

跨境隱私管理機制— GDPR下的透明與同意

達文西個資暨高科技法律事務所

王慕民 律師

muming@davinci.idv.tw

2019 年 9 月 11 日

足夠透明是有效同意的前提

ARTICLE 29 DATA PROTECTION WORKING PARTY



17/EN
WP259 rev.01

Article 29 Working Party
Guidelines on consent under Regulation 2016/679

Adopted on 28 November 2017
As last Revised and Adopted on 10 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE

PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.
The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-58 02/013.
Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=8936

ARTICLE 29 DATA PROTECTION WORKING PARTY



17/EN
WP260 rev.01

Article 29 Working Party
Guidelines on transparency under Regulation 2016/679

Adopted on 29 November 2017
As last Revised and Adopted on 11 April 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

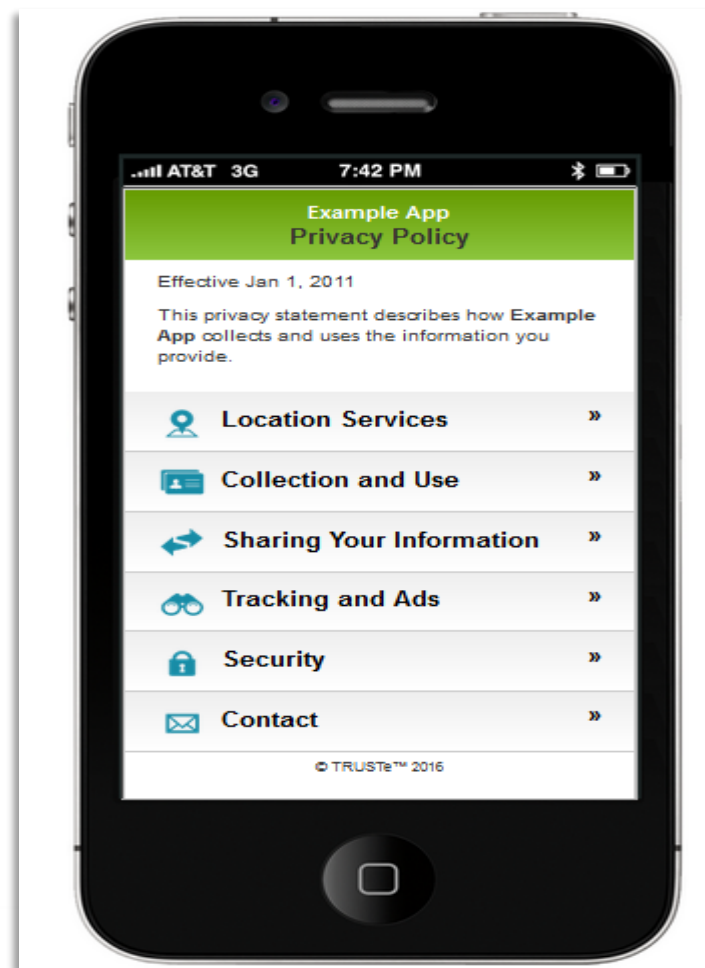
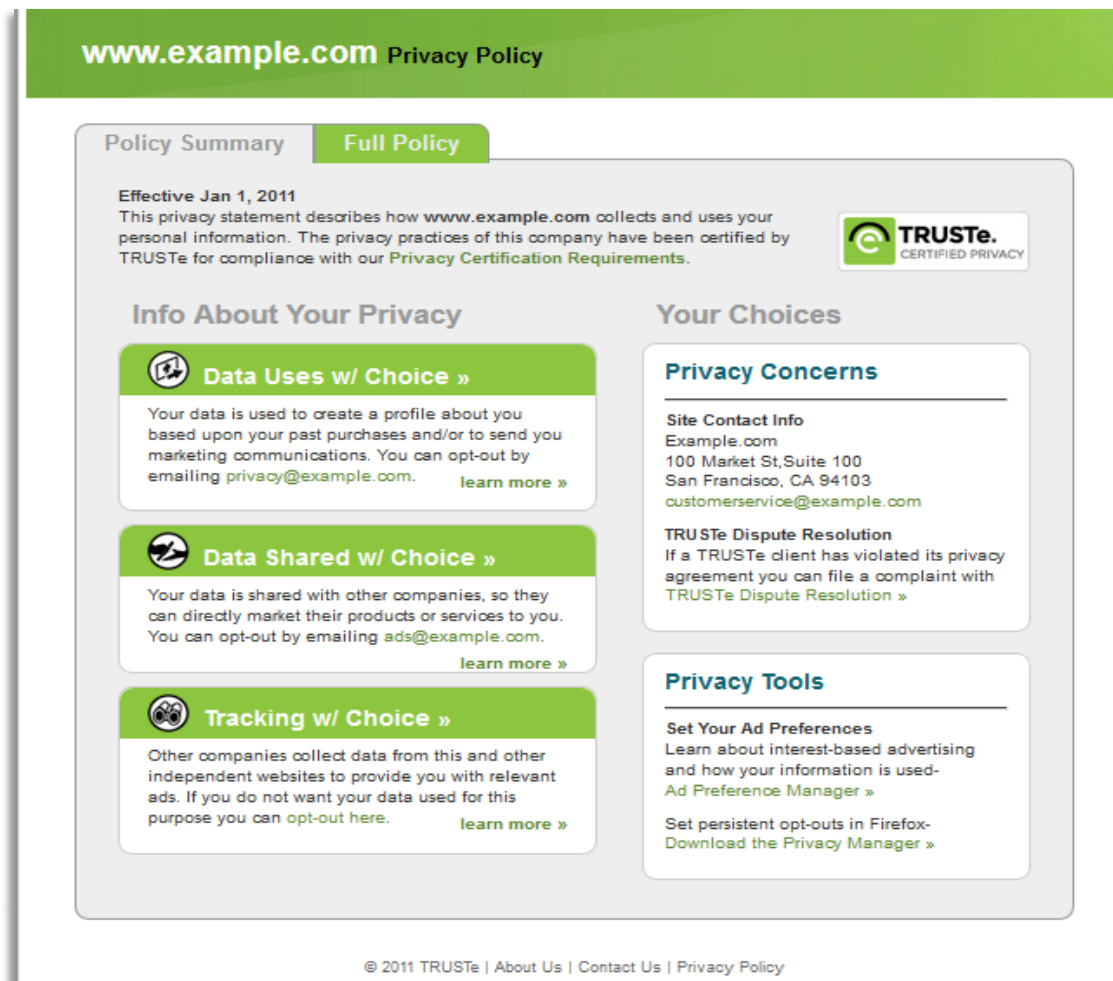
HAS ADOPTED THE PRESENT GUIDELINES:

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-58 02/013.

Website: http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358&tpa_id=8936

透明方式多元



(圖片來源：TRUSTe)

透明方式多元

The image shows a screenshot of the UK Information Commissioner's Office (ICO) website. A blue cookie consent overlay is visible on the left side of the screen. The main content area displays the 'Your data matters' section, which includes a search bar and a list of links. The 'In detail' section lists various topics related to privacy information, such as 'Are there different ways we can provide privacy information?' and 'What is a layered approach?'. The 'Save and close' button is located at the bottom of the cookie consent overlay.

Our use of cookies

We use necessary cookies to make our site work. We'd also like to set optional analytics cookies to help us improve it. We won't set optional cookies unless you enable them. Using this tool will set a cookie on your device to remember your preferences.

For more detailed information about the cookies we use, see our Cookies page [link](#)

Necessary cookies

Necessary cookies enable core functionality such as security, network management, and accessibility. You may disable these by changing your browser settings, but this may affect how the website functions.

Analytics cookies ☐ Off

We'd like to set Google Analytics cookies to help us to improve our website by collecting and reporting information on how you use it. For more information on how these cookies work please see our 'Cookies page'. The cookies collect information in an anonymous form.

Save and close

ICO.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

[Your data matters](#) [For organisations](#) [Make a complaint](#) [Action we've taken](#) [About the ICO](#)

[Organisations](#) / [Guide to Data Protection](#) / [The General Data Protection Regulation \(GDPR\)](#) / [The right to be informed](#) /

What methods can we use to provide privacy information?

[Share](#) [Download options](#)

[this document](#) [In detail](#)

[this detailed guidance](#)

[Is the right to be informed and why is it important?](#)

[What privacy information should we provide?](#)

[Should we provide privacy information?](#)

[Are there any exceptions?](#)

[Should we draft our privacy information?](#)

[What methods can we use to](#)

[Are there different ways we can provide privacy information?](#)

[What is a layered approach?](#)

[How can dashboards help?](#)

[What is a just-in-time notice?](#)

[Can we use icons as well?](#)

[How can we provide people with privacy information on mobile devices?](#)

[What about the Internet of Things and other smart devices?](#)

Are there different ways we can provide privacy information?

Yes, you should not necessarily restrict the delivery of privacy information to a single notice or page on your website. The term 'privacy notice' is often used as a shorthand term, but rather than seeing the right to be informed as being about

(圖片來源：ico.org.uk)

透明方式多元

Create an account

Title

Mr

Name

Joe Bloggs

Email address

Username

Password

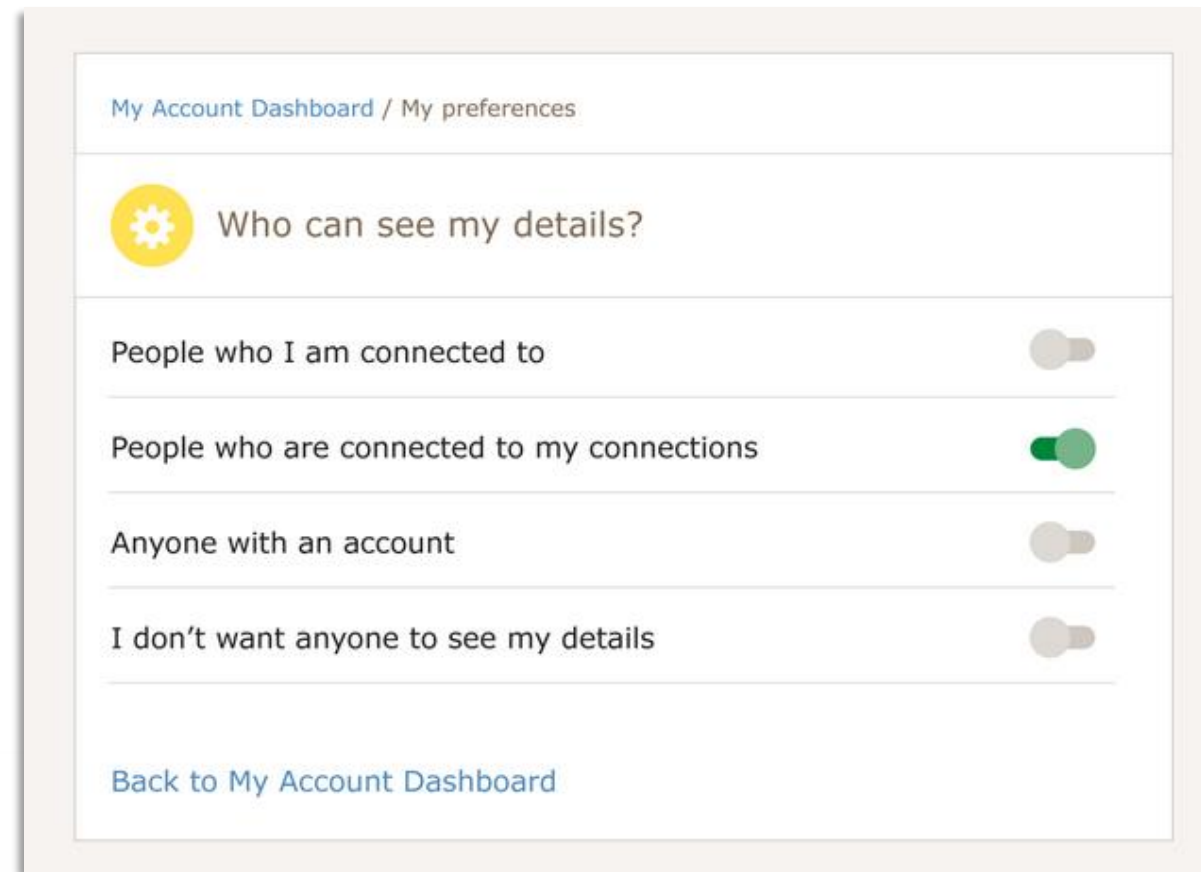
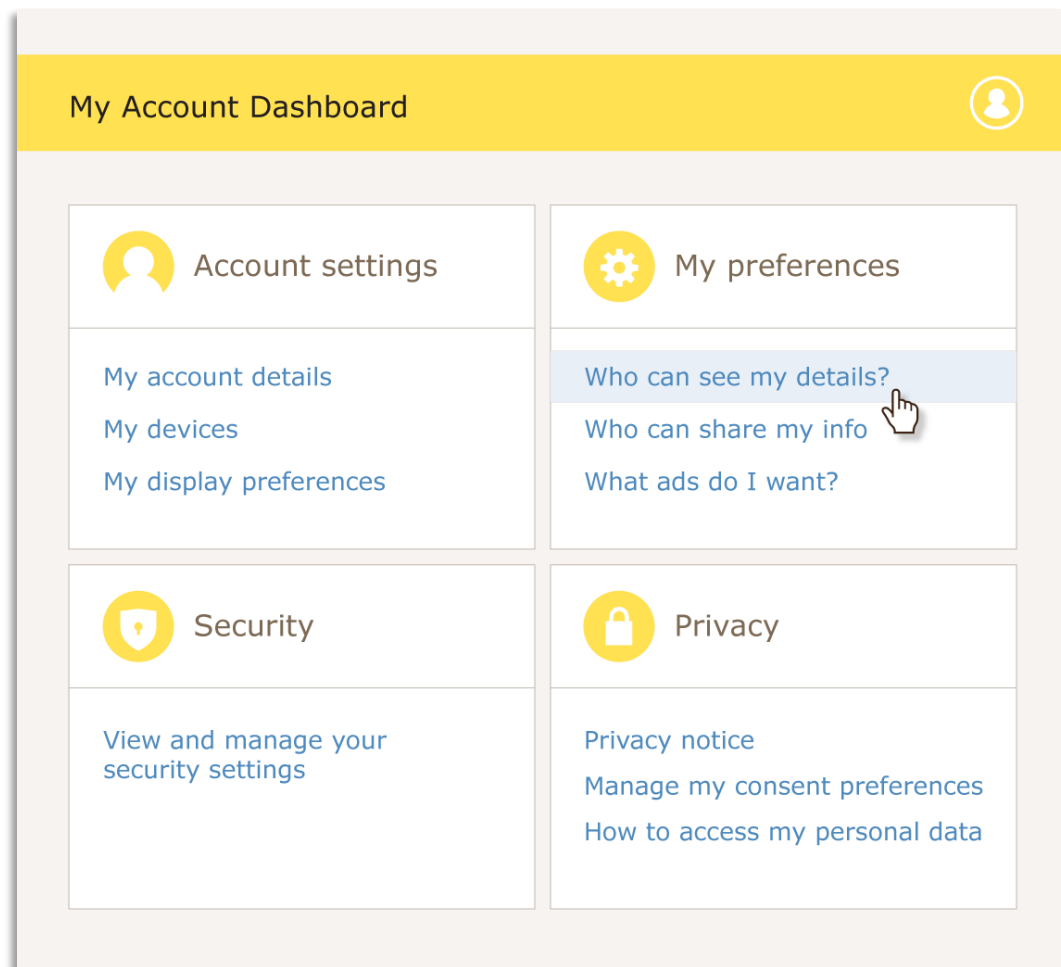
Confirm password

Create account

We use your email address as part of allowing you access to your account, and in order to contact you with important information about any changes to your account. [Please follow this link for further information.](#)

(圖片來源：ico.org.uk)

透明方式多元



(圖片來源：ico.org.uk)

兩部法律比較

台灣個資法

§7.1

第十五條第二款及第十九條第一項第五款所稱同意(註：蒐集、處理個人資料)，指當事人經蒐集者告知本法所定應告知事項後，**所為允許**之意思表示。

§7.2

第十六條第七款、第二十條第一項第六款所稱同意(註：目的外利用個人資料)，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，**單獨所為**之意思表示。

歐盟GDPR

§4(11) consent

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.

兩部法律比較

台灣個資法

§7.1

第十五條第二款及第十九條第一項第五款所稱同意(註：蒐集、處理個人資料)，指當事人經蒐集者告知本法所定應告知事項後，所為允許之意思表示。

§7.2

第十六條第七款、第二十條第一項第六款所稱同意(註：目的外利用個人資料)，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，單獨所為之意思表示。

歐盟GDPR

§6.1(a)

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes

兩部法律比較

台灣個資法

§7.4

蒐集者就本法所稱經當事人同意之事實，應負舉證責任。

歐盟GDPR

§7.1

Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

兩部法律比較

台灣個資法

§7.2

第十六條第七款、第二十條第一項第六款所稱同意(註：目的外利用個人資料)，指當事人經蒐集者明確告知特定目的外之其他利用目的、範圍及同意與否對其權益之影響後，**單獨**所為之意思表示。

歐盟GDPR

§7.2

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

兩部法律比較

台灣個資法

撤回同意(X)

歐盟GDPR

§7.3

The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

兩部法律比較

台灣個資法

自主性評估條件(X)

歐盟GDPR

§7.4

When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

兩部法律比較

台灣個資法

§7.3

公務機關或非公務機關明確告知當事人第八條第一項各款應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，**推定**當事人已依第十五條第二款、第十九條第一項第五款之規定表示同意。

歐盟GDPR

推定同意(X)

兩部法律比較

	台灣個資法	歐盟GDPR
自主性	未強調	○
特定性	○	○
知情性	○	○
非模糊性	未強調	○
證明同意	○	○
撤回同意	未規定	○
推定同意	○	X

歐盟GDPR下的有效同意

	歐盟GDPR
自主性	
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

自主性

	歐盟GDPR
自主性	① 真正自主的選擇/控制 ② 非自主情形： • 權力不對等(例如雇傭關係) • 綑綁其它條件，超過必要範圍 • 只能對所有不同目的統一表達同意 • 拒絕/撤回同意將受到不利益
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

歐盟GDPR

[示例1]

某相片編輯行動應用程式向使用者要求啟用衛星定位功能以使用其服務。此應用程式亦告知使用者將基於行為廣告之目的而利用所蒐集的資料。無論地理位置或線上行為廣告皆非相片編輯服務所必要，且逾越提供其核心服務之範圍。**鑒於使用者若不同意該目的即無法使用此應用程式，其同意即無法認定為自主給予。**

歐盟GDPR

[示例2]

某地方政府正在規劃道路養護工程。由於該道路工程可能長時間妨礙交通，該政府提供其市民以電子郵件訂閱工程進度及預期延工等資訊的機會。該政府清楚告知市民並無參與義務，並基於該（單一）目的徵求使用電子郵件地址之同意。**不同意的市民不會因此無法獲得該政府的核心服務或無法行使任何權利**，因此市民得自主地對該利用行為表示同意或拒絕。該道路工程的所有資訊亦皆可於政府網站上取得。

歐盟GDPR

[示例3]

某自然人擁有之土地需取得地方政府及該地方政府所在地之省政府的特定許可。兩公務機關為發布許可，需取得相同之資訊，但卻無法存取彼此的資料庫。因此，雙方皆要求提供相同之資訊，而該土地所有人即將資料寄送予兩公務機關。地方政府及省政府向該人徵求合併檔案的同意，以避免重複程序及通信聯繫等問題。兩公務機關均保證該同意具選擇性，**且若該人不同意合併資料，其許可程序仍將分別進行**。該土地所有人即可自主地向公務機關就合併檔案之目的給予同意。

自主性

歐盟GDPR

[示例4]

某公立學校徵求學生同意學校使用其照片以出版學生雜誌。只要學生不會遭拒絕提供教育或服務，並可拒絕學校使用照片而不會受到任何損害，則同意在此情形即具備真正的選擇性。

自主性

歐盟GDPR

[示例5]

某攝影團隊將拍攝辦公室的特定區域。由於受雇人可能出現於影片的背景中，雇主即向坐在該區域內的受雇人徵求被拍攝的同意。**不同意被拍攝者不會以任何方式受到處罰，而僅需在拍攝期間移至該建築內其他區域相同的辦公桌。**

自主性

歐盟GDPR

[示例6]

某銀行要求客戶同意允許第三方基於行銷之目的使用其付款資訊。此行為對於履行與客戶間的契約及提供一般性的銀行帳戶服務並非必要。若客戶不同意該目的，將導致遭拒絕提供銀行服務、關閉銀行帳戶，或依案例情形增加費用時，該同意即非自主給予。

自主性

歐盟GDPR

[示例7]

某零售商以同一請求，徵求消費者同意使用其個資於寄送行銷電子郵件，並與集團內其他公司分享消費者資訊。**由於無法針對這兩個目的個別表示同意，此同意即不具備區別性，因此不生效力。**

歐盟GDPR

[示例8]

下載某生活時尚app時，該app要求同意存取手機的加速度計。此非執行應用程式所必要，但有助於控管者更瞭解使用者的移動軌跡和活動程度。當使用者日後撤回該同意時，**發現該應用程式僅可在有限範圍內運行(撤回同意將遭受不利益)**，表示獲得的同意自始即屬無效。

自主性

歐盟GDPR

[示例9]

某當事人向時尚產品零售商訂閱一般折扣的產品新訊。該零售商徵求當事人同意蒐集更多購物偏好資料，以便根據其購物歷史或自願填寫的問卷而向其提供符合偏好的产品。當該當事人日後撤回同意時，將再收到非個人化的時尚產品折扣。**由於僅損失控管者提供的獎勵誘因，此將不構成損害。**

歐盟GDPR

[示例10]

某時尚雜誌提供其讀者在產品正式發表前即可購買化妝新品。

該產品隨後即將上市，但此雜誌的讀者可獨家預覽這些產品。為了享受這項優惠，必須提供郵寄地址，並同意列於該雜誌的訂閱者郵寄清單。

郵寄地址是為寄送所必要，而郵寄清單是用來每年寄送例如化妝品或短衫等產品的商業資訊。該公司解釋，郵寄清單上的資料將僅用於寄送產品以及該雜誌自己的紙本廣告，且不會與任何其他組織分享。

鑒於讀者最終仍可購買該產品，因此如讀者不願基於此原因揭露地址，將不致受到任何損害。

特定性

	歐盟GDPR
自主性	① 蒐集個資目的需具體、特定 ② 利用個資行為原則上只能在蒐集目的之範圍內
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

特定性

歐盟GDPR

[示例11]

某有線電視網基於訂戶同意而蒐集訂戶的個人資料，依訂戶的收視習慣針對新上架電影向訂戶提出個人化建議。一段時間後，**該電視網決定要讓第三方按訂戶的收視習慣寄送（或播送）精準廣告**。為了這個新目的，必須獲得新的同意。

知情性

	歐盟GDPR
自主性	① 當事人需先知情(必要資訊揭露)，才能有效同意 ② 揭露資訊方式：書面、言詞、影音 ③ 清楚、簡白語言，不可為冗長而難理解的隱私權政策或法律用語聲明 ④ 不可將必要資訊隱藏於其它條款中 ⑤ 可考量以階層方式揭露
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

知情性

[示例12]

X公司為控管者，收到「當事人不清楚該公司要求同意利用個資的目的」之申訴。該公司認為有需要查明當事人是否理解該公司在要求同意時提供的資訊。X依客戶分類組成自願受測小組，並在對外公布之前，將更新的同意資訊提供給這些受測人員。小組人員的挑選符合獨立性原則，並且基於確保產出結果的代表性及不帶偏見之標準。該小組收到問卷並寫下其對資訊的理解，以及對於資訊的可理解性與關聯性如何評分。控管者持續進行測試，直到小組表明該資訊已可理解。X將測試結果製成報告並保存作為未來的參考。此示例即展示X得以證明「當事人在同意X運用個資之前，已獲得清楚資訊」的可能方式。

知情性

[示例13] 不清楚、簡白

- 「我們可能會使用您的個人資料來開發新服務」（因就「服務」之定義或該資料將如何協助開發皆不明確）
- 「我們可能會將您的個人資料用於研究目的」（因就何種「研究」之定義不明確）
- 「我們可能會使用您的個人資料以提供個人化之服務」（因就何謂「個人化」之定義不明確）

知情性

[示例14] 夠清楚、簡白

- 「我們將保留您的購物歷史記錄並使用您之前購買產品的詳細資訊，以便為您提供我們認為您也會感興趣其他產品之建議」（此語句清楚表示將運用何種類型之資料、當事人將成為目標式產品廣告對象且其資料將用於達到此目的）
- 「為了瞭解用戶如何使用我們的網站，以便我們可以改善網站的直觀性，我們將保留和評估您最近造訪我們網站之資訊以及就您如何使用網站上不同部分之行為進行分析」（此語句清楚表示將運用何種類型之資料以及控管者將進行何種類型之分析）
- 「我們將會記錄您所點擊網站上之文章，依據您閱讀之文章並使用該資訊將網站上與您興趣相關之廣告提供予您」（此語句清楚表示個人化之需求為何，以及如何確認當事人之興趣）

知情性

[示例15]

每個經營網站的組織都應在其網站上公佈隱私聲明/通知。

隱私聲明/通知的直接連結應在該網站的每個頁面上以常用術語（例如「隱私」、「隱私政策」或「資料保護通知」）清楚表現之。

若因擺放位置或配色方式使內容或網址連結不明顯或難以及在網頁上搜尋，該隱私聲明/通知將不被認為係便於取得的。

知情性

[示例16]

下載app時應能從網路商店獲得必要之資訊。在安裝app後，仍需便於從該程式中取得相關資訊。

滿足此項要件方式之一係**確保搜尋資訊絕不可必須「點擊超過兩次」**

（例如透過在應用程式功能表中建立「隱私」/「資料保護」選項）。

此外，**所涉及之隱私資訊應針對特定應用程式**，而非僅為擁有或向公眾提供該應用程式公司之一般隱私政策。

知情性

[示例17] 隱私聲明呈現方式

- 階層式隱私政策呈現(網站/app)，但不應需要多次點擊
- 電話進線可先(語音/人工)告知第一階層，再email完整聲明或連結
- 彈跳通知 / 滑鼠游標懸停通知 / 隱私儀表板(dashboard)
- 影音、漫畫、資訊圖、流程圖
- 智慧型手機/物聯網裝置的語音警示
- 如無螢幕呈現文字(例如物聯網裝置)，應考慮例如紙本說明書、包裝上提供連結或QR code、setting時呈現內容等
- 全部資訊應放置同一位置或以同一文件完整呈現

非模糊性

	歐盟GDPR
自主性	① 當事人同意需積極、肯定、主動 ② 預先勾選同意框格是無效同意 ③ 單純沉默、不作為或繼續使用服務，不視為同意 ④ 特種個資的額外要求： • 明確聲明，簽名、填寫電子表格、寄送電子郵件、上傳簽名後掃描文件檔、電子簽章 • 考慮雙階驗證
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

非模糊性

歐盟GDPR

[示例18]

在安裝軟體時，應用程式要求當事人同意利用非匿名的當機報告以優化軟體。階層式隱私聲明提供包含同意之請求在內的必要資訊。

藉由**主動勾選「我同意」**的框格，使用者即可有效作出一個「清楚肯定的行為」以同意運用個資。

非模糊性

歐盟GDPR

[示例19]

只要已提供清楚的資訊，且該動作可清楚表明對特定請求的同意（例如將捲軸滑至左方，即表示同意基於Y目的而利用X資訊。重複該動作以確認），則**滑動螢幕上的捲軸、在智慧鏡頭前揮手、將智慧型手機順時鐘或八字形旋轉**，均是表示同意的選項。控管者必須證明以此方式獲得同意，且當事人可以同樣簡易方式撤回同意。

非模糊性

歐盟GDPR

[示例20]

下捲或滑過網站無法滿足清楚及肯定行動的要求。這是因為對於**繼續瀏覽即構成同意的警示**可能不易辨認，且/或在當事人快速瀏覽大量文字時恐遭忽略，進而使該行為有模糊空間。

非模糊性 / 明確性

歐盟GDPR

[示例21] 針對特種個資/自動化決策(包含profiling)的同意需「明確explicit」在螢幕上提供是、否勾選框格，只要文字清楚指出同意，例如「我在此同意對我的個人資料之運用行為」，而非例如「我清楚我的個人資料將被運用」，則資料控管者也可以此獲得網站訪客的明確同意。

非模糊性 / 明確性

歐盟GDPR

[示例22] 針對特種個資/自動化決策(包含profiling)的同意需「明確explicit」
某整形診所為向專家就病人的情況尋求第二意見而請求病人明確同意傳輸其醫療紀錄。該醫療紀錄為數位檔案。考量該資訊的特定性質，該診所要求當事人**提供電子簽章**以獲得有效的明確同意，並可證明已取得該明確同意。

證明同意

	歐盟GDPR
自主性	① 控管者有義務證明獲得當事人同意 ② 保存同意文件、線上行為紀錄等 ③ 建議：適時更新同意，確保當事人處於足夠的知情狀態
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

證明同意

歐盟GDPR

[示例23]

某醫院發起一個名為X計畫的科學研究計畫，需要實際的病人牙科紀錄。該計畫招募參與者的方式為致電病人，詢問是否同意自願加入候選名單，以便依此目的向其聯繫。控管者向當事人尋求明確同意使用牙科紀錄。此同意是經由電話中獲得，該醫院並錄下當事人確認同意為X計畫之目的使用其個資的口頭聲明。

撤回同意

	歐盟GDPR
自主性	① 當事人有權隨時撤回同意 ② 撤回同意方式應和給予同意方式相同 - 以點擊滑鼠、滑動螢幕或按鈕等方式獲得同意時，應以相同簡易方式撤回同意 - 透過該服務特定使用者介面(例如網站登入帳號、app、IoT裝置介面、電子郵件)獲得同意時，應以相同介面撤回同意 ③ 不可讓當事人因撤回同意而需受到其它不利益
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

撤回同意

歐盟GDPR

[示例24]

某音樂節透過線上票券代理商銷售門票。在每一次線上販售票券時，均針對基於行銷目的利用其聯絡方式，尋求(顧客)同意。

針對此目的，顧客可選擇不同意或同意，且控管者通知顧客有權撤回同意，如欲行使該權利，**可在營業日的早上8點到下午5點間致電客服中心**，不須給付任何費用。

相較於24小時均可透過線上票券販售商以一鍵點擊滑鼠方式給予同意，須在營業時間撥打電話才可撤回同意，對當事人將造成不利益。

推定同意(?)

	歐盟GDPR
自主性	無
特定性	
知情性	
非模糊性	
證明同意	
撤回同意	
推定同意	

結論

簡白性測試

活用戶善方式

不全有/全無

適時更新同意

歐盟GDPR作為優良實務

謹慎使用推定同意

告知可撤回同意

不同意不導致不利益

撤回同意不導致不利益

不抄他人範本

不網綁目的

有意義的語言

重複取得資訊

台灣個資法為底線

謝謝聆聽

THANKS FOR YOUR ATTENTION



王慕民律師

muming@davinci.idv.tw

10089 台北市中正區羅斯福路三段162號3樓

TEL: 02-2367-0902