



歐盟GDPR快易通

簡報人：廖淑君

職 稱：組長

財團法人資訊工業策進會

科技法律研究所

2018.07.24

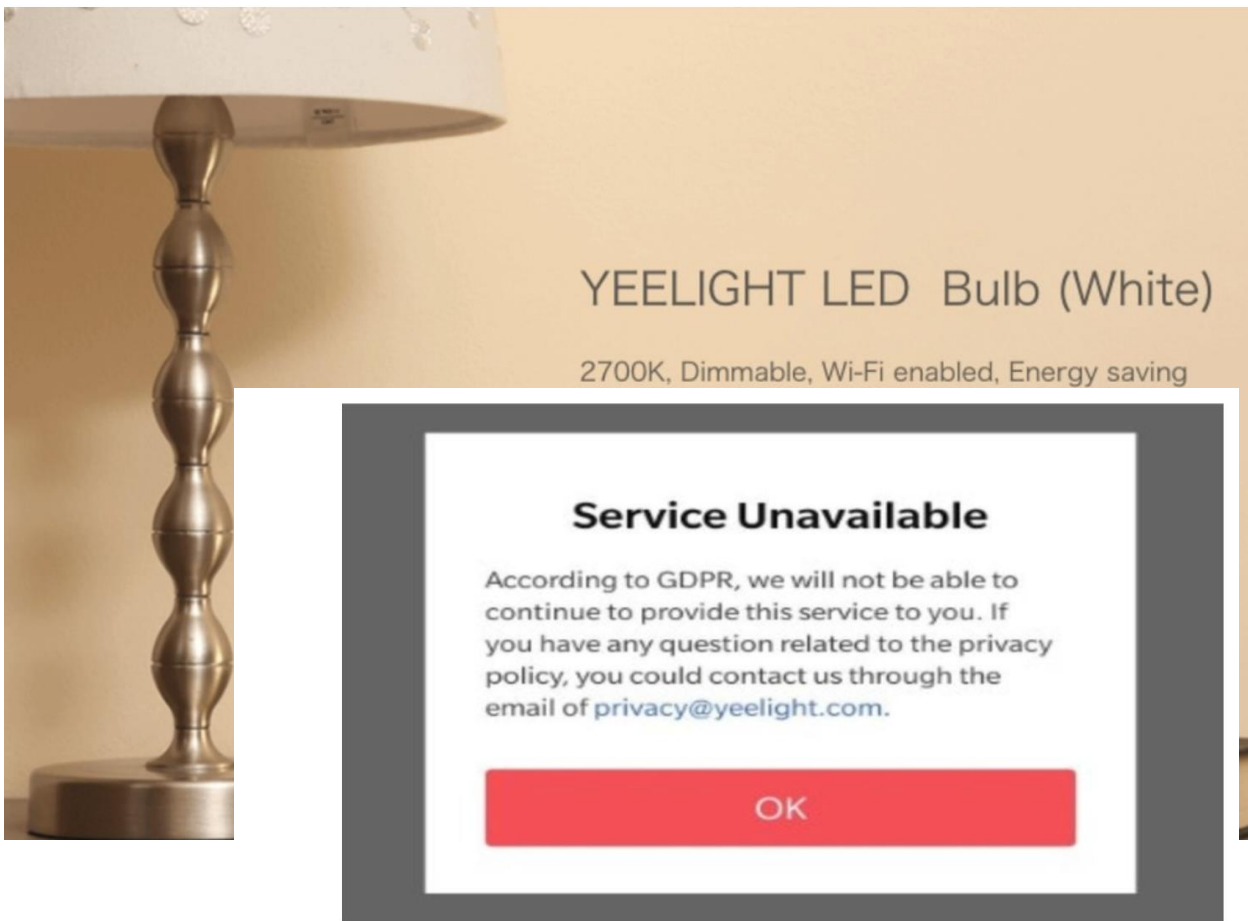


為什麼談GDPR?

小米智能燈 Yeelight 疑收集用戶數據！歐盟 GDPR 未能通過

| Kay | 28-05-2018 09:59 |

| Like 541



近日 Yeelight 已有不能通過歐盟最新 GDPR 通用數據保護條例的要求，需要停止 Yeelight 智能燈功能的通知。

資料來源：

<https://ezone.ulifestyle.com.hk/article/2081816/%E5%B0%8F%E7%B1%B3%E6%99%BA%E8%83%BD%E7%87%88%20Yeelight%20%E7%96%91%E6%94%B6%E9%9B%86%E7%94%A8%E6%88%B6%E6%95%B8%E6%93%9A%E7%BC%81%E6%AD%90%E7%9B%9F%20GDPR%20%E6%9C%AA%E8%83%BD%E9%80%9A%E9%81%8E>

保存開燈、關燈的紀錄？

據專門收集受 GDPR 通用數據保護條例影響的產品及服務網站 GDPR Hall of Shame 的文章所提，Yeelight 已有服務停止的告示，意味智能燈的大部分功能都不能使用。正因為 Yeelight 未能通過歐盟最新 GDPR 通用數據保護條例的要求，因此有網友 ruanyf 於微博發帖懷疑，Yeelight 是否有收集用戶數據，保存用戶開燈、關燈的紀錄。

CEO 表示不收集用戶私隱？

微博網友 ruanyf 有以上的懷疑，實屬正常，那麼 Yeelight 方面有何回應呢？品牌 CEO 姜兆寧就在微博回覆了這位網友：「我們不會保留用戶隱私數據，這個是道德問題，對於要長期經營的企業來說，這是重要的基本點，歐盟 GDPR 要求非常寬泛，所有非歐盟地區的 api 調用和數據訪問都被禁止，作為中國廠家，歐盟的服務器完全不和中國通信，需要大量的軟件開發和測試，為了避免可能產生的問題，暫時下線，歐盟合規後還會繼續上線。」如此一來，Yeelight 會致力配合 GDPR 的要求，務求能將智能燈重新上架。



為什麼談GDPR?

共享租借平臺StreetLend.com因GDPR而宣布停止服務

Streetlend.com創辦人認為，這個新的GDPR個資法傷害了小型以及新創公司，而且反而有助於鞏固像是Facebook、Google和Twitter的市場地位，他們擁有足夠的法律團隊以及資金為公司做準備以及辯護，而且現在又少了來自於新創公司的競爭。

文/ 李建興 | 2018-04-30 發表

讚 4.8 萬

按讚加入iThome粉絲團

讚 157

分享

G+

熱門書籤服務Instapaper因GDPR，突暫時停止服務歐洲用戶

Instapaper給用戶的E-mail中提到，從2018年5月24開始，歐洲居民將開始無法存取Instapaper。Pinterest產品工程經理Brian Donohue表示，他們正積極的解決這些問題，但他無法對外公開他們遭遇到的問題。

文/ 李建興 | 2018-05-25 發表

讚 4.8 萬

按讚加入iThome粉絲團

讚 25

分享

G+

無法跨過GDPR法遵難關，開源即時通訊軟體Monal停止歐洲地區服務

Monal創辦人Anurodh Pokharel表示，Monal的營運全由他自己一人完成，由於沒有多餘的資源處理Monal的GDPR法遵問題，為避免法律風險，Monal將停止歐洲的服務。

文/ 李建興 | 2018-05-18 發表

讚 4.8 萬

按讚加入iThome粉絲團

讚 17

分享

G+



為什麼談GDPR?

Vienna, 25 May 2018



GDPR: noyb.eu filed four complaints over "forced consent" against Google, Instagram, WhatsApp and Facebook

Corporations forced users to agree to new privacy policies.
A clear violation of the GDPR. Potential penalty: up to € 7 billion in total.

Privacy à la "take it or leave it"? The new General Data Protection Regulation (GDPR) which came into force today at midnight is supposed to give users a free choice, whether they want to share their data usage or not. The opposite feeling spread on the screens of many users: Tons of "consent boxes" popped up online or in applications, often combined with a threat that the service will no longer be used if user do not consent. One the first day of GDPR noyb.eu has filed four complaints against Google (Android), Facebook, WhatsApp and Instagram over "forced consent". Max Schrems chair of noyb.eu: "Facebook has even blocked accounts of users who have not given their consent. In the end users only had the choice to delete the account or hit the "agree"-button. This is not a free choice, it more reminds of a North Korean election process."

Overview over complaints Very similar complaints were filed with four authorities, to ensure European coordination. In addition to the four authorities at the residence of the users, the Irish Data Protection Commissioner ([link](#)) will probably get involved in the cases too, as the headquarter of the relevant companies is in Ireland in three cases.

Company / Service	Authority	Headquarter	Maximum possible penalty (4%)	Complaint (Original)
Google (Android)	CNIL (France)	USA	€ 3,7 Mrd	Link
Instagram (Facebook)	DPA (Belgium)	Ireland	€ 1,3 Mrd	Link
WhatsApp	HmbBfDI (Hamburg)	Ireland	€ 1,3 Mrd	Link
Facebook	DSB (Austria)	Ireland	€ 1,3 Mrd	Link

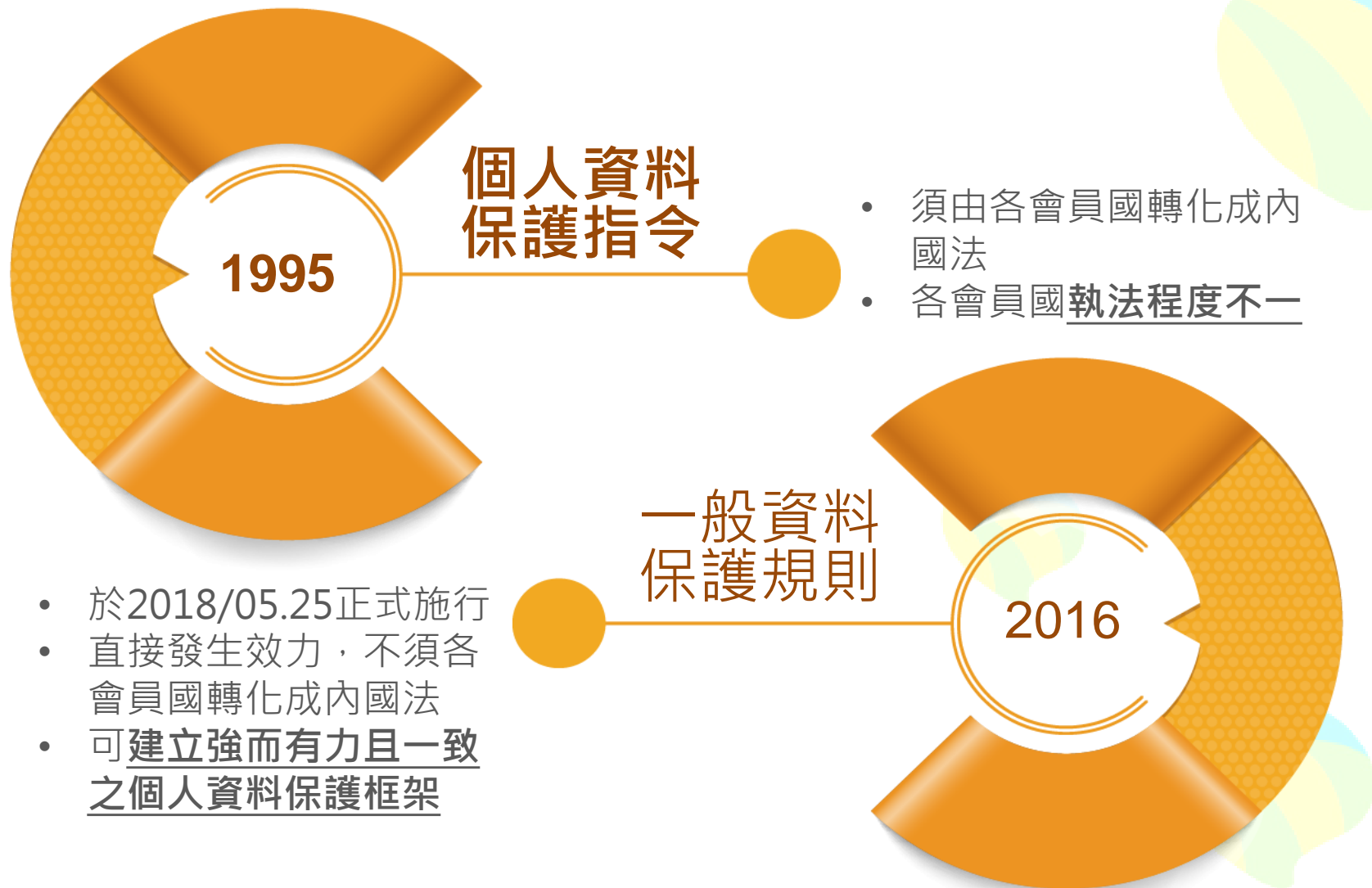
資料來源：https://noyb.eu/wp-content/uploads/2018/05/pa_forcedconsent_en.pdf





什麼是GDPR?

GDPR是歐盟於2016年4月27日通過，2018年5月25日正式施行之一般資料保護規則(general data protection regulation)，性質相當於我國之個人資料保護法。





什麼是GDPR?

GDPR施行前

主要規定：

1995個人資料保護指令

保護客體：

個人資料指可以用來識別一個人的資訊

適用主體：

於歐盟境內設立之資料控制者與資料處理者

資料控制者與處理者義務

個人資料蒐集處理利用原則；個人資料安全性維護；資料外洩通報與通知義務；國際傳輸限制

資料主體權利保護

- 個人資料蒐集前之告知
- 資料主體得查詢、請求更正、刪除、拒絕行銷...等。

GDPR施行後

主要規定：

一般資料保護規則

強化保護客體認定範圍：

IP位址、Cookies、RFID標籤號碼等網路識別碼將可能被認定為個人資料

擴大適用主體範圍：

未在歐盟境內之資料控制者與資料處理者，但對歐盟境內之居民提供商品或服務或監控歐盟居民在歐盟境內之行為，而有蒐集處理與利用個人資料者，必須適用GDPR。

加重資料控制者與資料處理者義務：

強化個人資料蒐集處理利用之同意規定；新增聯絡代表、個人資料保護官之設置與資料保護隱私評估要求

強化資料主體權利保護

新增被遺忘權、資料可攜權等規定



-
- The diagram illustrates the flow of personal data within the EU and to a provider outside the EU. A large blue oval labeled "歐盟境內" (Within the EU) contains two main components: "設立於歐盟境內者" (Established within the EU) and "資料主體" (Data Subject). The "設立於歐盟境內者" is represented by a yellow figure standing next to a printer and scattered papers. The "資料主體" is represented by two white figures. Arrows labeled "個人資料" (Personal Data) show the flow of data from the "資料主體" to the "設立於歐盟境內者" and from the "設立於歐盟境內者" to the "資料主體". Outside the oval, a white figure is seated at a desk with a computer, representing the "供應商" (Provider). An arrow labeled "個人資料" (Personal Data) shows the flow of data from the "資料主體" to the "供應商". A list of conditions for data transfer is provided:
- 對歐盟境內之資料主體提供商品或服務(不論有無付款)
 - 追蹤或監控資料主體在歐盟境內之行為





如何判斷是否須適用GDPR?

個人資料：任何與可識別或可能被識別之自然人有關的資訊；可能被識別之自然人指其可以直接或間接透過識別碼(identifier)被識別出來。





Plan

Do

如何符合GDPR?

Act

Check

- GDPR**
- 第1章 通則(\$1~ \$4)
 - 第2章 原則(\$5~\$11)
 - 第3章 資料主體之權利(\$12~\$23)
 - 第4章 資料控制者與處理者(\$24~\$43)
 - 第5章 傳輸個人資料至第三國或是國際組織(\$44~\$50)
 - 第6章 獨立主管機關(\$51~\$59)
 - 第7章 合作與一致性(\$60~\$76)
 - 第8章 賠償、責任與罰責(\$77~\$84)
 - 第9章 有關於特別蒐集、處理與利用個人資料之規定(\$85~\$99)

1. 就所持有之歐盟居民個人資料進行清查
 - ☐會員國當地法令之遵循
 - ☐於個人資料本人所屬國當地指定代表(representative)?
 - ☐設置個人資料保護官(data protection officer)?
2. 就所持有之歐盟居民個人資料進行風險識別與評估
 - 個人資料保護政策與相關程序
 - ☐蒐集、處理與利用個人資料程序
 - ☐資料主體行使其權利之程序
 - ☐個人資料委託他人蒐集處理利用之程序
 - ☐個人資料保護衝擊評估之程序
3. 資料安全保護措施
 - ☐採取技術性與組織性之措施，確保個人資料之安全
 - ☐個人資料侵害事故之通報與應變機制
4. 國際傳輸(將個人資料自歐盟境內傳輸至第三國或國際組織)之檢核程序與安全機制
5. 個人資料蒐集處理與利用活動之記錄(書面，包括電子形式)
6. 定期測試、評估和衡量所採科技與組織性措施的有效性



個人資料清查

參考GDPR相關規定，建議至少可以清查下列項目：

1. 個人資料之種類，如：一般個人資料、特種個人資料、犯罪資料
→可以合法蒐集、處理與利用之依據不同
2. 資料主體之種類，如：員工、兒童(16歲以下)
→員工之特種個資蒐集得為履行勞動法令所定之義務(GDPR§9)
→於資訊社會服務，兒童個人資料之取得須有其法定代理人之同意(GDPR§8)
3. 個人資料蒐集之目的與合法性依據
→判斷是否符合GDPR§5合法、公平、透明原則
4. 個人資料保存期間及決定保存期間之原則
→判斷是否符合GDPR§5保存期限原則、踐行GDPR§13&§14 向資料主體告知之義務
5. 個人資料之數量、蒐集頻率與型態(如：是否有監控或追蹤行為)
→配合項目1之清查，判斷是否有需要設置DPO、代表、進行資料保護衝擊評估等
6. 資料傳輸之對象類型(資料控制者/聯合資料控制者/資料處理者/其他)
→有關資料控制者間之責任(GDPR§26)、對資料處理者之管理(GDPR§28)...
7. 是否有將個人資料傳輸至歐盟境外
→有關GDPR將個人資料傳輸至歐盟以外之第三國或國際組織規定之符合



代表(representative)



1. 未於歐盟境內有設點者，應以書面指定在歐盟境內的代表
2. 代表設於資料主體所在之國家
3. 代表受資料控制者或處理者之委託在歐盟境內與個人資料本人或主管機關對話
4. 不因代表之指定，而免除資料控制者或處理者之責任→個人資料本人仍得對資料控制者或處理者提起訴訟



1. 個人資料之蒐集、處理與利用是偶發性的，且未涉及大規模的特種個人資料或犯罪資料，同時，不太可能對個人資料本人之權利造成任何風險
2. 公務機關

特種個人資料：與個人人種、種族、政治意見、宗教或哲學信仰、工會資格、基因、生物資訊、健康資訊、性生活有關之資訊


依GDPR規定，有揭露代表資訊之要求，如：

- 依GDPR第13條、第14條，踐行告知義務時，向個人資料本人告知代表之資訊
- 依GDPR第30條規定，有關個人資料蒐集、處理與利用活動之記錄，其記錄項目包括代表之姓名/名稱及其聯絡資訊




個人資料保護官(data protection officer)

什麼情況須設置DPO?

- 
1. 公務機關
 2. 大規模地、經常且系統化地追蹤或監控資料主體
 3. 大規模蒐集、處理與利用特種個人資料或犯罪資料
 4. 會員國法令規定須設置者


需要為集團內的每家企業設置DPO嗎?

- 
1. 一個集團可以指定一位DPO，但前提是集團內的企業都可以很容易地聯絡到那位DPO
 2. 資料主體必須可以和DPO聯絡，以獲取相關資訊並行使GDPR所定權利
 3. 須確保DPO可以即時地與適當地涉入與個資保護有關之議題

DPO一定是要公司的員工嗎?並專責嗎?

- 
1. 可以是公司員工，也可以是以簽定服務契約的方式來找尋DPO，但必須公開該服務契約之細節且須與主管機關提送該契約
 2. DPO可以兼任其他工作，但是必須確保其所兼任之工作和職責不

DPO 須具備什麼資格?




具有專業能力，尤其是個資保護法知識，並有足夠能去實施GDPR第39條

可以干涉DPO之職責嗎?

- 
1. 確保DPO不會收到任何與
 2. 不會因為職責之執行而受
 3. 直接向最高管理階層報告

DPO職責

- 
1. 就GDPR之遵循提供建議
 2. 監督組織是否有落實GDPR
 3. 針對資料保護衝擊評估提供建議並監督其落實
 4. 與主管機關合作
 5. 就資料保護衝擊評估及其他議題，作為與主管機關聯絡之窗口



資料主體之權利

資料主體得行使之權利(GDPR§12、§15- § 22)

- 查詢個人資料
- 更正個人資料
- 刪除個人資料(被遺忘權)
- 限制個人資料之蒐集、處理與利用



通知義務(通知資料提供揭露或提供之對象)

- 個人資料可攜
- 拒絕/反對個人資料之蒐集、處理與利用
- 不受限於與個人有關之自動決策，含側寫的結果



個人資料蒐集、處理與利用之原則(1/2)

問責性

資料
最小化

目的
限制

合法、
公平、
透明。

- GDPR§6 合法蒐集處理利用個人資料，如：取得當事人同意
- GDPR§7 同意的要件，如：資料蒐集者負舉証責任、請求同意之內容須與他意思表示有區別，且以白話易讀方式為之，否則無效
- GDPR§9 特種個人資料之蒐集、處理與利用，如：資料主體明示同意
- GDPR§13&§14 向資料主體進行告知

- 於合於目的範圍內，適當、相關且有限度地蒐集、處理與利用個人資料

- 於資料蒐集時，有特定、清楚與正當之目的
- GDPR§13&§14 向資料主體進行告知時，應告知蒐集資料之目的
- 合於蒐集目的之處理與利用個人資料
- GDPR§25採取適當的科技與組織性措施，確保個人資料僅在合於特定目的之必要範圍內被蒐集、處理與利用



個人資料蒐集、處理與利用之原則(2/2)

問責性

完整性
機密性

保存
期限

正確性

- 維持個人資料之正確性與最新性
- GDPR§16 資料主體得要求資料控制者更正其個人資料

- 不保存不要必要之資料
- GDPR§13&§14 向資料主體進行告知時，應告知資料保存期間，如可行，併同告知決定資料保存期間之原則

- GDPR§32 採取科技性與組織性措施，以防止個人資料毀損、滅失、不當揭露予第三人、未經授權存取等

Privacy by design

於個人資料蒐集、處理與利用之過程中，採取適當的科技與組織性措施(整合至流程中)，以確保個人資料之蒐集、處理與利用係符合歐盟GDPR，並達對個人資料本人權益保護之目的



個人資料保護衝擊評估

什麼情況須進行個人資料保護衝擊評估?

1. 當預定的個人資料蒐集處理利用可能會對資料主體造成高風險，特別是下列情況
 - ① 自動化決策(包括側寫)且其會對資料主體產生法律上之影響或其他類似重要的影響
 - ② 大規模地蒐集處理利用特種個人資料或犯罪資料
 - ③ 系統化且大規模地在公開可以存取的領域追蹤或監控行為
2. 主管機關公告者

何時要進行評估?每一個流程都要嗎?

1. 在開始蒐集處理與利用個人資料之前
2. 相似的流程且其顯示相類似的風險時，可不用每流程都評估

評估的內容是什麼?

1. 系統性地描述蒐集、處理與利用個人資料之流程及其目的，如有適用，併同說明資料控制者之正當利益為何
2. 蒐集、處理與利用個人資料之必要性及其與目的間之比例性
3. 蒐集、處理與利用個人資料之流程對資料主體權利之風險
4. 針對風險所採取之措施，包括安全措施與確保個人資料之蒐集、處理與利用符合GDPR之措施

是否應諮詢DPO或主管機關?

1. 個人資料保護衝擊評估須諮詢DPO
2. 當缺乏保護措施會對資料主體產生高風險時，應諮詢主管機關之意見



國際傳輸(將個人資料自歐盟境內傳輸至第三國或國際組織)

適當保護 + 資料主體權利及具救濟管道

適當保護，例如：經主管機關認可之約束企業條款、經歐盟執委會接受之標準個人資料保護條款

01

歐盟適足性決定

- GDPR§45
- 不需再取得任何特定許可 (authorization)

02

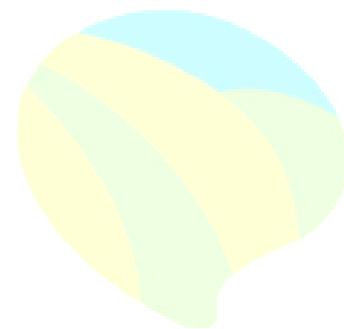
其他特殊情形

例如：資料主體被明確告知其個人資料將被傳輸至個人資料未有適當保護之地區及其可能造成之風險後，明白地表示同意此等傳輸行為

03



Q&A



1. 本簡報之內容不構成任何實質法律意見。
2. 如果您於因應歐盟GDPR有需要協助之地方，您可以與單一窗口聯絡，將會提供您必要的諮詢與資安顧問服務團轉介服務。

聯絡人：陳靜怡小姐

電子郵件：jeaniechen@iia.org.tw

聯絡電話：02-66311018

