

達文西

達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

從損害風險驅動個資法遵查檢 與管理制度建置

達文西個資暨高科技法律事務所

王慕民 律師

2019 年 8 月 14 日

一

重點回顧

二

實務趨勢

三

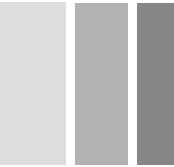
從損害風險驅動個資法遵查檢

四

從損害風險驅動個資管理制度建置

五

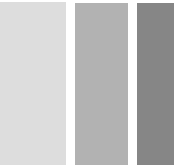
在管理制度之後



重點回顧

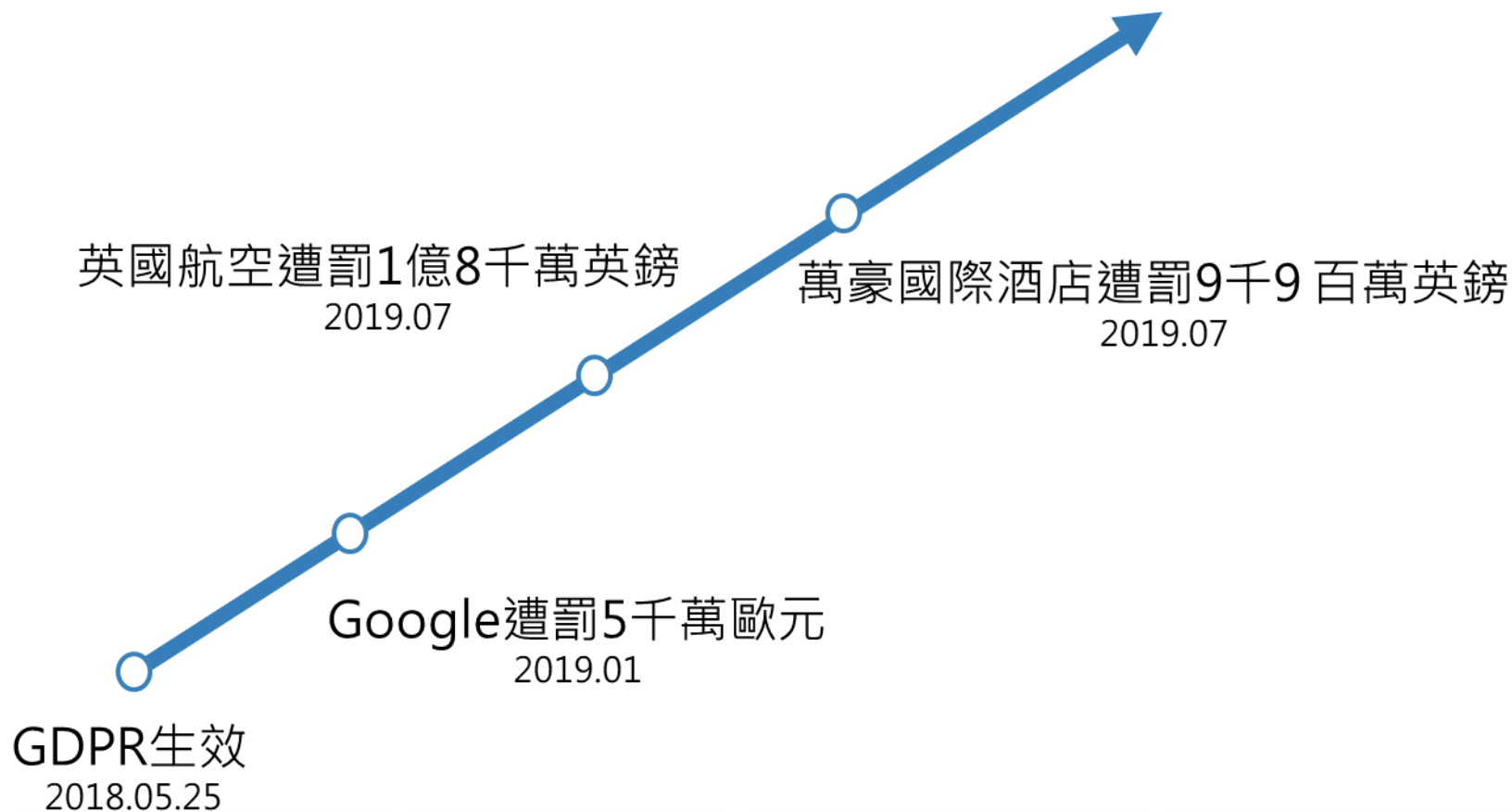
個人資料保護法要項





實務趨勢

來勢洶洶的歐盟





Home » News & Events » Press Releases » FTC

FTC Imposes \$5 Billion Privacy Restrictions on

FTC settlement imposes historic accountability and transparency

FOR RELEASE

July 24, 2019

Highest Penalties in Privacy Enforcement Actions

\$148 M

States
v.
Uber

\$230 M

British Authority
v.
British Airways
(proposed)

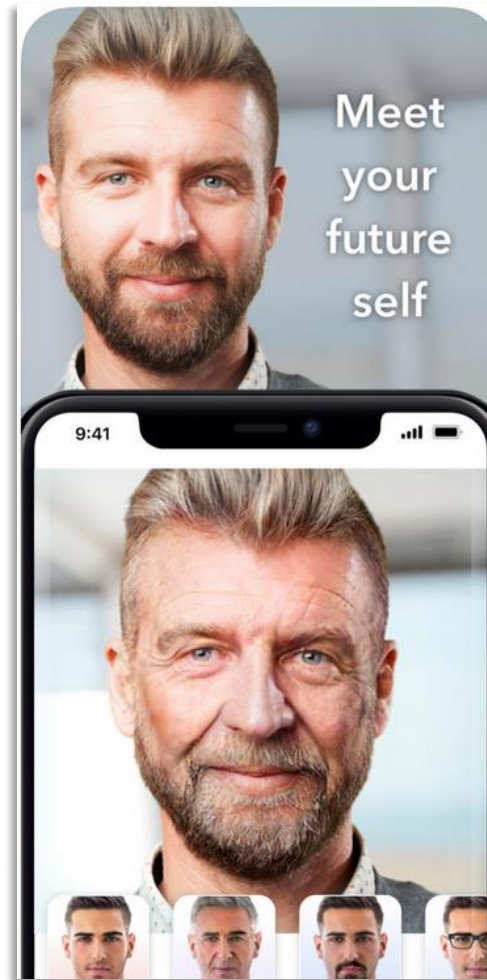
\$275 M

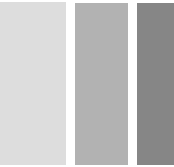
CFPB and States
v.
Equifax

\$5,000,000,000
FTC v. Facebook

Source: Federal Trade Commission | FTC.gov

放大檢視的個資保護/隱私爭議





從損害風險驅動個資法遵查檢

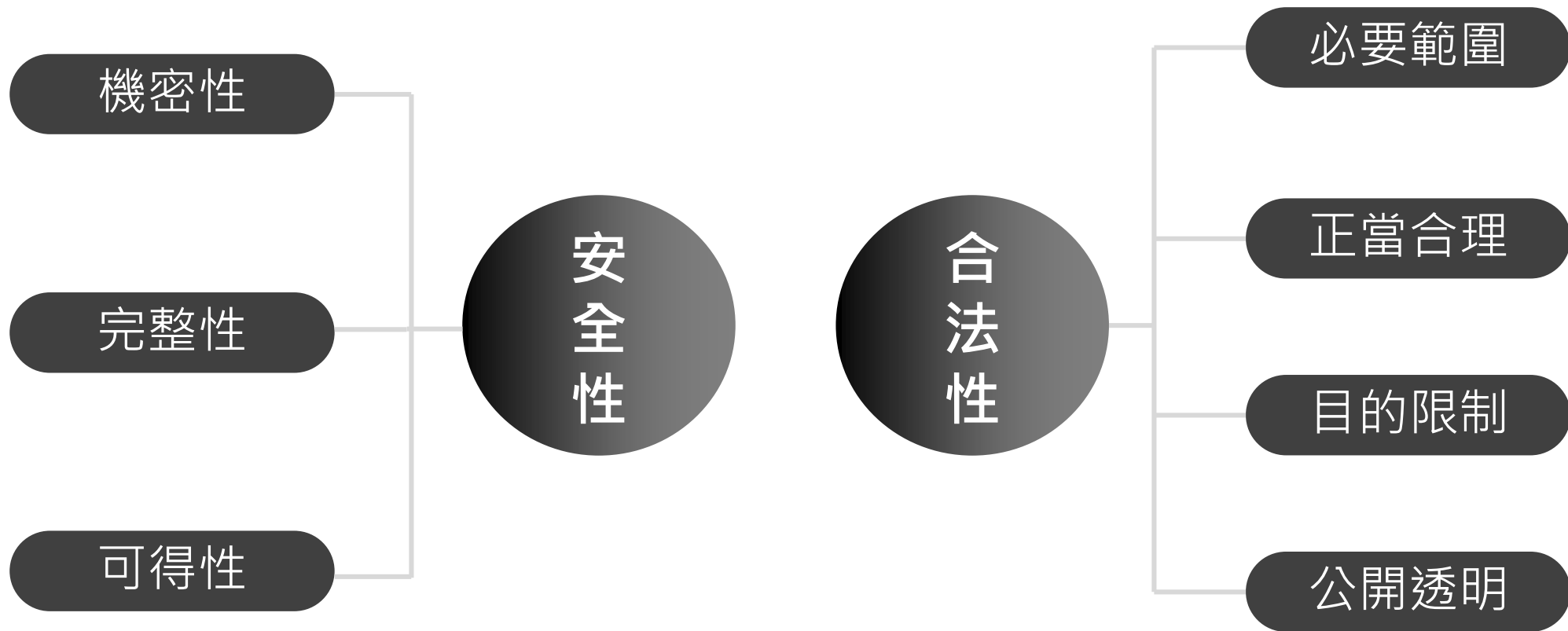
個資法遵查檢的最大秘密——

~在有限的時間中查檢最關鍵的項目~

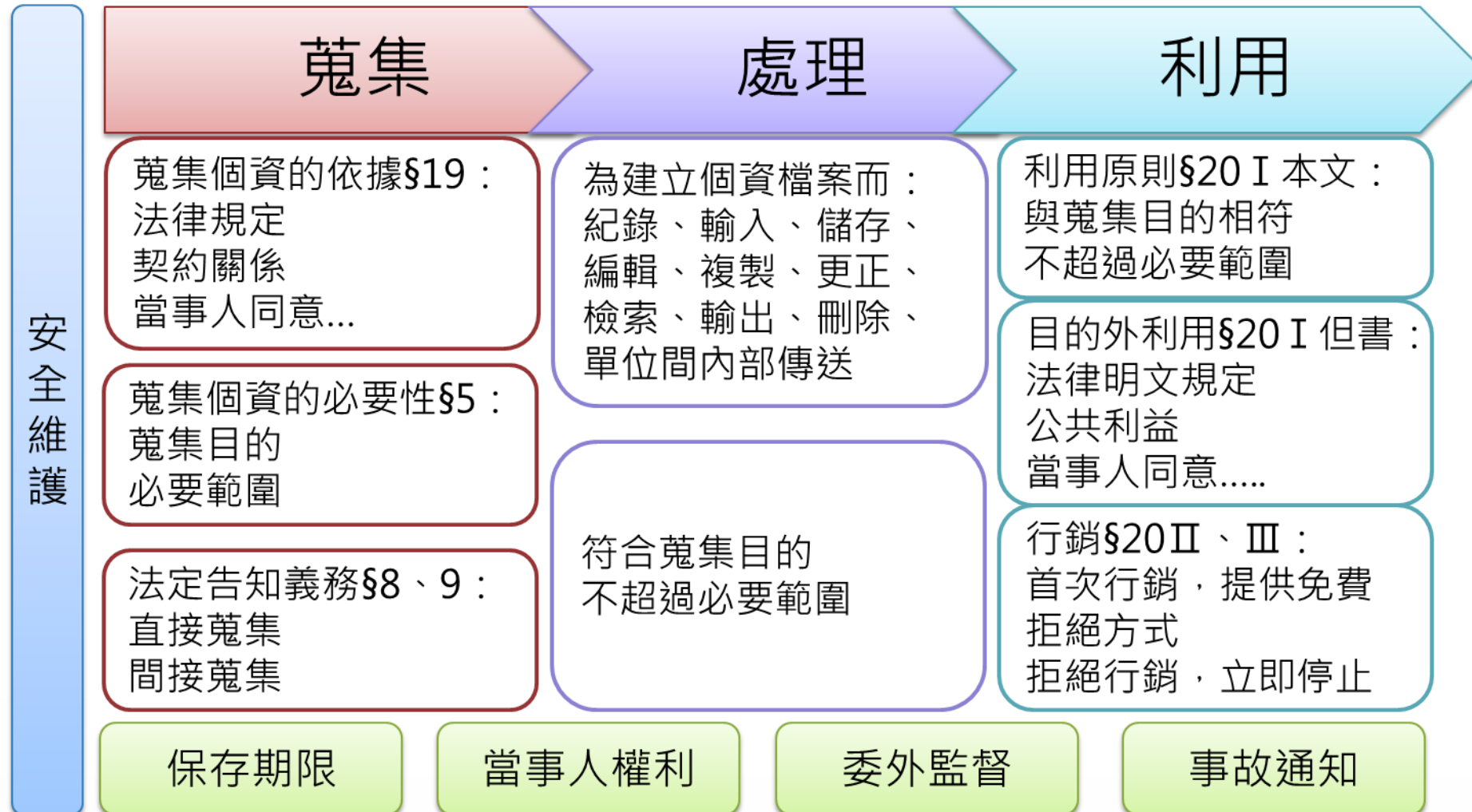
不關鍵項目實例

- 個資盤點表未定期更新
- 個資檔案風險評鑑等級有誤
- 同仁/廠商人員未簽署保密切結書/同意書
-
- (缺失不直接導致違法或侵害當事人權利)

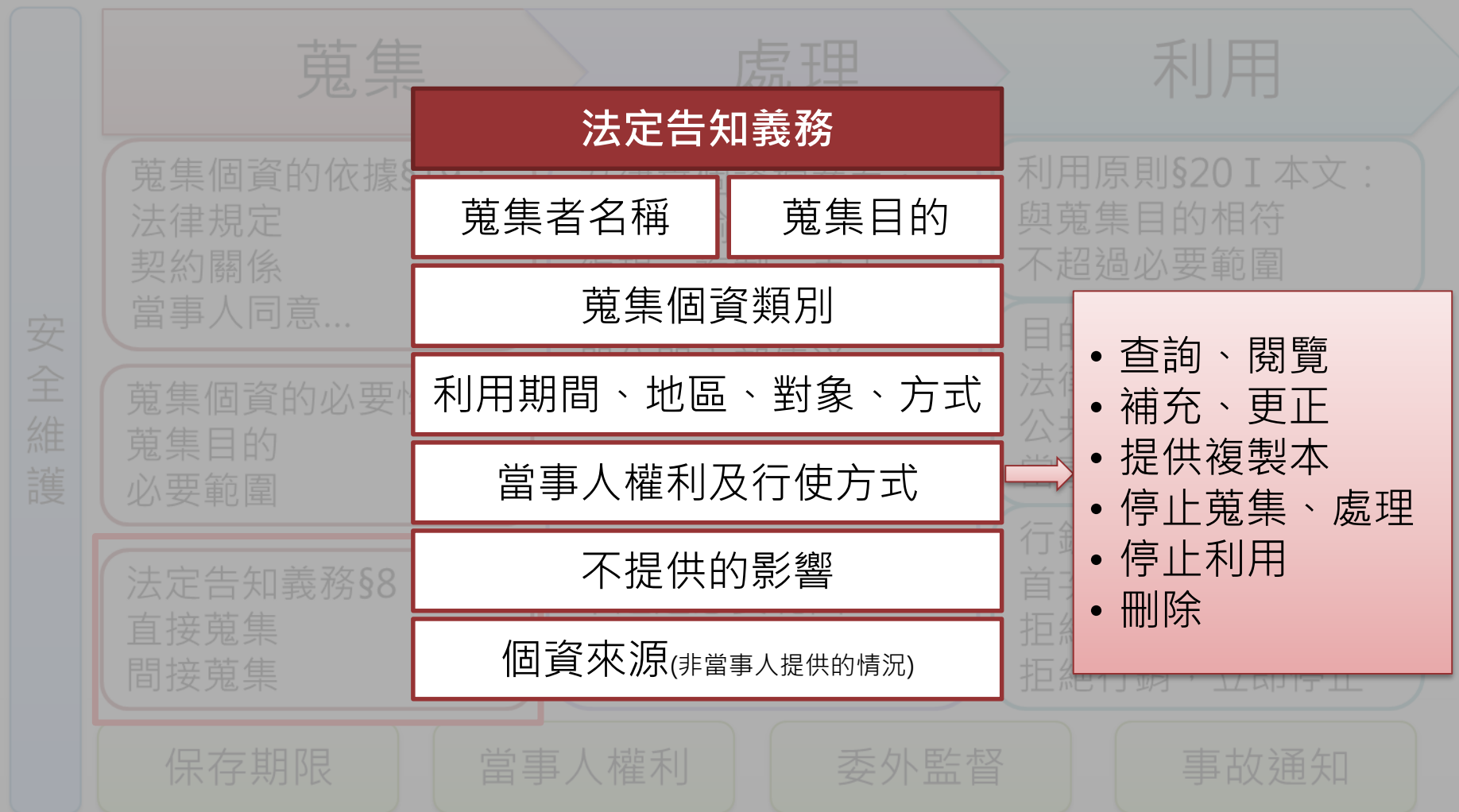
損害風險是個資法遵查檢的關鍵



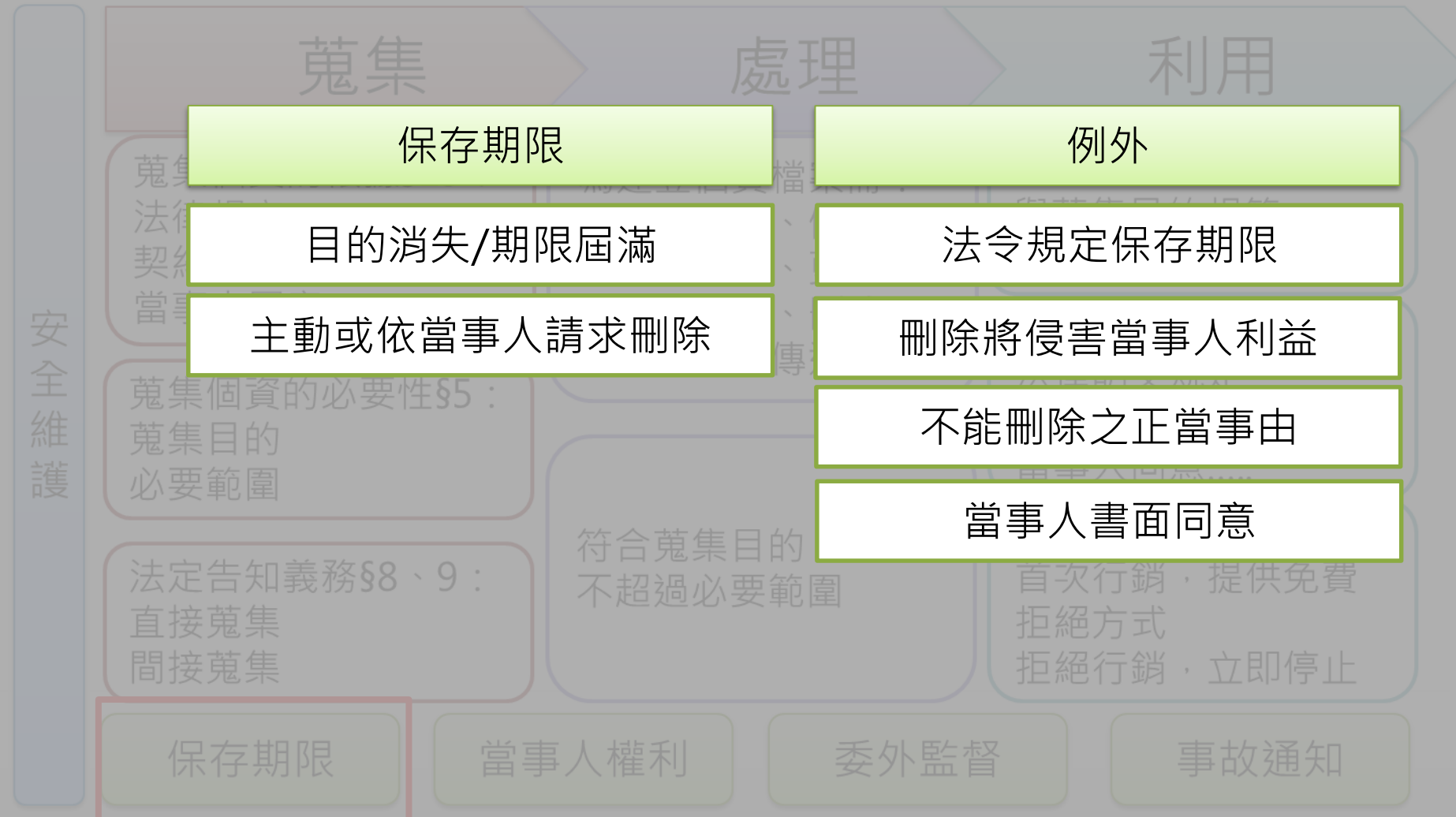
對應個人資料保護法設計查檢項目



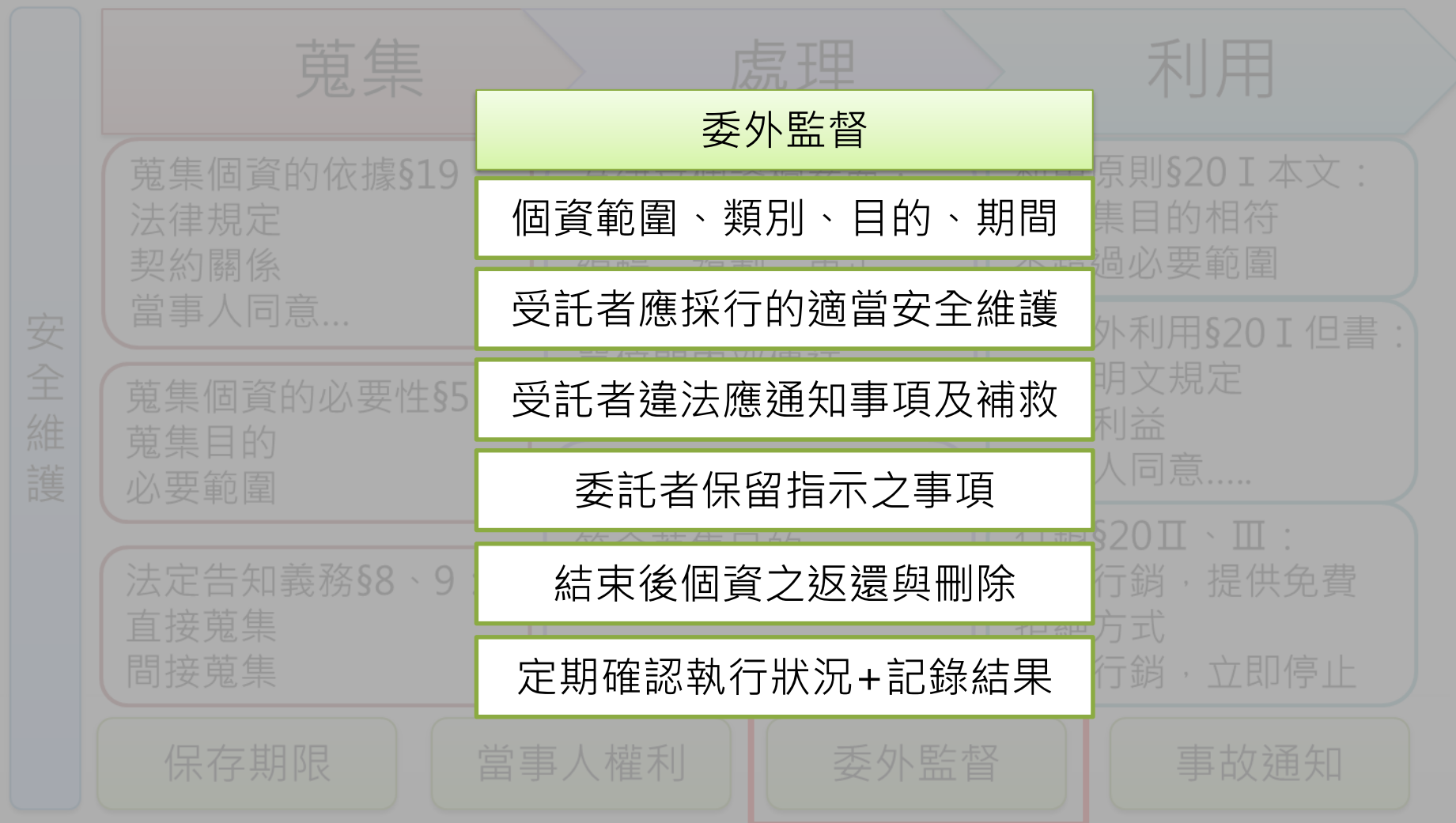
對應個人資料保護法設計查檢項目



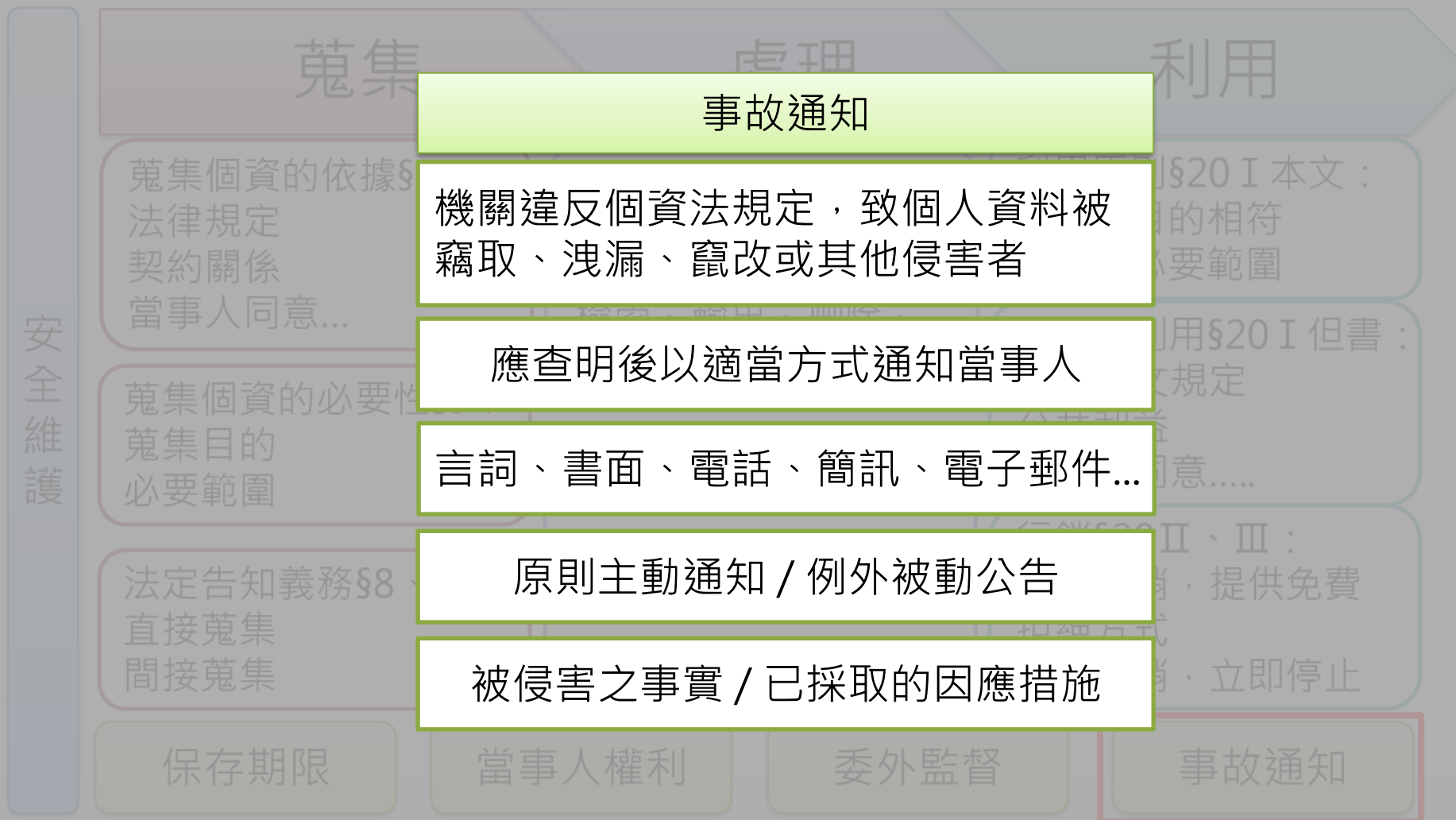
對應個人資料保護法設計查檢項目



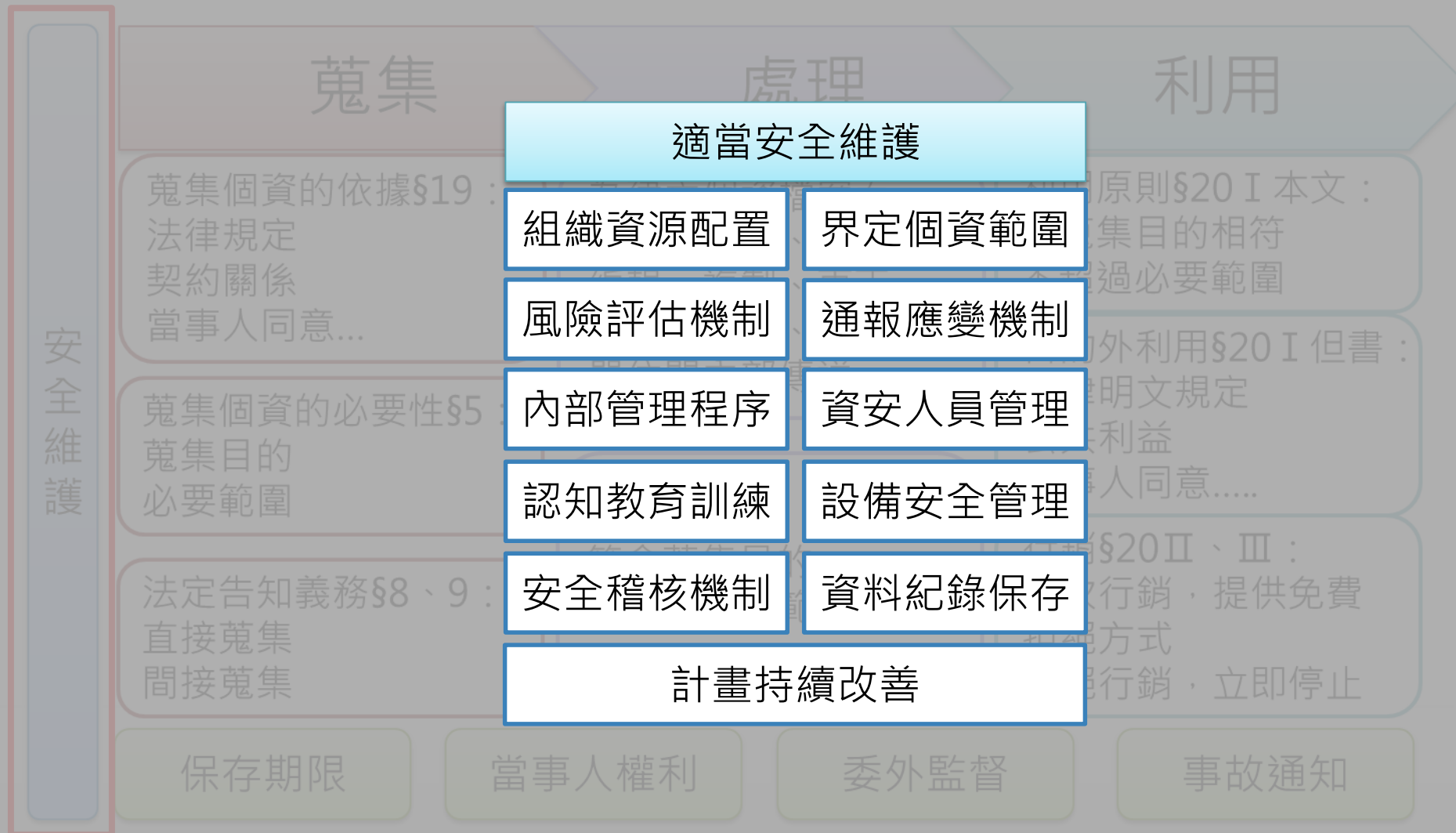
對應個人資料保護法設計查檢項目



對應個人資料保護法設計查檢項目



對應個人資料保護法設計查檢項目



建議—從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買商品明細，將抽獎單交給櫃台人員。
- ② 當晚結束營業後，門市人員將抽獎單交給行銷部抽獎，並由行銷部人員致電中獎者確認身分、告知中獎。
- ③ 隔天行銷人員將獎品及中獎人姓名、電話、地址交給物流廠商寄送。
- ④ 行銷部將抽獎單上資料鍵入客戶管理系統，為消費者建立會員身分，發送行銷資訊，並由數據部門將資料納入分析。

建議—從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買商品明細，將抽獎單交給櫃台人員。
- ② 當晚結束營業後，門市人員將抽獎單交給行銷部抽獎，並由行銷部人員致電中獎者確認身分、告知中獎。
- ③ 隔天行銷人員將獎品及中獎人姓名、電話、地址寄出。
- ④ 行銷部將抽獎單上資料鍵入客戶管理系統，並由數據部門將資料納入分析。

蒐集行為一

- 目的是什麼？
- 法律依據是什麼？
- 有沒有超過必要範圍？
- 會不會增加無謂風險？
- 法定資訊告知？

建議—從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買商品明細，將抽獎單交給櫃台人員。
- ② 當晚結束營業後，門市人員將抽獎單交給行銷部抽獎，並由行銷部人員致電中獎者確認身分、告知中獎。
- ③ 隔天行銷人員將獎品及中獎人姓名、電話、地址交給物流廠商寄送。
- ④ 行銷部將抽獎單資訊，並由數據部處理行為一
• 符合蒐集目的嗎？
• 符合法律依據嗎？
利用行為一
• 符合蒐集目的嗎？
• 有沒有超過必要範圍？

建議—從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買商品明細，將抽獎單交給櫃台人員。
- ② 當晚結束營業後，門市人員將抽獎單交給行銷部抽獎，並由行銷部人員致電中獎者確認身分、告知中獎。
- ③ 隔天行銷人員將獎品及中獎人姓名、電話、地址交給物流廠商寄送。
- ④ 行銷部將抽獎單上資料鍵入客戶管理系統，為消費者建立會員身分，發送行銷資訊，並由數據部門將資料納入分析。

委外行為—

- 事前約定範圍？
- 事後執行監督？

建議—從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買產品明細，將抽獎單交給櫃台人員。
- ② 當晚，消費者確認抽獎單交給行銷部。處理行為—
 - 符合蒐集目的嗎？
 - 符合法律依據嗎？利用行為—
 - 符合蒐集目的嗎？
 - 有沒有例外事由？
- ③ 隔天行銷人員將獎品寄給消費者。姓名、電話、地址交給物流公司寄送。
- ④ 行銷部將抽獎單上資料鍵入客戶管理系統，為消費者建立會員身分，發送行銷資訊，並由數據部門將資料納入分析。

- 利用行為—
- 符合蒐集目的嗎？
 - 有沒有例外事由？

建議一從個資流程著手

- ① 消費者在門市櫃台領取抽獎單，填妥姓名、電話、電子郵件信箱、身分證號、戶籍地址、收件地址、購買商品明細，將抽獎單交給櫃台人員。
- ② 當晚結束營業後，由行銷部人員將抽獎單交給行銷部人員，並由行銷部人員致電中獎者確認身分、告知中獎資訊。
- ③ 隔天行銷人員將抽獎單交給廠商寄送。
- ④ 行銷部將抽獎單上資料鍵入客戶管理系統，為消費者建立會員身分，發送行銷資訊，並由數據部門將資料納入分析。

整體安全維護

個資法遵查核簡易步驟

第一步：詢問蒐集個資業務

第二步：詢問個資來源與蒐集個資管道、方式

第三步：詢問蒐集個資目的

第四步：請求提供蒐集個資表單

第五步：檢視個資欄位與蒐集目的之必要性，並確認法律依據

第六步：檢視個資告知聲明 / 當事人同意（出示證明）

第七步：詢問處理個資情形

第八步：詢問利用個資方式、地區、期間及提供個資之對象

第九步：詢問個資保存方式與保存期間

第十步：詢問有無業務委外

其 他：依個資管理制度相關辦法執行稽核

從損害風險驅動個資管理制度建置

管理制度的真正(?)功能

【裁判字號】104,北小,376

【裁判日期】1040707

【裁判案由】損害賠償

【裁判全文】

臺灣臺北地方法院小額民事判決

104年度北小字第376號

(三)次查，被告為維護系爭網站個人資料之安全，業依個人資料保護法第27條第1項規定採取各項安全措施，包含訂定資訊作業安全管理辦法、於資料保存系統中設置加密措施、定期審查程式碼及防火牆等防護設備之安全性、實施員工資訊安全教育訓練、禁止員工自行安裝軟體於被告公司所配發之相關電腦設備等。被告並設有「個人資料保護處理小組」及「資訊安全事故處理小組」，負責個資保護事項之檢討及監督

名賣家聯繫，已如前述。綜此，被告既已確實對系爭網站進行例行性弱點掃描，平時亦針對會員資料採取各項安全措施，復於接獲原告通知後，積極查詢原告及其交易相對人之帳號有無自異常IP位置登入之情形，進而提出建議方法，益徵被告對於所屬會員資料之維護，已善盡管理維護責任。原告

管理制度的真正(?)功能

【裁判字號】106,北小,2161

【裁判日期】1070118

【裁判案由】損害賠償

【裁判全文】

臺灣臺北地方法院小額民事判決

106年度北小字第2161號

二、被告則辯以：被告為維護系爭網站個人資料之安全，業已採取各項安全措施，包含於旅客交易連線時採用加密技術（HT TPS）並建置虛擬專用網路（VPN）、旅客交易網站採用防火牆及建置防毒系統、旅客交易網路入口採用負載平衡機制並隔離實體伺服器，並採用網站應用程式防護、旅客交易網站監控網站主機與應用程式傳輸、旅客交易網站採用深度防護偵測技術（Deep Security）以偵測攻擊伺服器、旅客交易網站應用程式通過應用程式源碼檢測等措施以保護旅客交易資料，且有原告個人資料檔案已採行適當之安全措施，並無違反個人資料保護法之故意或過失等情事。再者，

易個資後應採取安全措施之具體內容。而被告就其已依前開辦法制定個人資料檔案安全維護計畫乙節，僅提出一紙載有個人資料檔案安全維護計畫管理手冊之文書為憑據（見本院卷第118頁），然觀諸該文書上所載初版日期為2017年6月1日，已是本案發生後3個月，自無足作為被告於本案發生時已依法訂定個人資料檔案安全維護計畫之佐證，而被告迄未提出本案發生前其已依前開辦法訂定、落實個人資料檔案安全維護計畫及個人資料安全稽核機制等相關事證，堪認被告違反前開辦法所規範之法定義務，而有未依個人資料保護法

如何選擇個資管理制度



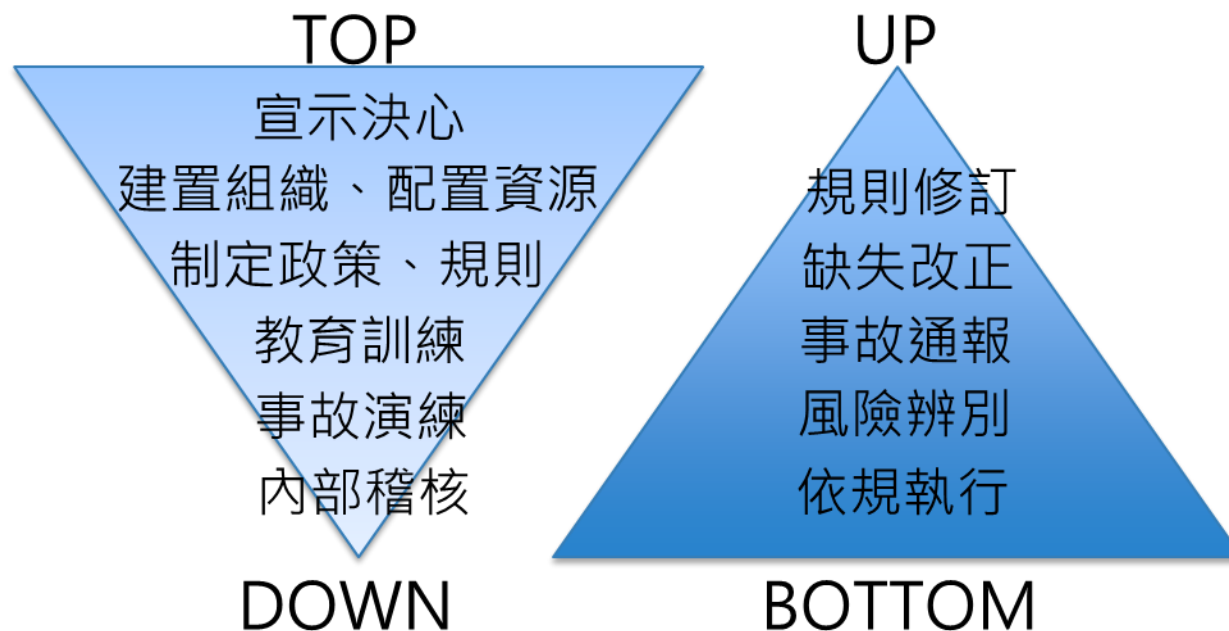
依組織取向選擇

為通過驗證取得標章

為實作符合我國個資法

為合作夥伴的商業要求

有效的管理制度是全組織業務



11+6+3+1

適當安全維護

組織資源配置

界定個資範圍

風險評估機制

通報應變機制

內部管理程序

資安人員管理

認知教育訓練

設備安全管理

安全稽核機制

資料紀錄保存

計畫持續改善

法定告知義務

當事人權利

保存期限

行銷控管

委外監督

事故通知

文件紀錄

個資清查記錄/隱私權聲明紀錄/資料流紀錄
事故紀錄/委外作業紀錄/.....

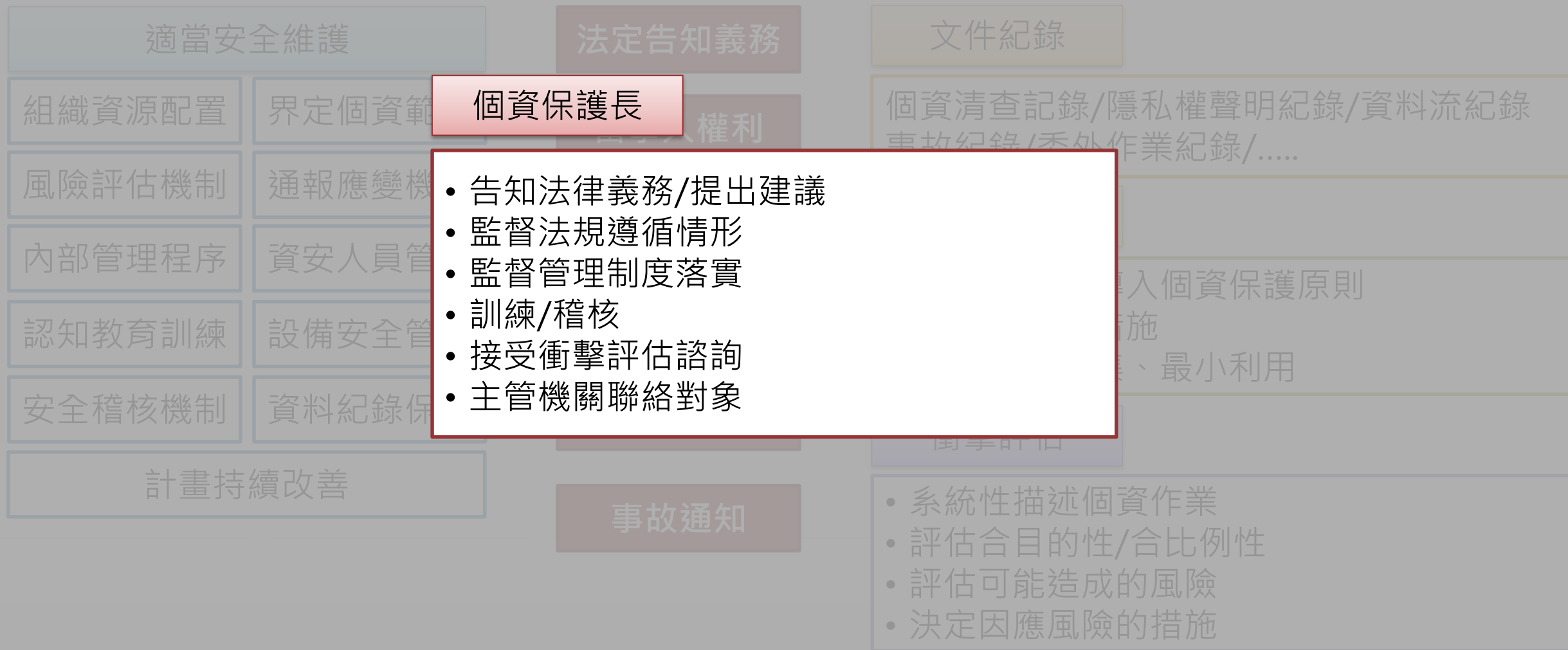
預設保護

事前於流程中導入個資保護原則
整合安全維護措施
預設為最少蒐集、最小利用

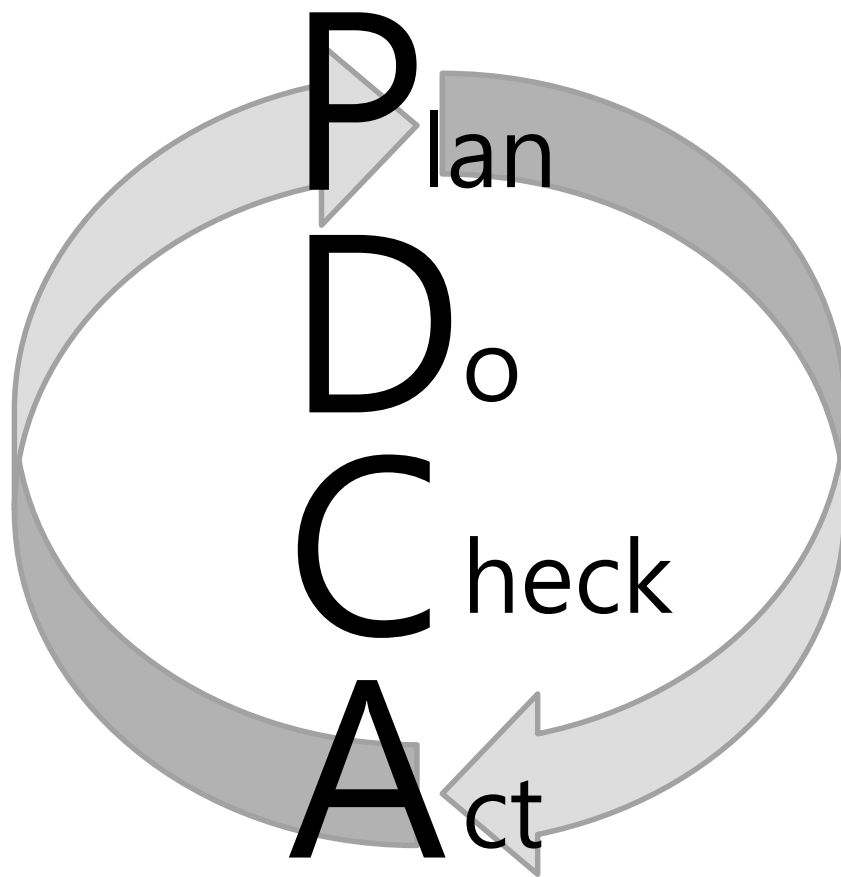
衝擊評估

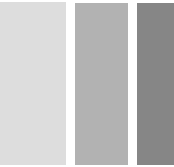
- 系統性描述個資作業
- 評估合目的性/合比例性
- 評估可能造成的風險
- 決定因應風險的措施

11+6+3+1



管理循環





在管理制度之後

下一步 – 資料加值應用

1

導入管理與制度

建立管理階層與政策

個資保護專責職位

個資保護衝擊評估

安全維護措施

匿名化措施

目的相容評估機制

2

提升透明與權利

完整揭露資訊

友善當事人資料存取

給予反對機會

尊重當事人選擇

各項權利行使機制

適度與當事人共享

3

強化問責與通報

合規舉證責任

資料正確性確認

內部稽核執行

考評、懲罰制度

事故通報主管機關

事故通知當事人

謝謝聆聽

THANKS FOR YOUR ATTENTION



達文西個資暨高科技法律事務所
Personal Data and High-Tech Law Firm

王慕民律師

10089 台北市中正區羅斯福路三段162號3樓

TEL: 02-2367-0902