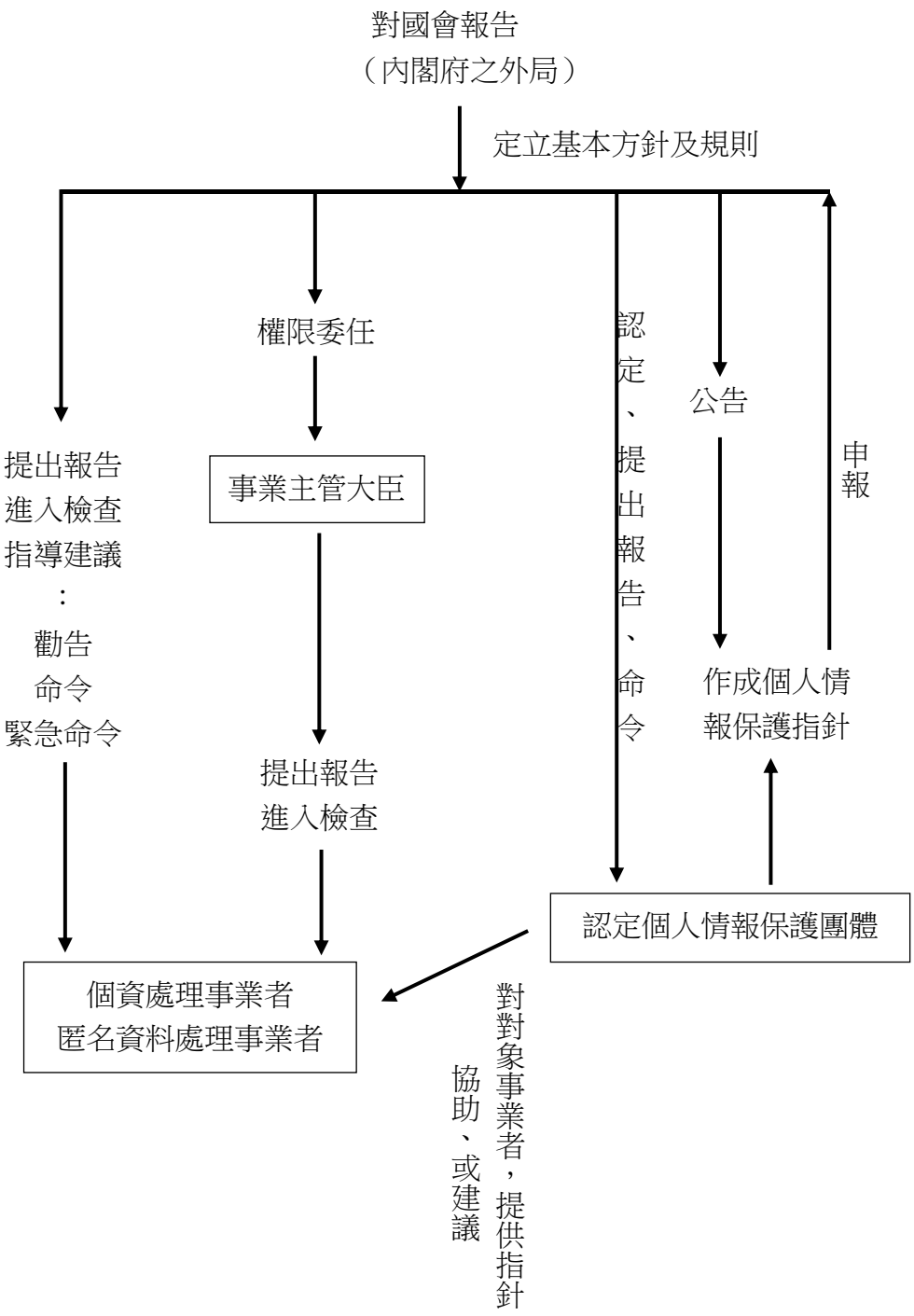
綜上，保護委員會權限之行使，為由緩之行政指導而至嚴之緊急命令之漸進式方式。

五、對國會之報告：

本法第 79 條規定,保護委員會每年應經由內閣總理大臣對國會報告所掌事務之處理狀況，同時公布其概要；此乃為讓人民理解保護委員會之運作狀況，藉此透明化本法之施行狀況，達到全民監督之效果。

[190] 日置巴美、板倉陽一郎，前揭 23，頁 56。

附圖：保護委員會之權限




六、獨立性與中立性之確保

保護委員會之設置最重要者，即為保護其能獨立行使職權，不受任何利益團體或政治勢力之干預，始能發揮其監督機關之功能，此亦為設置監督機關必

須符合之條件。本法除依第 65 條給予委員長及委員身分上保障外，因委員會置於內閣府，屬內閣總理大臣下，為除去可能受干擾之疑慮，更於第 62 條明示，委員會之委員長及委員獨立行使職權。委員會除須排除政治力干預外，尚須保持中立性，不代表任何政治團體，或與任何利益團體有關，始能獲得人民之信賴；故本法第 71 條 1 項規定，委員長及委員在任期中不得為政黨其他政治團體之幹部，或積極從事政治運動。

其次，本法亦有兼職禁止之規定，依法第 71 條規定，在任期中除得到內閣總理大臣之許可外，委員長及委員不得從事有報酬之其他職務或經營營利事業、執行其他以金錢利益為目的之業務。

**第三項 救濟制度**

如前述日本個資法立法時即已考量業者之營業自由，與能符合各業界處理個資之多樣性，故以行政指導方式，輔助業者自主、自律合法處理個資為最終立法目的，自始即未授權行政主管機關以公權力作強力之行政監督。即使修法後新設之獨立監督機關保護委員會，亦承襲未修法前主務大臣之輔導、指導為先之行政指導式監督。

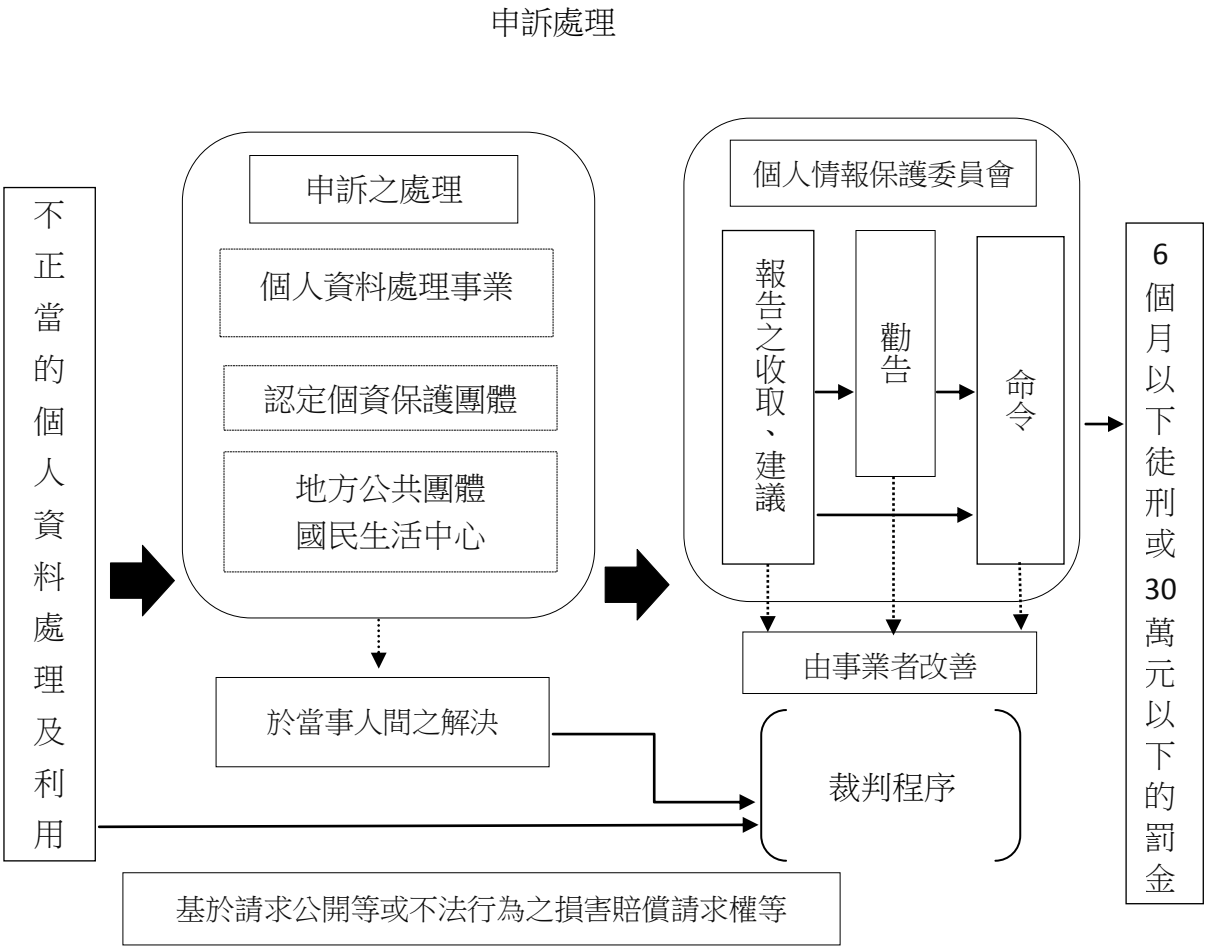
另一方面，為更有效實現民間業者自律守法之立法目的，個資法又設置多重之申訴處理制度，於當事人因有違法或不當蒐集、處理或利用個資之事情與業者間發生爭議時，得向「該當業者」或「個資保護團體」，或「地方自治團體之消費者生活中心等」提出申訴；而受理申訴之前開團體等得調查事實、提出建議或介入斡旋，讓當事人得快速獲得救濟，有效率解決當事人與業者間之紛爭；事實上亦有督促、輔導業者遵守個資法規範之功能。一般稱此為「多重之申訴處理機制」。

一貫日本期待民間部門自律、自治合法蒐集、處理或利用個資之立法宗旨，對民間部門與當事人間因個資之蒐集處理或利用發生紛爭時，認其本質上係私

人間之爭議，基本上應由當事人間先自行解決，且為快速、簡易之程序經濟考量，先依申訴程序處理較為妥當[191]。因此日本個資法第 31 條規定：個資處理業者應努力建立必要之體制，以適當且迅速處理有關個資蒐集，處理等當事人之申訴，由業者先檢討問題發生原因，自行尋求解決方法。另一處理紛爭機制，依修正後法第 47 條第 1 項第 1 款、第 52 條則是由「個資保護團體」，立於中立之立場，介入其會員業者與當事人間之紛爭中，能較客觀調查事實，協調雙方解決問題。且個資保護團體於累積各種申訴處理之經驗後，得將其經驗提供給其對象事業而發揮之功能，讓對象事業防止紛爭發生或適當解決紛爭[192]；故個資法第 42 條，個資保護團體於有當事人等申訴時，應給予當事人必要之建議，進行事實調查並通知該當業者，要求其迅速解決，此為第二個督促業者自行解決紛爭之機制。除上述由民間自行解決外，依個人資料保護基本之方針[193]第 7 條（3）、（4）地方自治團體亦得以消費生活中心或消費者諮詢窗口，受理當事人與業者間有關利用個資所引起紛爭之申訴，並介入斡旋處理。依法第 6 條第 2 款在中央則有保護委員會得進行斡旋，並與各地方消費者生活中心等諮詢機關聯繫，收集各種紛爭處理事例、經驗，分析整理後編輯成冊，供各機關團體參考，並協助進行諮商人員之訓練及養成等。綜上，顯見日本個資法對民間部門之規範以業者自律、自治為原則；當事人間紛爭發生時，則先依申訴程序由當事人間先行尋求解決方法，事實上亦內含由業者先自行反思，達到自律之作用，而非直接以強力行政管制佐以行政罰為主軸之方式，達到要求民間確實遵守個資法之目的。

191 日置巴美、板倉陽一郎，同前註 23，頁 133。
192 新保史生，個人情報保護の過去、現在、未来，JIPDEC IT-Report，2015Winter，頁 8-9。
193 平成 16 年 4 月 1 日內閣會議通過之法規命令，最新修正為平成 28 田 2 月 19 日。

附圖　救濟程序　參照平成 26 年日本消費者厅說明會資料



# 第四章 歐盟、日本及我國個資法制之比較、分析

## 第一節 我國個資法制之現況與課題

### 第一項 個人資料的定義

#### 第一款 個資之定義、範圍與判決實務

首先自我國個資法第 2 條第 1 款對個資定義觀之，個資為指：「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。」；故而該當資料得被認定為個資法保護客體之「個資」，須具備有「直接」或「間接」特定個人識別性[1]。上述規定與歐盟個資規則與日本法規定之體例，基本上相同。

所謂「直接特定個人識別性」應指單依該當資料本身，即得將其所指涉之人與他人區別識別出特定個人，如個人之身分證字號、個人肖像、個人姓名（但須考慮同名同姓之問題）等。至於所謂「間接特定個人識別性」之個資，依個資法施行細則第 3 條之規定，指單僅依該當資料無法自人群中識別出該當特定個人，然將之與其他資料作組合、比對後，得識別出特定個人者，例如車牌號碼，單依車牌號碼固無法辨識該車輛之所有人為何人，但將其與監理所登記車籍資料組合、比對下即得知車主為何人。然因特定個人識別性具有「相對性」及「流動性」之特質，造成個資之範圍難以界定。

在比較法上，本次歐盟個資規則修正，雖然未將指令第 29 條工作小組意見對於間接識別判斷所採取之綜合考量因素加以成文化，但不論是在個人資料定義規定中加入「位置資料」與「線上識別碼」作為可能間接識別資料之例示，抑或是在立法理由中說明間接識別之判斷應考量「所有客觀因素，並將資料蒐集、處

[1] 范姜真媺，個人資料保護法關於「個人資料」保護範圍之檢討，東海大學法學研究，第 41 期，頁 97-99，102 年 12 月。劉定基，個人資料的定義、保護原則與個人資料保護法適用之例外—以監視錄影為例（上），月旦法學教室第 115 期，頁 48-49，2012 年 5 月。

理或利用時可得的科技以及相關科技的發展一併納入」，仍顯示歐盟對於個人資料之定義採取較為廣義看法。相較之下，日本法似乎採取折衷作法，一方面有組合、比對容易性要件之限縮；另一方面，對於有無特定個人識別性之判斷，則採個資處理事業者基準進行判斷，操作標準較為明確。另外，日本對於識別個人之符號於本次修法時特別加入列為個資之一類型，而如何之個人符號係納入個資法保護之個資，為委由情報保護委員會依其訂立認定標準指定，非如歐盟將位置資料、線上識別碼以例示方式，擴大間接識別資料之範圍以為應對，似乎亦為較明確劃定個資範圍之立法方式。

就我國實務而言，對間接識別個資之判斷，見解未見統一。依法務部歷來之函釋，似未清楚說明有關「間接識別性」之認定標準。於早期時，其曾說明以「銀行帳戶之號碼與姓名、信用卡或簽帳之號碼、個人之其他號碼或帳戶等」，為個人資料類別中辨識財物者，故為個人資料[2]，而之後則以「建物之門牌、基地座落」[3]，「他人電子郵遞住址」（E-mail）[4]，機車新車領牌欄包括「機車新車領牌欄位之車主性別」、「廠牌名稱」、「發照日期」、「車型名稱」、「引擎號碼」、「車主出生年」、「顏色代碼」、「監理單位」[5]，「電話門號」[6]資料，因未與自然人之姓名等相組合尚不足以識別個人，亦無從以此方式直接或間接識別個人，故不屬於尚未修正前電腦處理個人資料保護法第 3 條第 1 款規定：「自然人姓名、出生年月日、身分證統一編號、特徵、指紋、財務情況、社會活動及其他足資識別該個人」之個資。此一時期可能因上開條文規定「足資識別」之要件，故法務部未將「間接識別性」個資納入保護對象，只要該當資料不足以識別特定個人，即認定不屬於個資，至於是否得有其他資料組合、比對則在所不問；於網路搜尋資料功能尚未至今日普及、方便之當年，採狹隘之個資概念，自是事出有因。

[2] 法務部 91 年 1 月 11 日法律決字第 0090046028 號函。
[3] 法務部 92 年 8 月 29 日法律字第 0920035652 號函。
[4] 法務部 94 年 5 月 6 日法律決字第 0940017397 號函。
[5] 法務部 96 年 11 月 19 日法律決字第 0960042113 號函。
[6] 法務部 96 年 6 月 21 日法律決字第 0960023899 號函。

至修法後之近年對於「住家電話號碼」、「行動電話」是否得以直接或間接識別特定人，法務部解釋以：「須從蒐集者本身綜合各種情況與事證判斷，原無一致性之標準，此宜於個案中加以審認[7]」；另外對特定「用電戶之電號」，「因其可提供○○公司作比對後，由該公司提供該特定用戶之歷年每個月用電量，顯見○○公司已保有完整可直接識別之個人資料，而水利署雖無自然人用電戶之完整客戶檔案，但已保有特定電號之資訊，如可比對水井登記人之個人資料而予以對照、組合、連結，亦屬可間接識別之個資[8]」，上開二函釋雖未對「間接識別性個資」認定標準表明其見解，然得推知「有無識別性之判斷」係以「蒐集者」、「利用人」為判斷對象，此觀點似乎與本文前述日本之通說相同，為採以處理個資者為判斷對象之「個資處理事業基準說」，亦即該當資料是否具有特定個人識別性，為依蒐集、處理或利用人所處之地位、條件、狀況而作不同之認定，非採「一般人」基準說。

此外，近兩年有關「行動電話號碼」與「電話號碼所屬電信別（即國家通訊傳播委員會公布之前 5 個阿拉伯數字）」是否屬於個資[9]？台北地方法院判決則有正反相對之見解。持肯定見解之判決[10]以，「自然人之電話號碼資料係屬其個人聯絡方式、電話號碼本身雖僅係一連串數字組合，並無特定識別性，但一旦與其他個人資料，如姓名、國民身分證統一編號，特徵及其他社會活動資料相互比對、組合、連結及勾稽結果，即得以間接方式識別特定自然人」。另電信事業別為行動電話用戶基於資費、促銷活動甚或企業形象等考量，選擇與何家電信公司締約或變更其締約對象,應屬其個人社會活動之一。……電話號碼所屬之電信

[7] 法務部 103 年 6 月 17 日法律決字第 1033506500 號函、法務部 103 年 6 月 18 日法律決字第 10303506790 號函、法務部 103 年 12 月 10 日法律字第 10303513640 號函。

[8] 法務部 104 年 2 月 24 日法律字第 10403502010 號函。

[9] 下列判決之事實及被告均相同，而各原告均以被告台灣大哥大股份有限公司開發建置、被告台灣酷樂時代股份有限公司出名推廣「M+ Messenger」通訊軟體，由行動電話用戶下載後，即可自由各電信事業共同建置之「號碼可攜集中式資料庫」查詢自己手機聯絡簿中各親友電話號碼所屬之「電信事業」名稱，並傳送顯示於手機上。原告以此種未經當事人同意將其與電信公司間之用戶資料提供給第三人為違反個資法第 29 條之行為。

[10] 台北地方法院，104 年度再微字第 1 號判決、103 年度小上字第 155 號判決。按前者為對後者判決確定後提起再審之判決。

事業別為個人電話號碼之附屬資料,得與其他個人資料如姓名、國民身分證統一編號等相互比對、組合、連結及勾稽後，據以作為間接識別特定個人之社會活動資料之一」屬個資法所保護之個資。

另一方面，持否定見解之判決[11]則先以：個資法立法目的中之促進個資合理利用，及為避免不當壓縮言論自由、資訊自由及公共利益，故解釋所謂間接識別之個資應以「合理、可能、容易之方法」為限，繼而認定：行動電話號碼僅為數字之組合，無法直接識別特定個人，而因行動電話號碼申辦幾無資格限制，是一人同時擁有多數門號者有，甚或借用、冒用他人名義抑或虛捏身分亦所在多有，故行動電話號碼不易與其他資料對照、組合、連結方式而識別特定個人，亦不具間接識別性，非屬個資。另電信事業別，並無法直接識別特定個人，縱與電話號碼相結合，依前述電話號碼已難直接或與其他資料連結間接識別特定人之情況，仍極難識別特定個人，故電信事業別非屬得以間接識別之個人資料。

綜觀上開實務見解，對「特定個人識別性」之認定，採肯定者，所重者在個人權利保護，相對之，採否定說者，則特別強調個資之合理利用，從而對間接識別性個資範圍之認定，有寬嚴之分。加之我國個資法對「間接識別性」認定之要件？以何人為對象進行判斷？均未訂明，實務上見解歧異不足為奇。再細觀發生有無間接識別性爭議之系爭個資，均為「建物之門牌」、「電子郵遞住址」、「引擎號碼」、「電話門號」、「用戶之電號」等個人識別符號，而非記述型個資，亦可預見將來對此類符號型個資是否有間接特定個人識別性之爭議必是方興未艾，亦屬於個資法適用範圍之灰色地帶。

**第二款 去個人識別性個資再認定之必要**

查我國個資法於第 6 條第 1 項但書第 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 款等，均有為統計或學術研究而有必要「資料經提供者處理後，或蒐集者依其揭露方式『無從

[11] 台北地方法院 103 年度訴字第 255 號判決；台北地方法院 103 年度訴字第 212 判決。

識別特定當事人』」之規定。依個資法施行細則第 17 條規定，所謂「無從識別特定當事人」係指：「個資以代碼、匿名、隱藏部分資料或其他方式，無從辨識該特定個人者」。

上述「無從識別特定當事人」之個資，在我國個資法上有其特殊地位。此類個資依個資法第 9 條第 2 項第 4 款免除告知當事人義務，再依同法第 19 條第 4 款得合法蒐集處理，並得依同法第 16 條但書第 5 款及第 20 條但書第 5 款為特定目的外之利用。然在實務上，對於此類個資之定性，尤其經各種去識別化方式，使其無從識別特定當事人之資料，究竟是否仍屬於個資法所稱之個人資料，其與前揭「間接識別」之資料又有何關係，一直未能加以釐清。

以法務部 102 年 3 月 12 日法律字第 10203501470 號函為例，該函旨在處理中央警察大學因辦理民意調查所需，函請新北市政府警察局提供住宅竊盜報案人住宅聯絡電話如何適用個資法之問題。法務部認為，如中央警察大學請求提供者，係經警察局處理後無法識別特定當事人之資料者，則提供者既非個人資料，自無本法之適用。類似見解亦可見法務部 105 年 1 月 13 日法律決字第 10503500370 號函，該函亦表示：「車輛原廠維修廠將前任車主之車輛維修紀錄提供予現任車主時，如已運用各種技術將之去識別化，而依其呈現方式已無從直接或間接識別特定生存之自然人者（例如：略去車主身分辨識及聯絡方式等欄位，以及有關肇事時、地、原因等可能辨識自然人之詳情；僅留與車輛物件描述與維修更換情況如入廠日期、里程數、工作敘述、更換零件項目），即非屬個人資料，對外揭露自無適用本法之問題。」

實則，不論是單純之報案電話號碼或車輛維修紀錄，因原資料蒐集者（即警察機關或維修場）仍保有完整紀錄可供比對、連結，是否可經去識別化成為「非屬個人資料」（亦即歐盟個資規則立法理由中所稱：無法以任何方式再識別之「匿名資料（anonymos information）」），恐怕仍有疑義。單以電話號碼而言，法務部亦曾表示：「行動電話是否得以直接或間接方式識別者，需從蒐集者本身綜觀

各種情況與事證加以判斷，原無一致性之標準，此宜於個案中加以審認」。[12]足見，去識別化後之資料，是否仍然屬於個資法所稱之個人資料，需要個案判斷，難單以資料種類或經去除一定之欄位，就逕行認定為非個人資料。

應說明者，從個資法第 6 條第 1 項但書第 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、第 20 條第 1 項但書第 5 款等相關規定，以及施行細則第 17 條規定之文義及體系解釋，上述規定所稱「無從識別特定當事人之資料」應仍屬（間別識別之）個人資料，亦即歐盟個資規則所稱「去連結（或稱為「假名化」）資料（pseudonymised data）」，否則若已完全無法直接或間接識別，本無個資法之適用，何須再加以規定。此一見解，亦可從本次歐盟與日本法律之修正，獲得進一步佐證。

首先，就歐盟個資規則而言，本次於第 4 條第 5 項新增去連結（資料）之定義，凡「在不使用額外資料之情形下，無法將個人資料歸屬於特定個人之資料處理或利用方式；但該額外資料必須分別保管，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之自然人」。如本報告第二章所述，此一去連結資料在歐盟個資規則開放為「公益之檔案保存、科學或歷史研究目的，或統計目的」而進一步利用個人資料時，扮演關鍵角色。應說明者，此處所謂去連結資料，因仍有額外可供比對資料存在，故仍屬（間接識別之）個人資料，受到歐盟個資規則之規範，並無任何疑義。

其次，就日本法而言，新增之「匿名加工資訊」規定，亦即將個資予以加工處理去除「特定個人識別性」，成為無法識別「特定」個人之資訊，進而免除其為原特定目的外第二次利用、或提供第三人時須得到當事人同意之義務。對於上述匿名加工資訊，日本法並未要求全面排除回復可能性，採將匿名加工之過程全面法定透明化，禁止處理加工者與接受加工匿名資料者回復其識別性，較之歐盟為更完整之法制規範。

[12] 同註 7。

綜上， 不論是歐盟或是日本在本次修法時均體認在大數據時代，要將資料完全去識別成為絕對不可回復之「非個人資料」實有一定困難。因此不約而同在新法中加入所謂「去連結（假名化）」或「匿名加工」資料之概念，以進一步調和個人資料保護與個人資料合理利用之利益。反觀我國，雖然有多項條文提及「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」，但個資法對於此種「無從識別特定當事人」資料（實較為接近歐盟個資規則所稱「去連結（假名化）」資料）究應如何適用（例如：可否將可以直接識別之個人資料提供予第三人進行研究，而由第三人在發表時再進行去識別之處理[13]）仍有待釐清？更何況相關條文對去個人識別性基準、程序等事項未置任何規定，無法防止個人識別性復原之可能，未能消除當事人對自己個資被濫用之疑慮。又，自上開相關規定可得知蒐集或利用去識別性個資之主體僅限於公務機關或學術研究機構，目的更局限在基於醫療、衛生或犯罪預防、或公共利益為統計或學術研究而有必要者，其適用範圍較為有限。此一較為限縮之立法模式，雖與歐盟個資規則類似，但與日本新法之規範卻有相當差異，若我國欲推動大數據產業發展，是否可以滿足各行業對個資利用之需求，恐怕亦值得檢討

## 第二項 敏感性特種資料之規範

### 第一款 定義之再考

我國個資法將個人資料定義為：「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」，進一步共同觀察個資法第 6 條第 1 項，其特別針對「病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料」，考量其資料性質較為特殊或具敏感性，明訂不得蒐集、處理或利用，而屬特殊種

[13] 關於此一問題，法務部於法律字第 10403508020 號函中採取肯定之見解，認為：「公務機關所保有之個人資料，並非一律均須達無從以直接或間接方式識別該特定個人者後，方得提供予其他公務機關或學術研究機構，重點在於統計或學術研究成果發表時，依其呈現或揭露方式必須已無從識別特定之當事人」。

類之個人資料。若以比較法之觀點，觀察日本及歐盟對於特種個人資料之界定，將發現其所歸類之敏感性個人資料，尚具有以下特點：列舉的部分，納入民族或種族、政治見解、宗教信仰或世界觀之確信、社會身份、工會會員資格、生物特徵、犯罪被害事實、性傾向[14]等個人資料類別；另外，日本法中甚至得見以概括條款之形式，[15]為納入更多特種個資之類型，保留其可能性。然而，我國個資法第 6 條之立法理由亦提及，目前規定的特種資料的類型，係「經審酌我國國情與民眾之認知」後而定，故係有意排除病歷、醫療、基因、性生活、健康檢查及犯罪前科 6 類以外之其他個人資料資料作為特種個資；但立法及行政機關亦因此必須關注時代環境變遷、科技技術發展與民眾對於隱私權認知的改變，適時回應特種個資擴充之需求。故是否應仿效日本或歐盟之立法，納入更多特種個人資料之類型，或許必須考量我國之社會環境及文化敏感性等各個不同面向的發展程度，為適當之評估與適時之調整。

**第二款 特種資料蒐集、處理及利用要件之檢視**

我國個資法中針對病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料，於第 6 條明訂原則不得蒐集、處理或利用。但於第 1 項下明訂 6 種例外得蒐集、處理及利用之情形，包括：法律明文規定（第 1 款）；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 2 款）；當事人自行公開或其他已合法公開之個人資料（第 3 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 4 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，且事前或事後有適當安全維護措施（第 5 款）以及經當事人書面同意之情況（第 6 款）。

[14] 我國個資法第 6 條第 1 項雖未明文將「性傾向」納入特種資料之類型，但若參照立法理由之說明，將可知其就性取向等相關事項，亦包含在「性生活」的範圍之內。

[15] 日本個資法第 2 條第 3 項：「本人之人種、信仰、社會身分、病歷、犯罪之經歷，因犯罪被害之事實及其他處理上不使對本人發生不當差別待遇、偏見其他不利益；而在處理上需要特別考量，依政令所指定之記述型等個人資料。」

上述規定係於 2015 年底完成立法程序，並於 2016 年 3 月 15 日生效施行，使先前凍結適用之第 6 條終得發揮其規範功能，亦讓蒐集、處理及利用特種個資之行為得有所據。但若進一步比較個資法第 6 條第 1 項對於特種個資例外得蒐集、處理及利用之要件，其與歐盟個資規則具有以下幾個較為顯著之差異：

1. 首先，相較於我國個資法第 6 條第 1 項第 3 款，歐盟個資規則第 9 條第 2 項第 e 款僅允許由當事人自行公開之特種資料，才能處理，而我國尚及於「其他已合法公開之個人資料」，[16]亦屬例外得蒐集、處理及利用之情況，要件似較為寬鬆。
2. 其次，歐盟個資規則針對出於勞動醫學、公共衛生、基於公益之檔案儲存、學術或歷史研究等目的，利用特種個資之行為，將其列屬「資料處理之特殊情形」，排除目的拘束原則之適用，並授權各會員國得自訂規範，限縮當事人得主張權利之空間，但同時亦強調技術及組織上之相應保護措施之不可或缺（歐盟個資規則第 88 條及第 89 條）；相較於我國個資法，對於所有特種個資之類型，均適用第 6 條下同一要件，似乎較為細膩，亦較能妥適考量不同特種資料之特性。
3. 續之，歐盟個資規則第 9 條中，不乏將重大公共利益、當事人本身之重大利益之維護，或為防止他人權益之重大危害，列為得以使用特種資料的例外情況；我國個資法雖在就一般性個人資料之蒐集、處理及利用要件中，亦得見類似之例外規定，[17]但針對特種資料，並未納入，而是選擇在個資法第 6 條第 1 項第 2 款之「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」外，增定第 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，且事前或事後有適當安全維護措施」，擴張例外得蒐集、處

[16] 所謂其他已合法公開之情形，係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。
[17] 例如：個資法第 16 條第 2、3、4 款，以及第 19 條第 1 項第 6 款，第 20 條第 1 項第 2、3、4 款。

理或利用特種個資之情況，[18]考量依據目前實務解釋，無論組織法規或作用法規，均可作為公務機關法定職務之依據，其是否會導致特種資料得在公務機關間「例外」傳輸之鬆綁？[19]上述條款自 2016 年 3 月施行後之實務運作情況，值得關注。相較之下，歐盟個資規則第 9 條第 2 項第 g 款，雖然亦允許基於「重大公益（substantial pubic interest）」而蒐集、處理或利用特種個資，但一方面該款限於「重大」公益（相較之下，歐盟個資規則第 6 條第 1 項第 e 款則僅稱「公共利益」）；另一方面，仍須有會員國法律作為依據，因此在範圍上，仍較個資法上述規定限縮。

4. 最後，歐盟個資規則中，針對為法律訴訟所必要，得例外使用特種資料（歐盟個資保護規則第 9 條第 2 項第 f 款）；但我國個資法中並無此一例外規定。

### 第三項　規範對象（適用主體）

現行個資法以公務機關與非公務機關為「適用主體」。依據個資法第 2 條第 7 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」；同條第 8 款則將非公務機關定義為：「前款以外之自然人、法人或其他團體」。相較於電腦處理個人資料保護法時代，僅特定之民間行業或團體方受到該法規範，現行個資法將規範對象擴大及於所有自然人、法人或團體，除個資法另有排除規定外，均受到規範，對於個人資料之保護，自是更為全面周全。

上述立法模式，原本即是仿效歐盟個資指令第 4 條第 7 項及第 8 項對於資料管理者之定義：「自然人、法人，公務機關，機構或其他組織」，本次歐盟個資規則未加修正而予以沿用。值得注意者，日本個資法本次修正，刪除舊法以處理個資數量（在過去六個月內之任何一天均未超過五千人）作為適用門檻之規定，將

[18] 於行政院提案的第 6 條修正草案中，將「為維護公共利益所必要」，列為例外事由之一，但通過版本改採現行「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」之規定。

[19] 相同的憂慮得見邱文聰，赤裸的國民與遁天入地無所不能的政府，自由時報自由廣場，2015 年 12 月 21 日，http://talk.ltn.com.tw/article/paper/942381（最後瀏覽日：2016 年 12 月 23 日）

所有「處理個資業者」原則上均納入規範之對象；如前所述，所謂處理個資業者，係指將個人資訊資料庫供「事業」之用者，解釋上只要反覆繼續從事同種活動，且為社會一般通念上所認定之事業，其雖不限以營利為目的，法人、非法人團體，甚至個人均有該當之可能，重點乃在須具備反覆利用以為事業利用之要件；又如本報告第三章所述，日本將個人資料分為「個人資訊」、「個人資料」及「保有個人資料」，分別對其處理之業者課予由輕至重不同層次之法律義務，亦可查知其立法時，並無意過度規範個人一般日常私生活之蒐集利用個資，同時考量業者負擔之輕重。

綜上，由於我國個資法適用主體範圍與歐盟個資規則較接近，而日本之個資法則較以「供事業之用」之方式限縮適用對象。

除上述個資法第 51 條第 1 項規定之解釋問題外，我國是否有必要仿效日本法就特定事業、團體增訂排除適用之規定，亦有必要加以討論。早在 2010 年電腦處理個人資料保護法於立法院審議時，是否為維護新聞報導、採訪自由而針對大眾傳播業者特別訂定排除規定，即曾產生重大爭議。部分論者擔憂個資法之施行，不論是特種個資原則禁止蒐集或告知義務之規定，均可能對新聞媒體採訪報導造成嚴重妨礙，產生寒蟬效應，因而主張增訂相關排除條款；[20]相對地，也有民間人權團體主張：「目前電子媒體快速發送及不斷重播的狀況下，此種發佈個人資料的方式，對於當事人隱私的侵害程度，絕對不下於其他機構」，假若「只要媒體『基於報導之目的』就可以免除告知…對於當事人的影響將無法想像」。[21]最終通過之版本則維持行政院版草案規定，在第 9 條第 2 項第 5 款規定：「大眾傳播業者基於新聞報導之公益目的而蒐集個人資料」得免除間接蒐集之告知義務；另於第 19 條第 1 項第 6 款規定：「與公共利益有關」之合法蒐集、處理事由，並

[20] 參見吳敏華，從法律應然面與媒體採訪工作實然面出發－評析個人資料保護法第六條、第八條，http://ccs.nccu.edu.tw/word/HISTORY_PAPER_FILES/1509_1.pdf （最後瀏覽日期：2016 年 11 月 20 日）。

[21] 邱伊翎，新聞自由、隱私與個資法，2010 年 5 月 3 日，http://www.tahr.org.tw/node/176 （最後瀏覽日期：2016 年 11 月 20 日）。

於立法理由中敘明，本款規定得作為新聞自由或知的權利與隱私權界線之判斷標準。

應說明者，個資法公布施行迄今，透過法務部適時解釋，並未造成媒體、學校、研究機構、宗教或政治團體運作上之重大妨礙；以大眾傳播媒體為例，雖然並未有全面排除個資法適用之規定，但透過個資法中公共利益條款之操作、告知義務除外之規定，依然穩健運行，未見因個資法引發寒蟬效應之情事，故可維持現行規定。至於現行適用主體打擊範圍是否過廣而應予限縮之問題，本文一方面認為個資法新法施行至今，情況尚稱良好，對於中小企業似未產生嚴重衝擊；另一方面，有關適用主體範圍過廣問題，應可透過進一步明確個資法適用之除外規定，以及增加蒐集、處理或利用之利益權衡條款等面向尋求解決，而不是背離國際趨勢，回頭限縮適用主體範圍。

**第四項 適用除外規定**

個資法第 51 條第 1 項規定：「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。」此一規定在個資法普遍適用主體之同時，提供安全閥之功能，避免過度擴張個資法之適用範圍，對自然人日常生活形成不當干預。

應說明者，個資法上開規定在解釋上並非毫無爭議。首先，第 2 款「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」，依據法務部所整理之立法理由，主要為解決在網際網路上張貼影音個人資料甚為普遍，而合照或其他在合理範圍內之影音資料須經其他當事人之書面同意始得蒐集、處理或利用之不便，故明定其不適用個資法。然而，本款規定所欲處理之絕大多數情形，原本即可由第 1 款規定所吸收，此對照歐盟舊個資指令或新通過之個資規則，均僅有第 1 款之除外規定，而無類似第 2 款之規定即明；更何況，在個資法 2015 年底修正後，已取消蒐集、處理或利用一般個資時，當事人同意須

以「書面」為之之僵硬規定，因此在合照等當事人明顯已有同意表示之情形，似已無須再另定此一排除規定。[22]

其次，就第 1 款之規定而言，究竟何謂「自然人為單純個人或家庭活動」？在網際網路各項應用服務快速發展之今日，判斷恐日漸困難。例如：自然人透過網路拍賣平台進行交易而取得個人資料，是否有本款除外之適用？如前所述，在本次歐盟個資規則修正過程中，草案曾一度考慮增加:「未獲得任何利益」或「可合理預期僅得由數量有限之人存取」等要件，惟最終通過之版本仍維持指令時代之規定，僅在立法理由中說明「不得與職業或商業活動有關」。

有鑑於個資法現行規定與歐盟個資規則並無重大差異，本文因此建議可暫不修正；未來如確有進一步釐清適用範圍之需要，或可透過解釋（行政規則）之方式為之。應附帶說明者，固然目前實務對於法務部有關個資法之解釋，一般均採取相當尊重之態度。然而，法務部之函釋，對於其他機關，尤其是司法機關而言，並無拘束力；正本清源之道，仍在於未來中、長期修法時，能將實務上累積之審酌、判斷要素，具體轉化為法律之規定，始能產生具有全國一致拘束力之標準，減少法律適用上之不確定性。

**第五項 適用地域範圍**

一般法規如未特別明定其「地域效力」及「人的效力」範圍，原則上其效力及於制定機關土地管轄範圍的全部，以及所有停留在該地域範圍內的人，不論其是否為本國人。[23]以現行個資法而言，其適用地域範圍，自包括中華民國領域全部及位於境內的本國及外國(法)人。茲有疑義者，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。」上述規定，是否意味位於中華民國領域外之「外國」公

[22] 審查意見認為第 2 款規定是否全無保留必要，仍可再斟酌，例如：某甲在社群網站公開其參與某演唱會所拍攝之照片（包含舞台上表演者或其他觀眾）。本文認為，如某甲目的仍是供自己個人或家庭活動目的而拍攝（蒐集）與張貼（利用），應仍有個資法第 51 條第 1 項第 1 款之適用。至於此一行為是否另有侵害表演者肖像權或其他觀眾隱私權（如：照片包括其他觀眾私密舉動）之問題，則應依其他法律（如：民法）判斷，與個資法無涉。

[23] 陳敏，行政法總論，自刊，2013 年 9 月，頁 134。

務機關與非公務機關，只要其蒐集、處理或利用中華民國人民之個人資料，即應受到我國個資法之規範？

本文認為上開規定所稱之公務機關及非公務機關應指位在我國境內，原即受個資法規範之公務、非公務機關(包括位於我國境內之「外國」自然人、法人或其他團體)，但迂迴從境外蒐集、處理或利用我國人民資料者；至於單純位於境外之外國人或外國機關，並不受現行個資法之規範，其理由有二。首先，上述條文之立法理由稱該項規定是為防止「規避法律責任」，似指原即有個資法適用，但卻設法逃避的情形而言；而位於境外之外國機關基於一般土地管轄原則原不受我國法律規範，無所謂規避問題，因此似非立法者所欲規範之對象。其次，上述立法理由明文參照之歐盟個資指令，其規範對象原則上也不包括位於境外之外國(法)人。

值得注意者，本次歐盟個資規則及日本新個資法之修正，不約而同地將各該法律規定之適用地域範圍予以擴張，以回應跨國（網路）交易日益頻繁、個人資料跨境傳遞日漸普及之現象，俾提供境內人民更周全之保障。具體而言，兩部法律均將其適用範圍延伸至「位於境外，但對境內人民提供商品或服務而蒐集、處理或利用其個人資料之資料管理者」；此外，歐盟更進一步規定，凡對於歐盟境內人民之行為進行監控者，亦受到歐盟個資法規則之規範。

然而，在國際上對於歐盟與日本此類擴張個人資料保護法適用範圍之作法，並非沒有質疑之聲音。例如美國隱私法學者 Paul M. Schwartz 即認為前述歐盟個資規則所稱「對歐盟資料主體銷售物品或提供服務」或有「監控歐盟資料主體行為」不夠明確、打擊範圍過廣，將徒然增加某些對於歐盟人民隱私威脅極低之外國雲端服務提供者之法令遵行成本；[24]即便在歐洲，也有論者剴切指出，內國個資法之域外適用將增加個人資料保護法制衝突之可能性，且有鑑於此類規定往往

[24] Paul M. Schwartz, EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation 2-3, Bloomberg BNA: Privacy and Security Law Report, April 29, 2013, http://paulschwartz.net/wordpress-content/uploads/2012/01/schwartz-eu-privacy-and-the-cloud-BNA-May-2013.pdf (last visited Nov. 20, 2016).

難以落實執行，恐將形成資料主體一種不切實際之期待，以為其資料不論於國內或國外遭到蒐集、處理或利用，均可獲得一致之保障。[25]

綜上，雖然學者對於內國個資法域外適用之規定有持保留意見者，但本文認為我國個資法，恐怕仍須嚴肅考慮下列問題。首先，依據現行規定，我國人民大量使用之境外網路購物平台、影音平台或是雲端服務提供者，蒐集、處理或利用我國人民之個資，均不受我國個資法之規範，已形成保護漏洞；[26]反觀台灣資料管理者若跨境蒐集歐盟或日本資料當事人之個資，卻要受到該國個資法規之拘束，立足點顯不平等。其次，所謂「對內國人民銷售物品或提供服務」之要件，雖有一定之不確定性，但卻久為國際民事訴訟中考量內國法院是否具有管轄權之判斷要素之一，仍有一定之操作可能性。再其次，內國個資法之域外適用雖然可能增加個人資料保護法制衝突之可能性，但有鑑於國際間所採取之個人資料保護原則並無太大差異，法律衝突之問題未必有想像中嚴重。最後，固然此類規定之落實執行有其難度，尤其跨國行政檢查，恐怕力有未逮，但內國執法機構對於境外平台或服務提供者亦非全無掌控可能性，例如：日本此次修法即表明將透過加入國際組織或簽署雙邊合作協議之方式，透過情報交換，由服務提供者所在地國家之個人資料保護機關協助執法；又，境外業者如有與國內金融機構往來，內國執法機關亦有可能執行其相關財產。

**第六項 告知義務**

有關資料管理者於蒐集個資時之告知義務，現行個資法於第 8 條及第 9 條，分別針對「向當事人蒐集個資（直接蒐集）」及「非由當事人提供個資（間接蒐集）」之情形加以規定，明定應告知之事項及免除告知事由。

---

[25] *See* CHRITOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 128-29 &142 (2013).

[26] 審查意見認為，在現行法下是否可能將境外網路購物平台、影音平台或雲端服務提供者資料蒐集行為之「行為地」，解釋於發生在「境內」，進而可以立即適用個資法？本文認為此一見解固然用心良苦，但一方面因為業者伺服器設於境外，其「取得」個人資料之地點，實際上恐怕仍是在境外，難以往前延伸至當事人「提供」資料之地點；另一方面，從歐盟與日本分別修正其個資法，明文規定域外適用之情形，也可以得知，單純擴張解釋「蒐集行為之行為地」，是否符合明確性之要求，可能衍生爭議。尤其，若果如此解釋，則個資法第 51 條第 2 項之規定即無存在必要，是否符合立法原意，也有疑義。因此，本文仍認為應以法律明文規定為宜。

如前所述，本次歐盟個資規則修正，告知規定之強化是其修正重點之一。除著眼於增進資料當事人對於告知事項之理解及考量其資訊接收負荷能力，增訂告知之一般規定（個資規則第 12 條第 1 項），並採取基本告知及進階告知之模式外（個資規則第 13 條第 2 項、第 14 條第 2 項），不論是直接或間接蒐集之告知事項，均有所增加（個資規則第 13 條第 1 項、第 2 項及第 14 條第 1 項、第 2 項）。

比較個資法與歐盟個資規則有關告知之規定，本文認為個資法至少在以下幾方面有所缺失。首先，個資法及施行細則目前僅對於告知之「方式」（亦即得以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式）有所規定，但就告知內容對資料當事人而言是否具有「可接近性」，卻沒有要求；實務上告知事項被以含糊、籠統且艱澀難懂之文字表述者，並非少見。然告知內容對於當事人資料自主決定權及其他權利之行使，具有關鍵地位，如何確保當事人對於告知事項有清楚、明確之認識，實屬個資法不可迴避之問題。

其次，就告知事項而言，個資法第 8 條第 1 項規定亦有檢討必要。有關「蒐集之目的」部分，參考歐盟個資規則（第 13 條第 1 項(c)款、第 14 條第 1 項(c)款），似應一併告知蒐集之合法事由，以便當事人判斷資料蒐集之合法性與必要性。而在「個人資料之類別」部分，現行規定未必能讓資料主體清楚瞭解究竟何資料被蒐集；更重要者，若相關資料係由資料當事人主動提供（而非由資料管理者透過機器自動蒐集），此一告知事項似無必要（歐盟個資規則僅在間接蒐集時方要求告知蒐集資料之類別，第 14 條第 1 項(d)款）。而就「利用期間、地區、對象及方式」等資訊而言，有關利用時間，得參考歐盟個資規則第 13 條第 2 項(a)款，如無法具體說明期間之末日者，至少應告知決定利用期間之標準；有關利用地區，應僅限於資料管理者欲將蒐集之資料傳遞至境外處理或利用之情形才須特別說明；有關利用對象，應指資料蒐集者外，其他個資之收受者(recipient)而言，然參考歐盟個資規則第 13 條第 1 項(d)款，似可保留一定彈性，在個案中

允許僅告知利用對象之類型；至於「利用方式」，現行規定之意義即有未明，或可參考歐盟規定，限於利用個資作成自動化決定或剖析等特殊方式時，才須詳細告知。

第三，另一值得思考之問題在於個資法是否有必要將相關告知事項劃分為「基本告知事項」與「進階告知事項」；依據歐盟個資規則，二者區分之主要標準在於後者僅在確保資料蒐集、處理或利用之公平與透明而有「必要時」方須提供。本文初步認為，由於要求個別資料管理者判斷進一步提供相關資訊是否具有必要性，在執行上恐有一定困難（對資料管理者而言，負擔或許較完整告知所有資訊更重），且個資法對於告知之方式已有相當彈性（包括多種告知方式），似不必再將告知機制複雜化，而可維持現制。

最後，在免告知事由之規定上，若與歐盟個資規則相較，最大差異在於直接蒐集時之免告知事由。依據歐盟個資規則第 13 條第 4 項之規定，僅有在當事人已知悉相關告知資訊時，資料管理者方可免除告知義務；相對地，個資法第 8 條第 2 項則列有六款免告知事由。應說明者，直接蒐集是個人資料蒐集、處理或利用之原則與根本，必須先存在直接蒐集之行為，才有另一間接蒐集之可能性。因此，有關直接蒐集之免告知事由不宜過寬，方能確保資料當事人至少可以從直接蒐集者處，知悉相關必要資訊。

就現行第 8 條第 2 項各款規定而言，有關個人資料之蒐集本身即係執行法定職務或履行法定義務之免告知規定，雖然自各該法規或可一窺蒐集目的或利用對象，但就其他告知事項而言，例如：利用期間、地區（是否有跨境傳遞）、方式、當事人得行使之權利及方式、甚或本文前述建議新增之蒐集合法事由（亦即究竟依據何法規蒐集個資），卻未必能從相關法規中得知。有關「告知將妨害公務機關執行法定職務」或「個人資料之蒐集非基於營利之目的，且對當事人顯無不利之影響」之情形，由於個資法對於告知之方式已有彈性規定：可以採取言詞、書面…電子文件，或採用公告…等當事人可得知悉之方式告知，學理上更承認混合

多種方式之「多層次告知」之方式，對於公務機關執行職務或非基於營利目的而蒐集個資者應不至造成妨害或增加過度負擔，似亦無排除之必要。至於「告知將妨礙公共利益」，審酌個資法第 8 條第 1 項之告知事項內容，實難以想像具體情形為何。

就間接蒐集免告知之情形而言，個資法第 9 條第 2 項之規定與歐盟個資規則較為接近。值得特別說明者，前述直接蒐集免告知之不合理情形，在間接蒐集則未必如此，或許仍有存在之必要（如：蒐集個資本身即係執行法定職務或告知將妨害公務機關執行法定職務），此乃因維護間接蒐集行為秘密之特性使然。就現行法而言，少數有疑義之事由，例如：「當事人自行公開或其他已合法公開之個人資料」是否可以免除告知義務，恐仍有討論空間。蓋資料管理者蒐集此類資料仍須具備特定目的與必要性，就資料當事人而言，其亦有主張個資法相關權利之需求，如單純以此為由免除告知義務，恐不利個人資料保護目的之達成。

**第七項　非公務機關一般個資蒐集、處理或利用之合法事由**

關於非公務機關蒐集、處理一般個資，個資法於第 19 條定有八款合法事由，同法第 20 條針對目的外利用，亦定有七款合法事由；上述事由多參考自歐盟個資指令之規定，與歐盟個資規則第 6 條第 1 項比對，亦大致相符。值得注意者，自歐盟個資指令時即存在且於個資規則中亦繼續維持之「利益權衡條款」卻未被我國個資法納入，導致我國非公務機關在蒐集、處理或利用一般個資時，有時難有適當之合法事由可以依循，無法確實平衡個人資料保護與個資合理利用之利益，甚至造成實務上限縮個人資料之定義、過度放寬公共利益之範圍、從寬認定對當事人權益無侵害或有利於當事人權益之現象。

有關利益權衡條款之重要性，可以自 2016 年 10 月歐洲法院（European Court of Justice）有關「動態網路位址 dynamic IP address）」資料是否屬於個人資料之判決充分得到展現。在上述判決中，歐州法院認為即使網路影音服務業者蒐集使用其服務消費者之動態網路位址，其本身並無可供對照組合之資料可以識別消費

者之身分（該額外之對照組合資料係由第三人，亦即提供該消費者上網服務之電信業者所保有），但因網路影音服務提供者在特定情況下（例如遭受駭客攻擊），可以請求有權機關命令電信業者提供額外可供對照組合之資料，藉以識別消費者之身分，因此對網路影音服務業者而言，動態網路位址資料，仍屬個人資料。[27] 值得注意者，歐州法院在採取上開見解後，進一步針對德國個人資料保護法僅在特殊情況下允許未經當事人同意而蒐集個人資料，欠缺利益權衡條款作為合法蒐集事由，認定其牴觸歐盟個資指令。

歐洲法院此一判決結果，在對個人資料之認定採取「擴張」見解之餘，同時肯定利益權衡條款之重要性，特別是在調和個人資料保護與個人資料合理利用上可以發揮之功能。換言之，歐洲法院一方面將動態網路位址資料納入個人資料保護之管制體系；另一方面，則肯定網路影音服務業者得以基於其合法利益（如：維護網路安全），透過利益權衡條款之操作，逕行蒐集、處理或利用動態網路位址資料。

回到我國個資法之規定，個資法第 19 條第 1 項第 7 款規定：「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」，即為以利益權衡之方式，作為個人資料蒐集、處理或利用合法事由之例；然而，上述規定限於個人資料係「取自一般可得之來源」（一般情形多為網際網路上之資料），適用範圍較歐盟個資規則狹窄，恐難以完整發揮利益權衡條款平衡資料當事人權益保護與個人資料合理利用之功能。尤其，如前所述，有鑑於我國部分實務見解，或出於對特定資料蒐集、處理或利用行為合理性之肯定，唯恐將特定資料（例如：電話號碼、電信業者別…）解釋為個人資料，將導致難以繼續合法使用之不合理結果，反而另闢蹊徑，將該等資料解釋為非個人資料，造成個人資料判斷標準之扭曲；抑或不當擴張其他合法蒐集事由之

[27] DLA Piper LLP, ECJ - Dynamic IP addresses constitute personal data and German law not compliant with Data Protection Directive, Oct. 20, 2016, http://www.lexology.com/library/detail.aspx?g=2f32162f-214c-41fc-8ab8-997ddf9ba418 (last visited Oct. 20, 2016).

範圍，設法將相關蒐集、利用行為合法化。本文因此建議，應參考歐盟個資規則之立法例，擴大利益權衡條款之適用範圍，使之成為「非」公務機關蒐集、處理或利用「一般個人資料」之一般性規定；亦即，不以資料係取自一般可得之來源者為限；允許資料管理者在個案中更廣泛地透過利益權衡之方式蒐集、處理或利用一般性個資，具體展現個資法兼顧與平衡個人資料保護與個人資料合理利用兩項利益之立法目的。至於特種個資部分，因特種個資原本即對資料當事人權益影響重大，一般而言，資料當事人對於禁止蒐集、處理或利用特種個資應有較值得保護之重大利益（個資法第 6 條第 1 項本文即原則上禁止蒐集、處理或利用特種個資），故不宜採取利益權衡條款作為蒐集、處理或利用特種個資之合法基礎。

**第八項 事前之安全管理機制--隱私影響評價（Privacy Impact Assessment, PIA）之增設**

隱私影響評價（Privacy Impact Assessment, PIA），PIA 係指在建立以資訊系統收集、處理個資檔案前，對當事人隱私權等權益可能造成之影響（risk）須先作評價，並檢視該資訊系統在技術上，是否為對個人權利影響最低限度之設計。此制度之理論依據與環境影響評估類似，因為環境一旦因開發公共事業而遭受破壞，即有難以回復原狀之特性；同理個資一旦依資訊系統處理成為檔案而利用，在網路上流出後，亦難以救濟；故在損害或風險未發生前，應先對系統設計、運用計畫及安全維護措施等事項進行評價，判斷是否能確保個人權利及適當、合法進行個資之處理；此制度之目的有三：1、確保安全、合法處理個資，其重點非僅在事故發生後之救濟，而應更積極在事前建立防止損害發生對策；2、其評價結果則由資訊管理者自己公布，提升資訊管理制度之透明度，以增加當事人之信賴；3、評價報告須報請獨立監督機關作確認，亦得擔保管理資訊系統者落實遵法（compliance）之義務[28]。

[28]新保史生，社会保障・税に関わる番号制度の導入とプライバシー，Nextcom，No.8，2011 年 12 月，頁 10。小林慎太郎，プライバシー影響評価（PIA）に基づく個人情報の有効活用を考える，NRI Public Management Review，vol. 113，2012 年 12 月，頁 5，網址 http://www.nri.co.jp/opinion/region/2012/pdf/ck20121203.pdf (最後瀏覽日：2016 年 6 月 25 日)。

日本於 2013 年 5 月 26 日定位為個資法特別法之「行政程序中為識別特定個人之編號利用法」（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，亦引進上開制度，於第 26 條、27 條法制化以下之評價制度：(1)、指針之作成與公布：特定個人情報保護委員會為確保特定個資之適當處理，應作成於欲保有特定個資檔案者，自己實施評價有關特定個資洩漏、其它事件發生之風險與影響，對抑制事件發生及適切管理特定個資所應採取措施之指針，並公布之。(2)、評價書之作成與公告：行政機關首長等欲保有特定個人資料檔案時，應依特定個人情報保護委員會規則，公告記載下列：①從事處理特定個人資料檔案事務之人數、②特定個人資料檔案所記錄特定個人資料之數量、③行政機關首長等過去處理個人資料檔案之狀況、④處理特定個人檔案事務之概要、⑤為處理特定個人資料檔案所使用之資訊處理組織構造及電腦處理等方式、⑥保護特定個人資料檔案所記錄特定個人資料之保護措施、⑦其它特定個人資料保護委員會規則所定事項之評價書，並廣徵民眾意見。(3)、評價書之承認：行政機關首長再充分考慮民間所提意見，作必要修正後，將該評價書上記載特定個人資料檔案處理方法，提交特定個人資料保護委員會承認。(4)、承認及公告:特定個人資料保護委員會應於審查上開資料檔案處理方法為符合前(1)之指針後，予以承認並迅速公告該當評價書。

此評價制度雖係針對利用電腦系統處理特定個資之行政機關等於建立系統前，要求其先作內部自我評估、檢視其是否能適法、安全處理特定人個資，在事前能確立有關資訊安全維護之制度。事實上對保有個資檔案一樣須負安全維護義務之非公務機關，亦應有其適用。

除日本法外，如前第二章所述，歐盟個資規則中更採取具體與抽象要件並列之方式，要求資料管理者針對「基於個人資料之自動化蒐集、處理或利用，對自然人個人進行系統性及大規模分析，並據以對特定個人作成具有法律效果之決定或產生類似影響」、「大規模蒐集、處理或利用第 9 條第 1 項規定之特種個人資料

或第 10 條規定之前科資料」、「大規模且系統性地監控公眾場所」，以及「可能造成資料當事人自由權利高度風險之資料利用行為」，於事前進行「個人資料保護影響評估」（第 35 條第 1 項及第 3 項參照）。至於評估之事項，除個資蒐集、處理或利用行為及其目的之具體描述，蒐集、處理或利用之合法事由為何外，也必須針對該資料使用與所設定目的間之必要性加以檢視；當然，最重要者之評估事項則是該行為對於資料當事人自由、權利可能造成之風險與資料管理者所採取之保護措施、安全措施（第 35 條第 7 項參照）。應注意者，依據歐盟個資規則第 83 條第 4 項之規定，違反個人資料保護影響評估規定者，將面臨最高一千萬歐元或前一年度全球營業額百分之二之罰鍰（以較高者計），足見歐盟對於個人資料保護影響評估之重視。

回到我國個資法之規定，現行個資法並未具體規定隱私影響評估或資料保護影響評估之機制，但個資法第 18 條及第 27 條分別要求公務及非公務機關應採行適當之安全維護措施，而依據個資法施行細則第 12 條第 2 項第 3 款之規定，所謂安全維護措施得包括「個人資料之風險評估及管理機制」，看似有類似之機制。然應說明者，上述「風險評估與管理機制」除內涵不若日本法及歐盟個資規則清晰、明確外；更重要者，此一安全維護措施之義務，解釋上應該係資料管理者已經蒐集、處理或利用相關資料「後」之「義務」，此與日本及歐盟法制強調「事前」之影響評估，實有相當差異。

值得注意者，個資法於 2015 年底部分修正，其中第 6 條第 1 項第 2 款及第 5 款均有「且事前或事後有適當安全維護措施」之文字。然一方面此一規定僅及於第 6 條所規定之特種個資；另一方面，此二款規定之適用範圍甚為有限（公務機關執行法定職務或非公務機關履行法定義務，或其他機關之協助行為），恐難以作為隱私影響評估之一般性規定。

本文認為，我國似有參考日本與歐盟之新規定，引進隱私影響評估（資料保護影響評估）機制之必要，將目前強調事中安全維護、事後處罰與損害賠償為主

之規範模式，適度轉向事前之評估與預防。尤其，在近年來強調政府資料開放與大數據分析之氛圍下，如何於「事前」透過一定之評估程序與機制，確保相關資料利用行為對於資料當事人權益不至造成侵害，恐怕是無法迴避之問題。

當然，考量隱私影響評估（資料保護影響評估）制度之實施，將伴隨一定之成本（包括專業人力），在制度設計上，應以資源較為豐沛之公務機關，以及進行特定資料資料蒐集、處理或利用行為之非公務機關（判斷標準可以「規模」及對資料當事人權利影響之嚴重程度判斷）為限。此外，亦可將此一制度與公務、非公務機關資料保護專責人員之設置適度連結（例如：由徵詢專責人員意見），以提升影響評估之專業性。

**第九項 跨境傳輸之管制**

關於個人資料之跨境傳輸，個資法第 21 條採取原則允許、例外限制之立法模式。詳言之，只有在個資之國際傳輸：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；或四、以迂迴方法向第三國（地區）傳輸個人資料規避本法，並且中央目的事業主管機關作成限制之決定後，方不得進行國際傳輸。據本文所知，目前實務上，僅少數中央目的事業主管機關曾作成限制傳輸之決定。反觀日本個資法及歐盟個資規則，則採取原則禁止、例外允許之立法模式，只有在確保資料當事人之權益能夠獲得適當程度保障之前提下，才可以進行個資之國際傳輸。

而在今日全球化之世界，個資之國際傳輸實為常態，無法避免，歐盟與日本所採取之原則禁止、例外允許模式，雖然對於資料當事人之權益能夠提供更周全之保障，但勢將造成欲進行國際傳輸之公務、非公務機關及中央目的事業主管機關龐大之遵法、執法成本。尤其，目前個資法並未設置專責之監督機關，各個中央目的事業主管機關各行其是之結果，除耗費資源外，勢必將產生對外國個人資料保護法制與實況，認定不一之問題。因此，短期內似可維持現制（亦即原則允許、例外禁止），並強化對當事人之告知，同時要求公務、非公務機關善盡安全

維護義務，不應國際傳輸而受影響，以確保當事人之權益；然自長遠看，若有專責監督機關之設置，能夠統一認定外國法制是否提供適當保障，或統一提出其他替代手段（如：標準契約條款），屆時再仿效歐盟與日本之立法例，將個資法目前「原則允許、例外禁止」模式改為「原則禁止、例外允許」，始能兼顧當事人權益之保障與認定之一致性。

**第十項 個資外洩通知義務**

2010 年個資法修正時，於第 12 條新增個資外洩通知義務之規定：「公務機關或非公務機關違反本法規定，致個人資料被竊取、洩漏、竄改或其他侵害者，應查明後以適當方式通知當事人。」至於通知之方式及內容，則於個資法施行細則第22條則進一步予以規範:「本法第十二條所稱適當方式通知，指即時以言詞、書面、電話、簡訊、電子郵件、傳真、電子文件或其他足以使當事人知悉或可得知悉之方式為之。但需費過鉅者，得斟酌技術之可行性及當事人隱私之保護，以網際網路、新聞媒體或其他適當公開方式為之（第 1 項）。依本法第十二條規定通知當事人，其內容應包括個人資料被侵害之事實及已採取之因應措施（第 2 項）。」

關於個資法個資外洩通知之規定，存在以下幾項問題，因而影響其成效。首先，有關通知之對象僅限於資料當事人，中央目的事業主管機關並不在通知之範圍內。因此造成中央目的事業主管機關無法第一時間掌握相關資訊，難以進行後續監督。其次，在要件上，上開規定以「違法個資法規定…致個人資料被竊取…」為通知之前提；然而，個資外洩通知義務之建置，主要著眼於使當事人知悉其個資已經外洩，藉以防止損害或避免損害擴大，至於資料管理者是否有違法之情事（通常係未盡安全維護義務）則非所問，現行規定以資料管理者違法為通知之要件，實有不當。第三、有關通知之時點，個資法僅泛稱「查明後」，可能導致公務、非公務機關藉機拖延；尤其，依據個資法第 48 條之規定，違反本條通知義務者，中央目的事業主管機關或直轄市、縣（市）應先限期改正，屆期未改正者，

方得按次處以罰鍰，更易使公務、非公務機關延宕通知，甚至遲至東窗事發，遭限期改正後，才進行通知。第四、依據現行規定，只要違反個資法規定導致個資外洩，似乎一律必須通知當事人，不論個資外洩是否果真對當事人之權益造成危險；此一立法模式，除可能增加公務、非公務機關之負擔外，對於資料當事人而言，也容易形成「狼來了」效應，亦即對類似通知產生麻木、輕忽之心態。

有鑑於個資法第 12 條之規定有上述缺漏，實宜參考歐盟個資規則之規定，將個資外洩通知義務分為「對監督機關之通知」及「對資料當事人」之通知兩類，並分別規定其通知之要件、通知時點及通知內容。此外，為避免過多無謂之通知可能造成資料當事人麻痺之結果，在對資料當事人通知之規定內，亦宜增加通知之門檻（如：可能對當事人權益造成風險）及免除通知義務之規定（如：資料管理者對於外洩的個人資料已採取適當地技術及組織上保護措施，使未經授權者，無法理解資料的內容），以求周延。

## 第十一項 當事人之權利

### 第一款 被遺忘權利之確認

被遺忘權利之討論，在歐盟基本權利憲章中可尋得其作為憲法層次基本權利之依據，並據此與其他類型之基本權利，例如：言論自由、資訊自由、新聞自由或是學術自由等，於具體個案中進行法益之權衡，但我國並未如歐盟或是德國，由憲法層次明確肯認其基本權利之地位。而在法律之層次，目前個資法第 3 條賦予當事人之權利，包括查詢或請求閱覽；請求製給複製本；請求補充或更正；請求停止蒐集、處理或利用以及請求刪除之權利。而同法第 11 條並要求公務機關或非公務機關應應主動或依當事人之請求更正或補充，以維護個人資料之正確性個人資料正確性，一旦遇有爭議，亦應主動或依當事人之請求停止處理或利用。我國個資法中雖未見被遺忘權之明文，但上述「刪除權」及「更正及補充權」之規定，若得配合個資法第 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」共同適用，在個案之解釋上，應該亦可從中導出「被遺忘權」之內涵予以適用。

但目前被遺忘權利在落實上所遭遇之最大困難，應即為如何將當事人被遺忘之權利，與代表公益或第三人之權益之，進行妥適之法益權衡，並建立較為明確清楚、且具有一致性之判斷標準。因此，實應持續關注歐盟個資規則施行後，各會員國對於被遺忘權所採行之作法以及所遭遇之困境，並透過個案之蒐集，釐清歐盟在被遺忘權在憲法及法律層次之操作標準，以作為我國個資法中刪除權行使要件明確化之參考；同時亦應思考建立相關配套，例如：協助非公務機關建立相關之審核標準及機制，並提供非公務機關所需之諮詢與建議等，以為因應。

**第二款 資料可攜權之賦予**

歐盟個資規則強化了當事人之權利，其中亦於第 20 條確認了當事人享有資料可攜權，據此，當事人得要求資料管理者就其個人資料，提供一共通形式之檔案，由資料管理者或當事人自行將該資料在不同資料管理者間傳輸，此一規定減輕了當事人在不同社群網絡中自由移動的難度，也減輕了資料管理者重新建立資料所需耗費之成本。但歐盟個資規則強調，資料可攜權與刪除權係相互獨立之權利，其主張不會互斥，且其行使需以不妨礙他人權利為前提。另外，歐盟個資規則亦授權各會員國得針對基於公益之檔案儲存目的之資料處理，訂定法令限制資料可攜權之行使（歐盟個資規則第 89 條第 3 項）。

我國個資法第 3 條第 1、2 款雖亦賦予當事人查詢或是請求製給複製本之權利，卻未明訂由當事人請求「攜帶」其個人資料之權利，亦未課予公務機關或非公務機關提供通用格式檔案之義務，但考量人民對於網路所提供之相關服務依賴程度與日俱增，而因此所累積之個人資料亦相當可觀，基於「個人自主控制個人資料之資訊隱私權」，亦考量對於當事人及資料管理者之便利性，若經當事人請求，應即許其個人資料得於不同資料管理者間自由傳輸流通。但該等權利之行使，仍須受有一定程度之限制，例如在基於檔案儲存目的處理個人資料之情況，若有

公益上之考量，資料可攜權之主張即有限縮之必要。

**第十二項 監督機關未設之問題**

我國個資法之監督機關，以公務機關或非公務機關所屬中央目的事業主管機關或直轄市、縣（市）政府為監督機關，惟於涉及個資法條文適用上之疑慮時，仍須仰賴法務部提供法律意見，自電腦處理個人資料保護法之時代起，至現今之個人資料保護法，雖亦累積了相當數量的函釋，得解決部分適用或解釋法律之疑義；然法務部非事業主管機關，對各種不同業界、領域處理個資之方式性質未必熟悉，對資訊科技操作技術無法全然掌握，又是與各部會平行之中央之二級機關，在施行之監督上能發揮之功能相當侷限。加諸現資訊網路極度普及下，許多新興事業乃為跨領域之業務或定性未明之業種，可能在發生問題時，如何確認其中央目的事業主管機關即先發生問題，造成三不管地帶，形成監督之漏洞。

另考量當事人與處理個資業者間，一旦發生紛爭時，因有資源、資力不對等之問題，又救濟程序費時，訟源增加之問題；如有一獨立機關得先介入當事人紛爭中調查、調解，對當事人之救濟較有利，亦可減少訟爭。最後，因網路無國界之故，個資之保護與被侵害救濟，需跨國之協力始能周全，在與外國協商合作個資法之執行，及跨境個資傳輸事務上，國家亦須有一統一對外窗口，較有效率及代表性。從而我國未來，為求能防止或解決跨國性個資侵害事件，在與各國交換意見、經驗，建立合作關係時，透過積極參與跨國組織或相關會議乃其必要之手段；然而，若我國未設置有具獨立性之個資監督機關，首先恐因未符合加入資格，而被拒於門外致使參與機會受限，如此不僅對於日益增多之跨境傳輸問題難以解決，亦將造成我國對個資之保護出現缺漏。

綜觀本計畫中所研究之歐盟及日本，雖可能在個資執行監督機關設置層級、組織方式及職權有所差異，但均將建置獨立監督機關視為完善個資保護所不可欠缺之環節。獨立監督機關之設置，應有助於統一法律解釋與適用，例如：資安維護制度之建立與風險評估，應不分領域公私要求具備一定水準，依同樣之標準進

行，凡此即應統一由專責機關監督執行，才可避免法解釋與適用之混亂，及安全維護標準之不一致之問題。另，個資之蒐集、處理及利用，為現今政府擬定政策、行政管理，大企業行銷所必須者，如何透過一獨立於政府機關外之監督機關，以中立立場，在不受政治等外力干涉下，公正、中立執法，監督政府機關或大企業依法蒐集、處理或利用個資，即有其重要性。故建置獨立之監督機關，藉由法律、資訊專業人員之組合之合議制方式，統一個資法執行之監督事務，對各機關、團體或個人有關個資問題作諮詢之服務，發現個資處理上有問題時，提供建議或調解糾紛，負責遵法之宣導、資訊安全、教育訓練等事宜，應可解決上開問題，亦可促進個資法之落實與發展；同時在跨國傳遞個資及個資法執行之國際協力上，能有一個統一對外代表窗口。

## 第二節 歐盟、日本及我國個資法制之比較

| 區域、國別<br>個資之定義與範圍 | 我國 | 日本 | 歐盟 |
|---|---|---|---|
| 個資之定義 | 第 2 條第 1 款<br>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。 | 第 2 條第 1 項<br>第 1 款　姓名、生、年、月、日及其他記述，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。<br>第 2 款　個人識別符號所包含者。 | 第 4 條第 1 項<br>任何有關一個已識別或足資識別自然人的資料；所謂足資識別之自然人指一個可以透過識別符號，例如：姓名、識別號碼、位置資料、線上識別碼，或經由其他一項或多項身體、生理、基因、精神、經濟、文化或社會身分特徵，直接或間接識別的自然人。 |
| 去識別化個資<br>加工匿名個資 | 第 6 條第 1 項第 4 款、第 9 條第 2 項第 4 款、第 19 條第 1 項第 4 款、第 20 條但書第 5 款「無從識別特定之當事人」指個人資料以代碼、匿名、隱藏部分資料或其他方式，無從識別該特定個人。 | 第 2 條第 9 項<br>「匿名加工資料」：加工於個人資料後，所得之無法識別特定個人，且無法復原者。<br>第 1 款　削除包含於該當個人資料中記述等之一部<br>第 2 款　削除包含於該當個人資料中所有個人識別符號 | 第 4 條第 5 項<br>去連結（pseydonymisatin）：個人資料經處理後，在不使用額外資料的情形下，無法將個人資料歸屬於特定個人的資料處理或利用方式；但該額外資料必須分別保管，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。 |

| | | | |
|---|---|---|---|
| 敏感性特種資料 | 第 6 條<br>病歷、醫療、基因、性生活、健康檢查及犯罪前科之個人資料<br>原則上須事先得到當事人同意，始能蒐集。 | 第 2 條第 3 項<br>本人之人種、信仰、社會身分、病歷、犯罪之經歷，因犯罪被害之事實及其他處理上不使對本人發生不當差別待遇、偏見其他不利益；而在處理上需要特別考量，依政令所指定之記述型等個人資料 | 第 9 條第 1 項將特種資料定義為：與民族或種族來源、政治見解、宗教或世界觀確信或所屬工會相關之個人資料，以及得明確識別特定人之基因資料、生物特徵資料，個人之健康資料或性生活或性傾向資料。<br>特種資料原則不得處理。但同條第 2 項列有例外得處理之十種情形。 |

| 區域、國別<br>規範對象<br>與適用地域範圍 | 我國 | 日本 | 歐盟 |
| --- | --- | --- | --- |
| 規範對象 | 公務機關、非公務機關、包括個人 | 1. 行政機關及公法人，另定有特別法規範。<br>2. 非公務機關第 2 條第 5 款，將個人資料庫等供事業之用者，不問是否營利。 | 第 4 條第 7 項<br>自然人、法人，公務機關，機構或其他組織（natural or legal person, public authority, agency or other body） |
| 適用除外 | 第 51 條<br>①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。<br>②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 | 第 76 條<br>1、 傳播機關、新聞社、通訊社、其他報導機關（包含以報導為業之個人）為提供報導之目的。<br>2、 以著述為業者，為供著述之目的。<br>3、 大學、其他以學術研究為目的之機關或團體、或為其所屬者，為供學術研究之用之目的。<br>4、 宗教團體，為供宗教活動（包含其附隨之活動）之用為目的。<br>5、 政治團體，為供政治活動（包含其附隨之活動）之用為目的。 | 第 2 條第 2 項<br>本命令之規定於以下情形不適用：<br>（a） 在一項不適用歐盟法的活動（activity）中之個人資料蒐集、處理或利用行為。<br>（b） 會員國在 TEU 第五編第二章規範下之活動<br>（c） 自然人純供個人或家庭活動<br>（d） 主管機關基於防止、偵察、調查或偵查犯罪、執行刑罰，包括維護或避免公共安全威脅等目的蒐集、處理或利用個人資料 |

| | | | |
|---|---|---|---|
| | | | |
| 適用地域範圍 | 1、 中華民國領域。<br>2、 第 51 條第 2 項:公務機關在中華民國領域外對中華民國人民蒐集個資者。 | 對日本國內之人提供物品或服務，而取得其本人之個人資料之個人資料處理事業者；即使在國外處理利用該當個人資料或使用該當個人資料所作成之匿名加工資料者，亦有適用。 | 第 3 條<br>本命令適用於設立於歐盟境內之資料管理者或受託者所為之個人資料處理活動；不論該資料處理活動是否發生於歐盟境內。<br>本命令適用於非設立於歐盟境內之資料管理者或受託者，對於歐盟境內之資料當事人為以下行為而蒐集、處理或利用個人資料之情形：<br>(a) 提供商品或服務；無論資料當事人是否需付款<br>(b) 在歐盟境內的行為（behaviour）進行監控（monitor）<br>本命令適用於非設立於歐盟境內，但基於國際公法，會員國之法律對之有適用之資料管理者。 |

| 區域、國別<br>蒐集處理之義務 | 我國 | 日本 | 歐盟 |
| --- | --- | --- | --- |
| 告知<br>（例外） | 第 8 條第 1 項<br>直接蒐集時原則應明確告知<br>第 8 條第 2 項<br>例外免告知<br>第 9 條第 1 項<br>間接蒐集時原則應明確告知<br>第 9 條第 2 項<br>例外間接蒐集免告知 | 1、 原則:取得個人資料時，除已預先公表其利用目的者外，應通知本人或公表之。<br>2、 特別規定:除為保護人之生命、身體或財產緊急而有必要者外，與本人間締結契約書、其他書面所記載該當本人資料，應預先對本人明示其利用目的。<br>3、 變更其利用目的時，應通知本人，或公表被變更之利用目的。<br>4、 例外:①對本人通知利用目的、或公表者，而有損害本人或第三人之生命、身體、財產、其他權利利益之虞；②有損害該當個人資料處理事業者之權利或正當利益之虞；③對國家或地方自治團體遂行法令所定事務有協助之必要，因通知本人利用目的、或公表時，對該當事務 | 第 12 條（告知的一般規定）<br>**第 1 項：告知事項應簡潔、清楚易懂、具有可接近性，使用淺白詞語，特別是向兒童告知時。**<br>第 2 項：標準（告知）標示的授權<br><br>第 13 條（直接蒐集）<br>**第 1 項及第 2 項（多層次告知）**<br>**第 1 項（一般告知）**：資料蒐集者的名稱、資料保護專責人員聯絡方式（如有適用）、蒐集資料的目的及合法事由、基於第 6 條第 1 項(f)款蒐集時之合法利益為何、個人資料的收受者或其類別、資料管理者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定<br>**第 2 項（為確保公平、透明之進一步告知事項）**：個人資料保存期限或其決定 |

| | | | |
|---|---|---|---|
| | | 之遂行有造成障礙之虞；④自其取得之狀況觀之，得認定其利用目的為明確等情形，不適用前三項規定。 | 標準、當事人相關權利、當事人得隨時撤回其同意、當事人向監督機關提出申訴之權利、提供資料是否是基於法律規定或契約要求或締結契約所必須、當事人是否得自由選擇提供個人資料及不提供對其權益的影響，以及是否存在自動化決定（automated decison-making），包括資料剖析（profiling），與自動化決定的邏輯與對當事人可能的影響<br>第 4 項：當事人已知悉相關資訊時不適用上述規定。<br><br>第 14 條（間接蒐集）<br>第 1 項（一般告知）：資料蒐集者的名稱、資料保護專責人員聯絡方式（如有適用）、蒐集資料的目的及合法事由、蒐集個人資料之類別、個人資料的收受者或其類別、資料管理者是否會將資料傳輸至第三國與歐盟執委會針對該第三國資料安全程度所做的決定<br>第 2 項(為確保公平、透明之進一步告知事項)：個人資料保存期限或其決定 |

| | | | |
|---|---|---|---|
| | | | 標準、基於第 6 條第 1 項(f)款蒐集時之合法利益為何、當事人相關權利、當事人得隨時撤回其同意、當事人向監督機關提出申訴之權利、個人資料的來源以及是否源自一般可得的來源，以及是否存在自動化決定（automated decison-making），包括資料剖析（profiling），與自動化決定的邏輯與對當事人可能的影響<br>第 3 項（告知的時機）<br>第 5 項：以下情形，不適用上述告知規定：<br>(a) 當事人已經知悉相關資訊<br>(b) 不能提供上述資訊或涉及不成比例的努力，特別是基於公益目的的檔案保存、科學或歷史研究目的或統計目的…<br>(c) 基於歐盟或會員國法律取得相關資料<br>(d) 基於歐盟或會員國法律所課予之職業上保密義務 |

| | | | |
|---|---|---|---|
| 利用目的之特定與限制 | 第5條 15條、16條、19條、20條<br>個人資料之蒐集、處理或利用，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。 | 第 15 條<br>個人資料處理事業者於處理個人資料時，應盡可能特定其利用之目的。<br>第 16 條<br>1、 原則:於事先未得本人同意下，不得逾越特定目的必要之範圍，為個人資料之處理。<br>2、 事業者因合併、其他事由，伴隨著事業繼承而自其他個人資料處理事業者取得個人資料時，於事先未得到本人同意下，處理該當個人資料不得超越為達成繼承前該當個人資料利用目的所必要之範圍。<br>3、 例外於：①基於法令；②為保護人之生命、身體或財產而有必要、為提升公眾衛生或推廣兒童之健全育成特別必要時，於得到本人同意為有困難者；③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，因得到本人同意，有對該當事務之遂行造成障礙之虞時，不適用之。 | 第 6 條<br>第 1 項（六款事由）：當事人同意、履行契約所必要、履行法定義務所必要、保護當事人或其他自然人重大利益所必要、為公共利益或基於法定職權所必要、基於資料管理者或第三人的合法利益但基於當事人更高之利益或自由權利而須保護其個人資料之情形，不在此限。<br><br>第 4 項(後續利用目的與蒐集目的是否相容的判斷) |

| | | | |
|---|---|---|---|
| 目的外利用<br>（提供第三人） | 第 16 條公務機關特定目的外利用：<br>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。<br>第 20 條非公務機關特定目的外利用：<br>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 | 第 23 條　原則上應事先得到當事人同意<br>1、 例外:①於法令規定者；②為保護人之生命、身體或財產而有必要，於得到本人同意為有困難時；③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，因得到本人同意，有對該當事務之遂行造成障礙之虞時，未事先得到本人之同意，得將該個人資料提供給第三人。<br>2、 opt—out 制:個人資料處理事業者對於被提供給第三人之個人資料，應本人之請求停止將得識別該當本人之資料對第三人提供者，關於下列事項，依個人資料保護委員會規則之規定，事先通知本人、或置於本人容易得知之狀態，並同時向個人資料保護委員會申報時，得該當個人資料提供給第三人。<br>①以對第三人提供為其利用目的。<br>②被提供給第三人之個人資料之項目。 | 第九章 針對特殊之處理情況<br>第 85 條 個人資料之處理與言論自由及資訊自由<br>1. 各會員國應制定法規，求取本規則所欲保護個人資料之權利與言論及資訊自由之間的平衡，包括出於新聞目的、學術、藝術或文學目的之處理。<br>2. 出於新聞目的、學術、藝術或文學目的之處理，各會員國得就本規則第 2 章（基本原則）、第 3 章（當事人權利）、第 4 章（管理者及受託利用者）、第 5 章（個人資料之第三國或國際組織傳輸）、第 6 章（獨立監督機關）及第 9 章（特殊處理情形）之規定，為不同或例外規定，但以為求取個人資料保護與言論及資訊自由之平衡所必要者為限。<br>第 86 條 處理及公開官方檔卷<br>行政機關、公法機構或履行公益任務之私法機構所持有官方檔卷中之個人資料，得依法令公開，以求取官方檔 |

| | | | |
|---|---|---|---|
| | 益無侵害。 | ③提供給第三人之方法。<br>④應本人之要求停止將得識別該當本人之個人資料對第三人提供。<br>⑤受理本人請求之方法。<br>3. 個人資料處理事業者變更前項第 2 號、第 3 號或第 5 號揭示之事項，應依個人資料保護委員會規則之規定，事先通知本人或置於本人容易得知之狀態，同時並向個人資料保護委員會申報。<br>4. 個人資料保護委員會於有依第 2 項申報時，應公告有關該當申報之事項。<br>5. 不該當於前開第三人者:<br>① 個人資料處理事業者於達成其利用目的所必要範圍內，因伴隨委託個人資料處理之全部或一部，而受該當個人資料之提供者。<br>② 因伴隨合併、其他事由繼承事業，而受該當個人資料之提供者。<br>③ 於特定人間被共同利用之個 | 卷向公眾公開與本規則所欲保護之個人資料權利之平衡。<br>第 87 條 國家代碼之處理<br>各會員國得進一步規定，在何種特定條件下，一般所理解之國家代碼或其他標示，得作為處理之標的。<br>第 88 條 受雇者之資料處理<br>1. 各會員國得透過法令或團體協約訂定特別規定，以保護關於受雇者個人資料於職業脈絡下處理之權利與自由，特別是為了聘用、履行勞動契約，包括履行透過法令或團體協約所確立之義務、管理、工作計畫及組織、工作場所之平等及多樣性、工作場所之健康及安全、保護雇主或客戶之財產權的目的以及與受雇者個別或集體權利及採行相關的目的，以及終止僱傭關係之目的。<br>2. 該規定應包括為維護人性尊嚴之適當及特殊措施，當事人之合法利益與權利，並特別關注處理過程之透明，公司集團間或與公司 |

| | | | |
|---|---|---|---|
| | | 人資料，被提供給該當特定人時，將其意旨及被共同利用個人資料之項目、共同利用者之範圍、利用者之利用目的及該當個人資料管理上負有責任人之姓名或名稱，預先通知本人或置於本人容易得知之狀態。<br>第 25 條（對第三人提供之記錄）<br>個人資料處理事業者將個人資料提供給第三人時，除該當於第 23 條第 1 項各號或第 5 項各號之任何之一者外，依個人資料保護委員會規則之規定，應作成提供之年、月、日、第三人之姓名或名稱，及其它個人資料保護委員會規則所定事項之記錄。<br>個人情報處理事業者，應自該當記錄作成之日起，依個人資料保護委員會規則所定期間，保存前項記錄。 | 共同進行經濟上活動之團體的資料傳輸，以及工作場所之監控系統。<br>第 89 條 保障基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理<br>1. 基於公益之檔案儲存目的、基於學術或歷史研究目的以及統計目的之處理，應遵循本規則對於當事人權利與自由之適度保障。其應確認合於資料縮減原則之技術和組織上之措施。該措施得以去連結之方式為之，若其有助於目的達成。所有資料再處理之情形，若其得於已無法識別當事人或已不可能之識別之情況下達成目的時，應即以此方式為之。<br>2. 基於學術或歷史研究目的以及統計目的處理個人資料，得於歐盟法或各會員國之法令中保留同條第 1 項所定條件與保障之適用，當第 15 條、第 16 條、第 18 條及第 21 條所定權利可能導致該特 |

| | | | |
|---|---|---|---|
| | | | 殊目的無法達成或受到嚴重妨礙且此例外（之限制）係屬達成目的所必要者。<br>3. 基於公益之檔案儲存目的處理個人資料，得於歐盟法或各會員國之法令中保留同條第 1 項所定條件與保障之適用，當第 15 條、第 16 條、第 18 條、第 19 條、第 20 條及第 21 條所定權利可能導致該特殊目的無法達成或受到嚴重妨礙且此例外（之限制）係屬達成目的所必要者。<br>4. 第 2 項與第 3 項之處理若同時具有其他目的，上述例外僅限於基於本條所稱目的之處理。 |
| 正確性與安全性確保 | 第11條第1項正確性確保<br>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。<br>第 11 條第 2 項正確性確保爭議處理<br>有爭議者，除因執行職務、業務所必須，或經當事人書面同意，並經註明其 | 第 19 條　資料之正確 最新性及刪除<br>個人資料處理事業者，於為達成利用目的之必要範圍內，於保持個人資料正確及最新內容之同時，於利用之必要消失時，應致力於刪除該當個人資料。<br>第 20 條　安全措施<br>個人資料處理事業者為防止其處理之 | 第 32 條（安全措施） |

| | | | |
|---|---|---|---|
| | 爭議者外，應主動或依當事人之請求停止處理或利用。<br>第 18 條公務機關安全性確保義務<br>應指定專人辦理安全維護事項，防止個人資料被竊取、竄改、毀損、滅失或洩漏。<br>第 27 條非公務機關安全性確保義務<br>應採行適當之安全措施，防止個人資料被竊取、竄改、毀損、滅失或洩漏。 | 個人資料之洩漏、滅失或毀損，及其他個人資料之管理，應採取必要且適當之措施。 | 考量科技水準、成本、資料蒐集之性質、範圍、脈絡及目的，風險可能性，以及涉及自由權利的嚴重性，資料管理者及受託者應採針對風險，採取適用的技術或組織措施，包括：<br>（a） 去連結或加密<br>（b） 確保秘密、完整、系統之可利用性<br>（c） 在物理或技術事故發生後，恢復個人資料的能力<br>（d） 定期檢查、評估相關措施之有效性 |
| 對境外之提供 | 第 21 條（對非公務機關之限制）<br>為國際傳輸個人資料，而有：<br>1、涉及國家重大利益；2、國際條約或協定有特別規定；3、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；4、以迂迴方法向第三國（地區）傳輸個人資料規避本法時，中央目的事業主管機關得限制之： | 第 24 條<br>個人資料處理事業者，對於位於外國之第三人提供個人資料時，除第 23 條第 1 項各號所揭示者之外，應事先得到當事人同意對外國之第三人提供之意思表示。 | 第 5 章（第 44 條至第 49 條）<br>第 44 條（一般原則：僅在符合本命令的條件下可以境外傳輸）<br>第 45 條（經執委會認定該第三國提供個人資料適當之保護）<br>第 46 條（資料管理者或受託者提供適當的安全維護措施且資料當事人權利可以執行並有有效救濟途徑存在）<br>第 47 條（具拘束力企業規則） |

| 區域、國別<br>當事人權利 | 我國 | 日本 | 歐盟 |
| --- | --- | --- | --- |
| 閱覽 | 第 3 條第 1、2 款<br>當事人就其個人資料依本法規定行使查詢或請求閱覽；請求製給複製本之權利，不得預先拋棄或以特約限制。<br>第 10 條　例外<br>除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者外，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。 | 第 28 條<br>1. 本人得對個人資料處理事業者，請求公開保有之個人資料。<br>2. 例外:①因公開而有該當於有損害於本人或第三人之生命、身體、財產、及其他權利、利益之虞者；②有對該當個人資料處理事業者業務之適當執行，造成明顯妨礙之虞者：③形成違反其他法令者外，得為全部或一部分之不公開。<br>3. 個人資料處理事業者對依第 1 項規定請求有關保有個人資料之全部或一部，為不公開之決定時，或該當保有個人資料不存在時，應對本人通知其意旨。 | 第 15 條<br>當事人得請求知悉其個人資料是否被蒐集、處理或利用，以及取得以下資訊：蒐集目的、資料類別、個人資料的收受者或其類別（特別是收受者位於第三國）、資料保存期間或其決定標準、相關權利、向監督機關提出申訴之權利、資料來源、是否存在自動化決定（automated decison-making），包括資料剖析（profiling），與自動化決定的邏輯與對當事人可能的影響。<br><br>第 23 條（相關權利的限制）：共 10 款事由 |

| | | | |
|---|---|---|---|
| 訂正 | 第 3 條第 3 款<br>當事人就其個人資料依本法規定行使請求補充或更正之權利，不得預先拋棄或以特約限制。<br>第 11 條第 1 項第 2 項<br>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；正確性有爭議者，除因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者外，應主動或依當事人之請求停止處理或利用。 | 第 29 條<br>1. 本人對個人資料處理事業者，於所保有其個人資料之內容非為事實時，得請求之訂正、追加或刪除。<br>2. 個人資料處理事業者於受理前項請求時，關於其內容之訂正等，除依其他法令規定定有特別程序者外，在達成利用目的之必要範圍內，應不予遲延，進行必要調查，基於其結果為該當個人資料內容之訂正等。<br>3. 個人資料處理事業者依第 1 項規定進行個人資料內容之全部或一部進行訂正等時，或決定不為訂正等時，對本人應不得遲延通知其意旨（包含進行訂正等時，其內容。）。 | 第 16 條 更正權<br>當事人有權要求管理者立即更正其不正確之個人資料，在與處理目的相符之範圍內，當事人有權要求將不完整之個人資料補全，即便是透過附加說明之形式為之。 |
| 刪除<br>停止利用 | 第 3 條第 4、5 款<br>當事人就其個人資料依本法規定行使請求停止蒐集、處理或利用、請求刪除之權利，不得預先拋棄或以特約限制。<br>第 11 條第 3 項<br>除因執行職務或業務所必須或經當事 | 第 30 條<br>1. 本人對個人資料處理事業者，違反第 16 條逾越特定目處理其個資，或第 17 條依不正當手段取得個人資料，或未得當事人事先同意取得敏感性資料時，得請求該當個人資 | 第 17 條 刪除權（被遺忘之權利）<br>1. 當事人有權要求管理者立即刪除其個資。有下列之一原因時，管理者負有刪除之義務：<br>(1) 該個資對於當時蒐集或處理之目的已無必要， |

| | | | |
|---|---|---|---|
| | 書面同意者外，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。 | 料之停止利用或刪除。<br>2. 除停止利用等需要高額之費用、其他因進行停止利用等有困難，而採取為保護本人權利利益所必要替代措施者外，個人資料處理事業者於受有前項請求時，判斷為有理由者，在修正違反之必要範圍內，應停止利用。<br>3. 本人對個人資料處理事業者違反第 23 條第 1 項或第 24 條規定，將該當本人資料提供給第三人時，得請求停止該資料對第三人提供。<br>4. 除該當個人資料之停止對第三人提供需要高額之費用、其它停止對第三人提供為有困難，而採取為保護本人權利利益所必要之替代措施者外，個人資料處理事業者於受有依前項規定之請求，判斷為有理由時，應不遲延停止該當個人資料之對第三人提供。<br>5. 個人情報處理事業者對依第 1 項規定請求之保有個人資料全部或一部為停止利用等、或決定不為利用 | (2) 當事人撤回（widerrufen）依據第 6 條第 1 項第 a 款或第 9 條第 2 項第 a 款進行資料處理所需之同意，且該處理欠缺其他之法律基礎，<br>(3) 當事人依據第 21 條第 1 項對於處理提出異議，且該處理未具備有更優先之正當理由，或當事人依據第 21 條第 2 項對於處理提出異議，<br>(4) 個人資料之處理係屬違法，<br>(5) 個資的刪除係管理者依據歐盟法或各會員國法規履行法定義務所必要，<br>(6) 個資已由資訊社會所提供服務依據第 8 條第 1 項進行蒐集。<br>2. 若管理者已將個資公開且依據第 1 項之規定負有刪除義務，其應考量現行可行之科技技術及履行費用，選擇適當之措施，包括通知資料管理者關於當事人所提出刪除所有與其個資之連結或個資之影本或複本之要求。 |

| | | | |
|---|---|---|---|
| | | 等時，或對第 3 項規定請求之有關保有個人資料之全部或一部，停止對第三人提供，或決定不為停止提供時，對本人應不得遲延通知其意旨。 | 3. 第 1 項及第 2 項不適用，當處理乃<br>(1) 行使言論及資訊權，<br>(2) 為履行依據歐盟或各會員國法令所課予資料管理者之法定義務或受託者履行與公益相關或行使公權力所需之任務，<br>(3) 依據第 9 條第 2 項第 h 款及第 i 款及第 9 條第 3 項基於公共健康領域內之公益理由，<br>(4) 依據第 89 條第 1 項基於公益儲存檔案之目的，學術或歷史研究目的或統計目的，當第 1 項所定權利之行使可能對處理目的之實現造成嚴重妨礙或使其無法達成，或<br>(5) 主張、行使或防禦法律上之請求權所必要。 |

| 區域、國別<br>監督機制 | 我國 | 日本 | 歐盟 |
| --- | --- | --- | --- |
| 有無獨立監督機關之設置 | 無 | 第五章 個人資料保護委員會<br>新設設置之獨立機關、 | 第六章 獨立監督機關<br>（第 51-59 條） |
| 監督之權限 | 第 22 條第 1 項<br>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，<br>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。<br>第 25 條<br>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： | 第 40 條<br>1. 個人資料保護委員會於前二節及本節規定施行之必要範圍內，對個人資料處理事業者或匿名加工資料處理事業者有關於個人資料或匿名加工資料之處理，得要求提出必要之報告或資料之提出，或得使其職員進入該當個人資料處理事業者等之事務所、其他必要場所、質問有關個人資料等處理、或檢查帳簿書類及其他物件。<br>第 41 條<br>個人資料保護委員會於執行職務之必要範圍內，對個人資料處理事業者，得 | 第 58 條 職權<br>1. 調查權<br>(1) 向資料管理者、受託者或其代表指明、準備其履行任務所需之所有資訊，<br>(2) 以資料保護審核形式進行之調查，<br>(3) 依據第 42 條第 7 項審核驗證，<br>(4) 提醒資料管理者或受託者避免違反本規則之行為，<br>(5) 自資料管理者及受託者處取得其履行任務所必要之個人資料及資訊，<br>(6) 依據歐盟或各會員國之程序法令 |

| | | | |
|---|---|---|---|
| | 一、禁止蒐集、處理或利用個人資料。<br>二、命令刪除經處理之個人資料檔案。<br>三、沒入或命銷燬違法蒐集之個人資料。<br>四、公布非公務機關之違法情形，及其姓名或名稱與負責人。<br>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。 | 為有關個人情報等之處理必要之指導及建議。<br><br>第 42 條<br>1. 個人資料保護委員會對個人資料處理事業者違反第 16 條至第 18 條、第 20 條至第 22 條、第 23 條（第 4 項除外）、第 24 條、第 29 條第 2 項或第 3 項、第 30 條第 2 項、第 4 項或第 5 項、第 33 條第 2 項、或第 36 條（第 6 項除外）之規定者，或匿名加工資料處理事業者違反第 37 條或第 38 條之規定者，認為保護個人權利利益而有必要時，得對該當個人資料處理事業者等為應採取終止該當違反行為，其他改正違反所必要措施之勸告。<br>2. 個人資料保護委員會於依前項規定受到勸告之個人資料處理事業者等，無正當理由而未採取有關其勸告之措施，而認為對個人重大權益利益之迫切侵害時，對該當個人 | 進入資料管理者及受託者之營業處所，包括所有處理資料之設施及工具。<br>2. 輔助權(Abhilfebefugnise)<br>(1) 警告資料管理者或受託者其預計採行之處理流程可能違反本規則，<br>(2) 警告資料管理者或受託者其所採行違反本規則之處理流程，<br>(3) 向資料管理者或受託者指明，滿足當事人依據本規則所享有權利，<br>(4) 向資料管理者或受託者指明其處理流程，應透過特定方式及於特定時間內達到本規則之要求，<br>(5) 提醒資料管理者，通知個人資料受侵害之當事人，<br>(6) 處以暫時或永久的限制處理，包括禁止（處理），<br>(7) 個人資料之更正或刪除或依據第 16、17 及 18 條之限制處理，以及通知依據第 17 條第 2 項及第 19 條公開個人資料之接收者，關 |

| | | | |
|---|---|---|---|
| | | 資料處理事業者等得命令其應採取有關其勸告之措施。<br>3. 個人資料保護委員會於個人資料處理事業者違反第 16 條、第 17 條、第 20 條至第 22 條、第 23 條第 1 項、第 26 條或第 36 條第 1 項、第 2 項或第 5 項之規定者，或匿名加工資料處理事業者違反第 38 條之規定者，認為因有侵害個人重大權利利益之事實而有採取緊急措施之必要時，對該當個人資料處理事業者等，得命令中止該當違反行為、其他為改正違反上應採取之必要措施，不受前二項規定之適用。 | 於應採行之措施，<br>(8) 撤回認證或要求認證機關廢止依據第 42 及 43 條核發之認證，或要求認證機關停止發給認證，當不符或或不再符合認證之標準，<br>(9) 依據第 83 條處以罰金，依據個案之情況加上或以本項所定措施取代之，<br>(10) 暫時停止向位於第三國或國際組織之接收者傳輸資料。<br>3. 許可權及諮詢權<br>(1) 依據第 36 條之事前協商程序，提供資料管理者諮詢<br>(2) 對於所有與個人資料保護相關之問題，自行或經詢問向各國國會、各會員國政府、或在符合各會員國法令之規定下，向其他機構及單位以及公眾提供意見，<br>(3) 核准依據第 36 條第 5 項之處理，當會員國之法令要求此種事前許可時，<br>(4) 提出意見，並批准依據第 40 條第 5 項擬定之行為準則草案， |

| | | | |
|---|---|---|---|
| | | | (5) 依據第 43 條對驗證機關進行認證，<br>(6) 發給與第 42 條第 5 項相符之驗證，及批准認證標準，<br>(7) 依據第 28 條第 8 項及第 46 條第 2 項擬定資料保護之標準條款，<br>(8) 依據第 46 條第 3 項第 a 款許可契約條款，<br>(9) 依據第 46 條第 3 項第 b 款核准行政協約，<br>(10) 依據第 47 條許可內部具拘束力之規範。<br>4. 救濟途徑之確保<br>監督機關行使本規則所賦予職權，應提供適當保障，包括有效之司法救濟及與歐盟法及各會員國法令相符之程序，以求取與歐盟基本權利憲章之一致性。<br>5. 舉發及訴訟參與<br>所有會員國得透過法令賦予其監督機關向司法機關舉發違反本規則行為之權限，同時進行或參與該司法程序，以落實本規則之規定。<br>6. 所有會員國得透過法令賦予其監 |

| | | | |
|---|---|---|---|
| | | | 督機關在第 1、2 及 3 項所定職權外之其他職權。該職權之行使不得影響第 7 章之有效實行。 |
| （地位） | | 第 62 條<br>委員會之委員長、委員為獨立行使職權之合議制機關。<br>內閣府外機關 | 第 52 條 獨立性<br>1. 所有監督機關依據本規則全然獨立地履行任務或行使職權。<br>2. 監督機關之成員依據本規則履行任務或行使職權時，不受到外界直接或間接之影響，亦無須請示或接受指示。<br>3. 監督機關之成員不得為與其擔任職務不相符之行為且不得於擔任職務期間執行其他與其職務不相符之有償或無償之職權。<br>4. 各會員國應確保各個監督機關所需人員、技術及經費來源、空間及設備之設置，以使其在職務協助、共同合作及委員會中協力之任務及職權得以實踐。<br>5. 每個會員國應確保各個監督機關選擇其人員，並受監督機關之指 |

| | | | |
|---|---|---|---|
| | | | 揮監督。<br>6. 每個會員國應確保各個監督機關之財政受到不影響其獨立性之監督，其得編列個別、公開、年度之預算，並作為總預算之一部分。 |

## 第五章 結論與具體建議

綜合本文前述對於歐盟個資規則（第二章）與日本新個資法（第三章）之介紹，以及對我國現行個資法面臨問題之比較分析（第四章），茲將本文認為短期立即可行之建議與中、長期努力方向，分別盧列說明如下，作為本計畫之結論。

### 第一節 短期立即可行之建議

在本文所探討之十二項個資法議題中，短期內可立即進行補強、修正之事項如下。

#### 一、 間接識別定義之釐清

由於目前實務上對於間接識別個人資料判斷所採取之標準寬嚴不一，本文認為法務部或可參考日本之作法，立即著手修正個資法施行細則第 3 條間接識別之定義，明定所採取之判斷標準究為資料管理者抑或一般人之標準。

#### 二、 適用除外規定之釐清

個資法第 51 條第 1 項第 1 款規定：「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」不適用個資法。在網際網路各項應用服務快速發展之今日，判斷恐日漸困難，實務上亦已出現不少爭議案件。本文因此認為法務部或可透過解釋（行政規則）之方式，具體說明本款規定適用時應該審酌之因素，如：是否限於與事業或商業活動無關…等，較具體確定其範圍，以提供未來實務適用之參考。當然，由於法務部之解釋對於其他機關，尤其是司法機關而言，並無拘束力；為減少法律適用上之不確定性，建立全國一致遵行之標準，亦可於未來中、長期修法時，能將實務上累積之審酌、判斷要素，具體轉化為法律之規定。

### 第二節 中程建議

除上述短期內立即可行之建議事項外，本文認為中程努力方向應係規劃通盤檢討、修正個資法之規定。以本文研究所及之議題而言，以下事項應列入個資法修正時之參考。

#### 一、 新增「間接識別」之判斷標準

有關間接識別之判斷標準，除了短期可以透過修正個資法施行細則之方式，試圖予以釐清外，亦可配合個資法之修正，直接在個資法中明定採取何種標準（包括究竟以「個資處理事業者」或「一般人」為標準，又在識別之可能性上，是否採取歐盟「所有合理可能手段」標準）。

## 二、 新增「去個人識別性」個資之定義

展望未來，如在政策上確定將進一步推動大數據相關應用，宜參考歐盟個資規則及日本新個資法之規定，增定「去個人識別性」個資（或稱為「去連結個資或假名化個資」）之定義，並明定去個人識別性之基準、程序（包括驗證）等事項，同時進一步檢討是否放寬此類去個人識別性個資蒐集、處理或利用之範圍。

## 三、 敏感性特種資料之定義

有關個資法第 6 條敏感性特種資料之定義，建議考量時代環境變遷、科技技術發展與民眾對於隱私權認知的改變，納入具體特種個人資料之類型，例如：種族或民族、工會會員資格、社會身分等。

## 四、 擴大個資法適用地域範圍

基於我國人民大量使用境外網路購物平台、影音平台或是雲端服務，為避免形成保護漏洞，並回應歐盟、日本等主要國家擴張其各自個資法保護法令適用地域範圍之趨勢，本文建議未來個資法修正時，至少應將「對中華民國境內人民銷售物品或提供服務」，因而蒐集、處理或利用個人資料之境外資料管理者，亦納入個資法之適用範圍。

## 五、 告知義務規定之修正

參考本次歐盟個資規則修正之立法例，個資法未來修正時，亦應將告知義務之強化列為修正重點。至於修正內容，應包括以下幾項：

- 增定告知之一般性要求，如：「告知事項應簡潔、清楚易懂、具有可接近性，使用淺白詞語」。
- 在告知事項方面，應要求告知蒐集之合法事由；有關利用時間，如無法具體

說明期間之末日者，至少應告知決定利用期間之標準；有關利用地區，應僅限於資料管理者欲將蒐集之資料傳遞至境外處理或利用之情形才須特別說明；有關利用對象，似可保留一定彈性，在個案中允許僅告知利用對象之類型；至於「利用方式」，似可限於利用個資作成自動化決定或剖析等特殊方式時，才告知。

- 在免除告知義務之事由方面：在直接蒐集之情形，免告知之事由應大幅刪減，僅於當事人已知悉相關資訊時方得免除告知義務；至於在間接蒐集方面，目前多數免告知事由仍有維持必要，但「當事人自行公開或其他已合法公開之個人資料」是否可以免除告知義務，宜審慎檢討。

**六、 非公務機關蒐集、處理或利用一般個資應增定「利益權衡條款」**

為具體展現個資法兼顧與平衡個人資料保護與個人資料合理利用兩項利益之立法目的，避免實務過度限縮個人資料定義、過度擴張公共利益或有利於當事人權益等合法事由之範圍，建議仿照歐盟個資規則，將利益權衡條款（亦即：「為資料管理者或第三人合法利益所必要。但資料當事人對該資料之保護具有更重要利益者，不在此限」）納入非公務機關蒐集、處理或利用「一般個資」之合法事由（同時配合刪除現行個資法第 19 條第 1 項第 7 款之規定）。應附帶說明者，因公務機關蒐集、處理或利用個人資料宜有法律明文規定之具體、明確基礎，故本文贊同歐盟個資規則之規定，「不建議」將利益權衡條款納入公務機關蒐集、處理或利用一般個資之合法事由中。

**七、 增定「隱私影響評估」機制**

為妥善控制、避免政府資料開放與大數據分析等可能對於資料當事人權益產生重大影響之資料蒐集、處理或利用行為，建議參考日本或歐盟有關隱私影響評估之建制方式，課予公務機關及進行特定資料蒐集、處理或利用行為之非公務機關（判斷標準可以「資料蒐集、處理或利用之規模」及「對資料當事人權利影響之嚴重程度」判斷），進行「事前」隱私影響評估（資料保護影響評估）之義務。

### 八、 修正個資外洩通知義務之規定

目前個資法個資外洩通知義務僅限於對當事人為之，造成中央目的事業主管機關監督不易，未來個資法修正時，建議將個資外洩之通知義務分為「對監督機關之通知」及「對資料當事人之通知」兩類，並分別規定其通知之要件、通知時點及通知內容。同時，為避免過多無謂之通知可能造成資料當事人麻痺之結果，在對資料當事人通知之規定內，亦宜增加通知之門檻及免除通知義務之規定。

## 第三節 遠程建議

### 一、 當事人權利：被遺忘之權利

未來個資法修正時，可觀察歐盟被遺忘權實施之狀況，將我國個資法中關於刪除權行使之要件明確化，並建立相關配套，例如：協助非公務機關對於當事人行使刪除權之情況，建立相關之審核標準及機制。

### 二、 資料可攜權之要件

基於當事人所享有之個人自主控制個人資料權，建議可依據我國人民使用網路之習慣以及新興之資訊服務類型，將資料可攜權納入當事人得主張之權利類型中，善用科技發展強化資料利用之便利性，但應同時妥適權衡可能衝突之法益，並將其要件明確化。

### 三、 修正個人資料跨境傳輸之限制規定

為有效確保資料當事人之權益，對於個人資料之跨境傳輸，建議於設置專責監督機關之前提下，改採原則禁止、例外允許之立法例；如此才能統一認定外國法制是否提供適當保障，或統一提出其他替代手段（如：標準契約條款）。反之，若未來仍保留目前由各中央目的事業主管機關負責執法之模式，則仍以維持現行個資法「原則允許、例外禁止」之模式為宜，以避免各目的事業主管機關各行其是之耗費資源，甚至大幅增加認定歧異之情況。

### 四、 獨立監督機關之設置

本文認為未來應建置獨立行使職權之監督機關，專司個人資料保護之職權，或亦可參考德國之作法，將資訊公開之業務，一併交由同一機關掌理。而其組織

及職權亦得參考日本或歐盟之體制。至於此一機關之層級，如第四章所述，若能說服立法院修正中央行政機關組織基準法，突破二級獨立機關數量之限制（或直接於個資法中明定「不受中央行政機關組織基準法之限制」），仍以中央二級機關為宜，以確保其具有適當之監督、協調地位。若增設二級獨立機關確有困難，亦宜仿照飛航安全調查委員會之設計，設置直屬行政院之三級獨立機關；但應強調者，在組織規模及員額上，考量個資（甚至資訊公開）業務涉及日常監理、相關指引之發布，甚至爭議裁決，宜有充足之配置，併此敘明。

## 參考文獻資料

### （一） 中文文獻

#### 1. 書籍

陳敏，行政法總論，自刊，2013 年 9 月，8 版。

李明勳，合理隱私期待之研究－以定位科技為例，國立政治大學法律學研究所碩士論文，2013 年 7 月。

#### 2. 期刊論文

范姜真媺，日本個人編號法對我國之借鏡，東吳法律學報，第 26 卷第 2 期，頁 1-33，2014 年 10 月。

范姜真媺，個人資料保護法關於「個人資料」保護範圍之檢討，東海大學法學研究，第 41 期，頁 91-123，2013 年 12 月。

范姜真媺，日本資訊公開救濟程序之探討，東吳法律學報，17 卷 1 期，頁 31-80，2005 年 8 月。

許炳華，被遺忘的權利：比較法之觀察，東吳法律學報，第 27 卷第 1 期，頁 125-163，2015 年 7 月。

徐彪豪，M2M 時代下的資料保護權利之進展-歐盟與日本觀察，科技法律透析，25 卷 11 期，頁 47-62，2013 年 11 月。

楊智傑，個人資料保護法制上「被遺忘權利」與「個人反對權」：從 2014 年西班牙 Google v. AEPD 案判決出發，國會月刊，第 43 卷第 7 期，頁 19-43，2015 年 7 月。

劉定基，雲端運算與個人資料保護－以台灣個人資料保護法與歐盟個人資料保護指令的比較為中心，東海大學法學研究，第 43 期，頁 53-106，2014 年 8 月。

劉定基，析論個人資料保護法上「當事人同意」的概念，月旦法學，第 218 期，頁 146-167，2013 年 7 月

劉定基，個人資料的定義、保護原則與個人資料保護法適用之例外—以監視錄影為例（上），月旦法學教室第 115 期，頁 42-54，2012 年 5 月。

劉靜怡，社群網路時代的隱私困境：以 Facebook 為討論對象，臺大法學論叢，第 41 卷第 1 期，頁 1-70，2012 年 3 月。

#### 3. 網路資料

邱伊翎，新聞自由、隱私與個資法，2010 年 5 月 3 日，http://www.tahr.org.tw/node/176 （最後瀏覽日期：2016 年 11 月 20 日）。

吳敏華，從法律應然面與媒體採訪工作實然面出發－評析個人資料保護法第六條、第八條，http://ccs.nccu.edu.tw/word/HISTORY_PAPER_FILES/1509_1.pdf （最後瀏覽日期：2016 年 11 月 20 日）。

## （二） 日文文獻

### 1. 書籍

日置巴美、板倉陽一郎，平成 27 年改正個人情報保護法のしくみ，商事法務，2015 年（平成 27 年）。

田島泰彦、三宅弘編，個人情報保護法，明石書店，2003 年（平成 15 年）。

瓜生和久，平成 27 年改正個人情報保護法，商事法務，2015 年（平成 27 年）。

宇賀克也，個人情報保護法の逐条解説（3 版），有斐閣，2009 年（平成 21 年）。

宇賀克也，個人情報保護法の逐条解説（4 版），2016 年（平成 28 年）。

岡村久道，個人情報保護法（新訂版），2009 年（平成 21 年）。

岡村久道，個人情報保護法，商事法務， 2005 年（平成 17 年)。

鈴木正朝，個人情報保護とコンプラインス•プログラム」，商事法務，2005 年（平成 17 年)。

園部逸夫編集，個人情報保護法の解説，ぎょうせい，2003 年(平成 15 年)。

藤原静雄，逐条個人情報保護法，弘文堂， 2003 年（平成 15 年）。

### 2. 期刊論文

小林慎太郎，「匿名加工情報」によるビッグデータビジネス活性化への期待と課題，知的資產創造，23 卷 10 号，2015 年 10 月（平成 27 年）。

久保田正志，パーソナルデータの利活用と個人情報保護法改正，法と調查，No360，2015 年 1 月（平成 27 年）。

宇賀克也，個人情報匿名加工情報・個人情報取扱業者，ジュリスト，No.1489，2016 年 2 月（平成 28 年）。

宇賀克也，個人情報保護法改正について(1)，情報公開•個人情報保護，Vol.59，2015 年（平成 27 年）。

宇賀克也，個人情報保護法改正案について(2)，季報情報公開・個人情報保護，

Vol.58，2015 年（平成 27 年）。

宍戸常寿，個人情報保護法制， 論究ジュリスト，No.13，2015 年 4 月（平成 27 年）。

青木耕一，企業による個人情報保護と流出対應，法律のひろば，2008 年 9 月（平成 20 年）。

岡村久道，ビッグデータの法的処理―個人識別性と非識別化の問題を中心に，法とコンピュータ学会研究会報告，No.32，July 2014（平成 26 年）。

宮下紘、プレイバシーイヤー2012、NEXT COM, Vol. 2012 winter

森亮二，個人情報の保護と利用，法律時報，88 巻 1 号，2016 年 1 月（平成 28 年）。

森亮二，實務解說平成 27 年改正個人情報保護法(第 1 回)，NBL，No.1059，2015 年 10 月（平成 27 年）。

森亮二，平成 27 年改正個人情報保護法(第 2 回)個人情報の定義，NBL，No.1601，2015 年 11 月（平成 27 年）。

森亮二，パーソナルデータの匿名化をめぐる議論，ジュリスト，No.1464，2014 年 3 月（平成 26 年）。

鈴木正朝，個人情報保護のための企業法務，法律ひろば，2003 年 9 月（平成 15 年）。

新保史生，パーソナルデータの利活用を促進するための枠組みの導入等，自由と正義，65 巻 12 号，2014 年（平成 26 年）。

新保史生，社会保障・税に関わる番号制度の導入とプライバシー，Nextcom，No.8，2011 年 12 月（平成 23 年）。

関啓一郎，個人情報保護法とその 10 年ぶりの改正について，知的資產創造，23 巻 10 号，2015 年 10 月（平成 27 年）。

藤原靜雄，個人情報保護制度の課題について，季報情報公開・個人情報保護，Vol.30，2008 年 9 月（平成 20 年）。

### 3. 網路資源

小林慎太郎，プライバシー影響評価（PIA）に基づく個人情報の有効活用を考える，NRI Public Management Review，Vol. 113，2012 年 12 月，網址 http://www.nri.co.jp/opinion/region/2012/pdf/ck20121203.pdf (最後瀏覽日：2016 年 6 月 25 日)

## （三） 英文文獻

### 1. 書籍

CHRITOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW (2013).

### 2. 期刊論文

Francoise Gilbert, *European Data Protection 2.0: New Compliance Requirements in Sight—What the Proposed EU Data Protection Regulation Means for U.S. Companies,* 28 SANTA CLARA COMPUTER & HIGH TECH. L. J. 815 (2012).

Paul M. Schwartz, *EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation*, 12 BNA PRIVACY AND SECURITY LAW REPORT 718 (2013).

### 3. 網路資料

Article 29 Data Protection Working Party, *Opinion on the Use of Location Data with a View to Providing Value-added Services* (November 2005), available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp115_en.pdf.

Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data* (June 20, 2007), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, 11, No. 01197/11/EN, WP 187 (July 13, 2011), available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.

Council of Europe, *The Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: Propositions of Modernization*, November 2012(29th Plenary meeting), available at http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Terms%20of%20reference%20-%20Ad%20hoc%20committee%20on%20data%20protection%202013.pdf

DLA Piper LLP, ECJ - Dynamic IP addresses constitute personal data and German law not compliant with Data Protection Directive, Oct. 20, 2016, http://www.lexology.com/library/detail.aspx?g=2f32162f-214c-41fc-8ab8-997ddf9ba418 (last visited Oct. 20, 2016).

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, available at

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at http://www.oecd.org/sti/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

## （四） 德文文獻

### 1. 專書

*Tinnefeld, Marie-Theres/ Buchner, Benedikt/ Petri, Thomas,* Einführung in das Datenschutzrecht, 5. Aufl., 2014.

### 2. 期刊論文

*Benecke, Alexander/ Wagner, Julian*, Ö ffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG- Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, DVBl 10/2016.

*Boehme-Neßler, Volker*, Das Recht auf Vergessenwerden- Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ 13/2014.

*Kühling, Jürgen/ Martini, Mario*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht? EuZW 12/2016.

*Meyer, Sebastian/ Rempe, Christoph*, Aktuelle Rechtsentwicklungen bei Suchmaschinen, K&R 5/2016.

*Schaar, Peter*, Datenschutz-Grundverordnung: Arbeitsauftrag für den deutschen Gesetzgeber, PinG 2/2016.

*Voßhoff, Andrea/ Hermerschmidt*, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung, PinG 2/2016.