Baker McKenzie.
國際通商法律事務所

AI時代的個資保護議題

Sean Shih 施汝憬律師 | November 3, 2021

Agenda

1. Why data protection matters
2. Personal data protection fundamentals
3. Data issues in AI

1

Why Data Protection Matters

AI 語音點餐惹禍！麥當勞被告侵犯顧客隱私，恐面臨巨額賠償

2021/06/29

伊利諾州麥當勞的一位顧客對麥當勞提起訴訟，稱該公司在**使用語音辨識點餐之前沒有事先獲得同意**，違反了伊利諾州的BIPA（Biometric Information Privacy Act，生物資訊隱私法）。

去年，一位名叫Shannon Carpenter的顧客開車光顧了伊利諾伊州的一家麥當勞，經過了得來速（Drive-through）服務，他的訂單被麥當勞基於 AI 的語音輔助服務接手。

Carpenter認為該項技術**未經他的同意蒐集他的聲紋資訊**，違反了伊利諾伊州2008年頒布的BIPA，今年4月Carpenter將麥當勞告上了當地巡迴法院，5月28日，訴訟被移送伊利諾伊州北部地區美國聯邦地方法院。

滴滴出行上市碰壁市值蒸發6000億

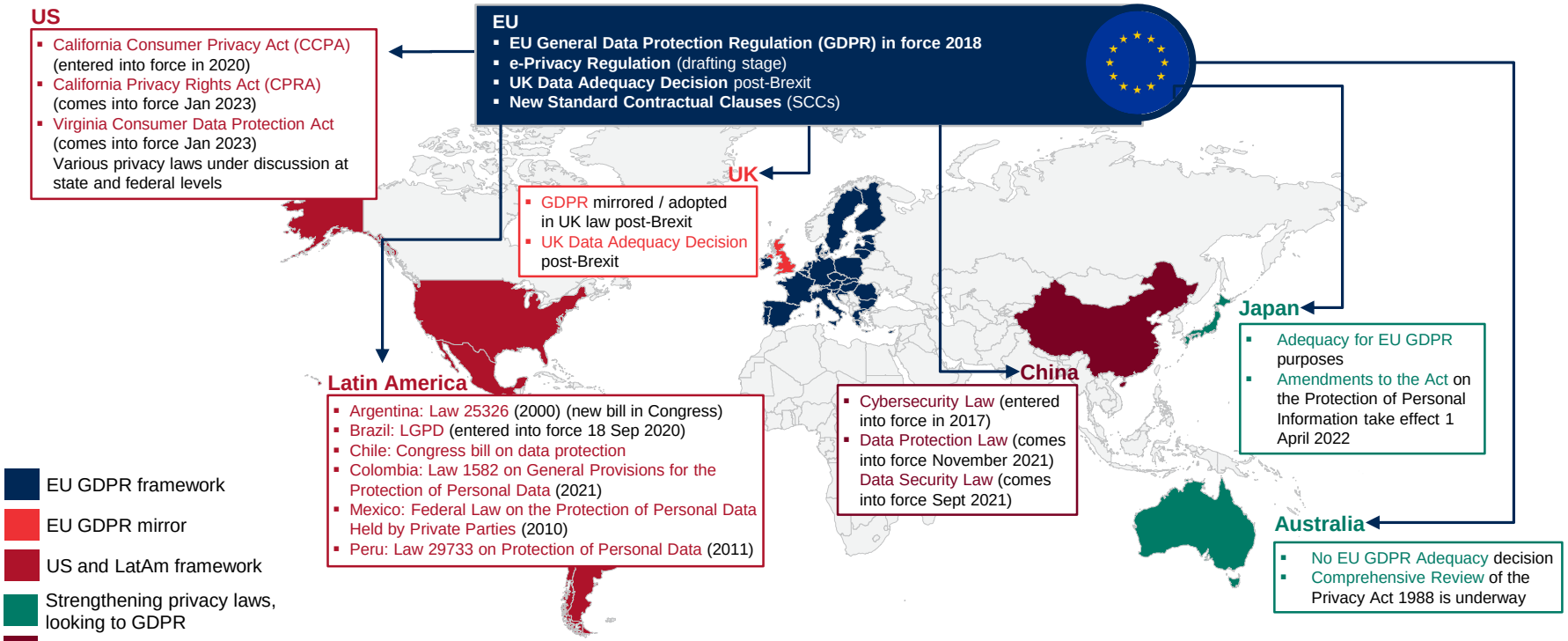
2021/07/16

中國最大叫車平台滴滴出行，2021年6月30日在美國紐約證交所風光上市，籌資約44億美元（約新台幣1228億元），是繼2014年阿里巴巴赴美上市後，規模最大的中國公司IPO（首次公開募股）案。

7月2日，中國網絡安全審查辦公室以**違反網路安全**為由，對滴滴進行審查，並且在審查期間暫停「滴滴出行」新用户註冊，隔兩天，中國網信辦以滴滴**違規收集用戶資訊**為由，將滴滴旗下的25款App在中國全面下架，中國市場占滴滴營運的8成，等於是要滴滴無法營運。才上市短短4天，滴滴市值蒸發2百億美元。

Recent Privacy / Data Protection Developments

The European General Data Protection Regulation (GDPR) has sparked a global privacy trend, with new laws emerging and countries updating their existing laws, increasing the compliance threshold across the world.



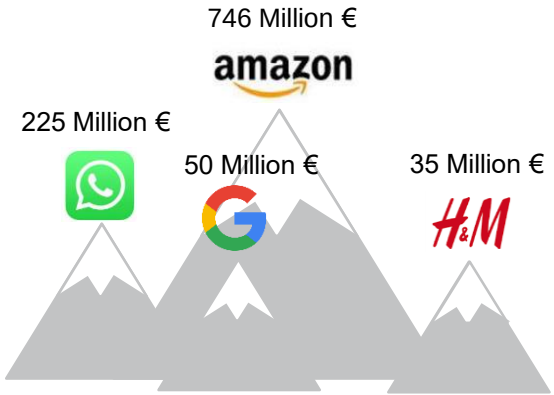
GDPR Enforcement

Drivers for non-compliance

- No management buy-in
- Underestimating requirements and regulatory action
- Insufficient resources
- Lack of awareness / training

Consequences

- Reputational damages
- Loss of customer trust
- Investigations
- Fines



GDPR Fines Stats since May 2018*

Total n° of fines

825

Total sum of fines

€ 1,296,180,178

Countries with highest sum of fines

1 - Luxembourg (€746, 206,000)
2 - Ireland (€ 225,876,400)
3 - Italy (€ 89,645,096)
4 - France (€ 57,314,300)
5 - Germany (€ 50,158,633)

*Source: GDPR Enforcement Tracker as of 26.10.2021

GDPR Enforcement - Fines by type of violation

Violation	Number of Fines
Insufficient legal basis for data processing	**295** (with total € 182,848,138)
Insufficient technical and organizational measures to ensure information security	**176** (with total € 68,583,119)
Non-compliance with general data processing principles	**175** (with total € 782,622,364)
Insufficient fulfilment of data subjects rights	**78** (with total € 16,316,825)
Insufficient fulfilment of information obligations	**61** (with total € 234,946,895)
Insufficient cooperation with supervisory authority	**33** (with total € 210,929)
Insufficient fulfilment of data breach notification obligations	**20** (with total € 1,284,091)

GDPR Enforcement - Fines by sectors

Violation	Number of Fines
Industry and Commerce	**175** (with total € 766,271,292)
Media, Telecoms and Broadcasting	**146** (with total € 363,052,541)
Public Sector and Education	**116** (with total € 9,123,263)
Finance, Insurance and Consulting	**87** (with total € 28,179,685)
Health Care	**76** (with total € 11,932,933)
Employment	**67** (with total € 47,661,677)
Individuals and Private Associations	**56** (with total € 1,342,396)

Why data protection matters

Increasingly huge amounts of personal data are processed online in the **digital age**.

Accelerated by **Covid**: Many work from home and connect to work assets remotely. Surge in consumer online shopping.

Increased **hacking of corporate networks** due to insecure connections & other issues.

Governments worldwide legislating to keep up with rapid development in technology and surge in online activity.

Personal data processed online may flow across borders.
→ Overseas laws may apply.

Current world politics leading to conflicting sets of data regulations and potentially different “data islands”. MNCs caught in the midst. Cross border transfer issues.

Why data protection matters

APAC has **varying laws** on personal data and increasing tendency to **enforce such laws**, **including fines and criminal penalties**.

Laws are evolving rapidly e.g. China launched Cybersecurity Law in 2016 & just passed 2 landmark pieces of legislation: Data Security Law & Personal Information Protection Law.

Fines under some laws, like EU GDPR & China laws, can be **hefty**. There are **personal liabilities** under new China PIPL. Severe breaches may lead to **business suspension or revocation of license**.

Customers, employees, end users & investors are **concerned** about data privacy or subject to data protection laws. **Consumers are turning away from companies that don't prioritize data privacy.**

2

Personal Data Protection Fundamentals

Personal Data Protection Fundamentals

(1)	個人資料保護法是什麼	(7)	當事人權利
(2)	個人資料	(8)	行銷
(3)	去識別化	(9)	資料安全措施
(4)	告知義務	(10)	資料外洩通知
(5)	法定情形	(11)	跨境傳輸
(6)	特定目的	(12)	違法責任

(1)

個人資料保護法是什麼

個人資料保護法

- 規範個人資料之蒐集、處理及利用
- 個人，指現生存之自然人。（施行細則第 2 條）
- 下列情形不適用個資法：

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。
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。（個資法第51條第1項）

(2)

個人資料

個人資料

- 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**。（個資法第2條第1款）
- **直接識別**
  - 姓名、國民身分證統一編號、護照號碼、特徵、指紋、基因
- **間接識別**
  - 指保有該資料之公務或非公務機關僅以該資料不能直接識別，須與其他資料對照、組合、連結等，始能識別該特定之個人。（施行細則第3條）
  - 臺北地院103年度訴字第212號民事判決：「所可能對照、組合、連結之其他資料，如不予限定，均納入個資法所指間接識別個人資料之範圍內，則所有資料均可透過與直接識別個人之上開資料次遞對照、組合、連結而一併納入，且恐失個資法為促進個人資料之合理利用之立法目的。從而，界定間接識別個人資料即不能無所限制，而**須以合理、可能且容易與其他資料對照、組合、連結即得識別個人者為限度**。」。
  - Phone number? Email address? Cookies? Geolocation? Device ID? IP address?

電信事業接獲非該公司客戶之民眾申訴電話號碼，該電話號碼是否屬於個人資料？

本案陳情人並非○○股份有限公司（下稱○○公司）用戶，○○公司未保有其個人資料，再查陳情人與上揭客服人員交談內容，陳情人亦未提及其個人身分識別資訊，於陳情人來電顯示號碼（下稱系爭電話號碼）未連結個人資料之情形下，該電話號碼是否屬個人資料保護法（下稱個資法）所稱個人資料？

- 查陳情人固非○○公司之用戶，惟陳情人之**電話號碼**得透過其所屬電信公司所保有之資料對照、組合、連結，而得以識別該陳情人，即**屬**上開個資法及其施行細則所稱**間接識別之個人資料**。

  （國家發展委員會發法字第1090015912號）

法務部：個人資料保護法之特定目的及個人資料之類別

代 號	識別類
C〇〇一	辨識個人者。 例如：姓名、職稱、**住址**、工作地址、以前地址、**住家電話號碼**、**行動電話**、即時通帳號、網路平臺申請之帳號、**通訊及戶籍地址**、相片、指紋、**電子郵遞地址**、電子簽章、憑證卡序號、憑證序號、提供網路身分認證或申辦查詢服務之紀錄及其他任何可辨識資料本人者等。
C〇〇二	辨識財務者。 例如：**金融機構帳戶之號碼與姓名**、**信用卡或簽帳卡之號碼**、保險單號碼、個人之其他號碼或帳戶等。
C〇〇三	政府資料中之辨識者。 例如：身分證統一編號、統一證號、稅籍編號、保險憑證號碼 、殘障手冊號碼、退休證之號碼、證照號碼、護照號碼等。

法務部：個人資料保護法之特定目的及個人資料之類別

代 號	特徵類
C○一一	個人描述。 例如：年齡、**性別**、出生年月日、出生地、**國籍**、聲音等。

代 號	財務細節
C○八三	**信用評等**。 例如：信用等級、財務狀況與等級、收入狀況與等級等。
C○九三	**財務交易**。 例如：收付金額、信用額度、保證人、支付方式、往來紀錄、 保證金或其他擔保等。

代 號	商業資訊
C一○二	**約定或契約**。 例如：關於交易、商業、法律或其他契約、代理等。

GDPR

- Article 4(1)
  - ‘personal data’ means any information relating to an **identified or identifiable natural person** (‘data subject’); an identifiable natural person is one who can be identified, **directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, **location data**, an **online identifier** or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

CCPA

- Section 1798.140 (o)

(1) “Personal information” means information that **identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked**, **directly or indirectly**, with a particular **consumer** or **household**. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, **online identifier**, **internet protocol address**, **email address**, account name, social security number, driver’s license number, passport number, or other similar identifiers.

(B) Any categories of personal information described in subdivision (e) of Section 1798.80…

(D) **Commercial information**, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) **Biometric information**.

(F) **Internet or other electronic network activity information**, including, but not limited to, browsing history, search history, and information regarding a consumer’s interaction with an internet website, application, or advertisement.

(G) **Geolocation data**.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) **Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer** reflecting the consumer’s preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(3)

去識別化

去識別化

- 個資法就去識別化（deidentification）、匿名化（anonymization）、假名化（pseudonymisation）並無規定
- 個資法所稱**無從識別特定當事人**，指個人資料以**代碼、匿名、隱藏部分資料**或**其他方式**，無從辨識該特定個人者。（施行細則第17條）
- 法務部 103 年 11 月 17 日法律字第 10303513040 號函

  如將公務機關保有之個人資料，運用各種技術予以**去識別化**，而依其呈現方式已無從直接或間接識別該特定個人者，即**非屬個人資料**，自非個資法之適用範圍。
- CNS 29100「資訊技術-安全技術-隱私權框架」、
  CNS 29191「資訊技術 - 安全技術 - 部分匿名及部分去連結鑑別之要求事項」國家標準

去識別化

衛生福利部健保署資料庫案：全民健康保險資料跨公務機構使用

- 最高行政法院106年度判字第54號行政判決:「**對資料之收受者而言**，首應探究，**其收受之資料是否還屬「個人資料」**。而其**判斷準則為資料內容之「去識別化」作業是否已經完成**。如果該資料內容已完成「去識別化」作業，「個人」屬性即已消失，不能再視之為新個資法所規範之「個人資料」，而該資料收受者對資料之後續處理及利用，亦不受新個資法之規範。但若未進行「去識別化」作業，或作業不嚴謹，未達成「去識別化」作業應有之實證效用（即**徹底切斷資料內容與特定主體間之連結**），該收受之資料仍具「個人資料」屬性時，則應依其收受目的是為「處理」或「利用」而受新個資法對應法規範之規制...。」

去識別化

- 最高行政法院106年度判字第54號行政判決:「**本院認為資料尚未『去識別化』**之主要理由即是，從被上訴人（按，衛生福利部中央健康保險署）與輔助參加人衛福部自承之「去識別化」作業模式觀之，由輔助參加人衛福部派專人來執行「加密」作業，再攜回加密之個人資料建置資料庫。如此作業模式即表示輔助參加人衛福部本也**有「還原」資料與主體間連結之能力**，此等結果顯然與由被上訴人「單方」掌握「還原」能力之「去識別化」標準不符。」

GDPR

- Recital 26
  - To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of **all objective factors**, such as the **costs** of and the **amount of time required for identification**, taking into consideration **the available technology at the time of the processing** and **technological developments**.
  - The principles of data protection should therefore **not apply to anonymous information**, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

GDPR

- Recital 26
  - Personal data which have undergone **pseudonymisation**, which could be attributed to a natural person by the use of additional information **should be considered to be information on an identifiable natural person**.
- Article 4(4)
  - '**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;

CCPA

- Section 1798.140 (o)
  (3) “Personal information” **does not include** consumer information that is **deidentified** or aggregate consumer information.

- 1798.140(h)

  “**Deidentified**” means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

  (1) Has implemented **technical safeguards that prohibit reidentification** of the consumer to whom the information may pertain.

  (2) Has implemented **business processes that specifically prohibit reidentification** of the information.

  (3) Has implemented **business processes to prevent inadvertent release of deidentified information**.

  (4) Makes **no attempt to reidentify** the information.

(4)

告知義務

告知義務

- 公務機關或非公務機關依**向當事人蒐集個人資料時**，應明確告知當事人下列事項：
  一、公務機關或非公務機關名稱。
  二、蒐集之目的。
  三、個人資料之類別。
  四、個人資料利用之期間、地區、對象及方式。
  五、當事人依第三條規定得行使之權利及方式。
  六、當事人得自由選擇提供個人資料時，不提供將對其權益之影響。
- 有下列情形之一者，得**免為前項之告知**：
  一、依法律規定得免告知。
  二、個人資料之蒐集係公務機關執行法定職務或非公務機關履行法定義務所必要。
  三、告知將妨害公務機關執行法定職務。
  四、告知將妨害公共利益。
  五、當事人明知應告知之內容。
  六、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。（個資法第 8 條）

告知義務

- 公務機關或非公務機關**蒐集非由當事人提供之個人資料**，應於處理或利用前，向當事人告知**個人資料來源**及前條第一項第一款至第五款所列事項。
- 有下列情形之一者，得免為前項之告知：

一、有前條第二項所列各款情形之一。

二、當事人自行公開或其他已合法公開之個人資料。

三、不能向當事人或其法定代理人為告知。

四、基於公共利益為統計或學術研究之目的而有必要，且該資料須經提供者處理後或蒐集者依其揭露方式，無從識別特定當事人者為限。

五、大眾傳播業者基於新聞報導之公益目的而蒐集個人資料。（個資法第9條）

告知之方式

- 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為之。（施行細則第16條）
- 此一告知並未要求當事人須簽署相關文件，亦未限制不得與其他文件（例如契約）併同為之。惟為達到「明確告知」之目的，蒐集者仍應以個別通知之方式使當事人知悉，不得以單純擺設（張貼）公告或上網公告之概括方式為之，而須足以使當事人知悉或可得知悉該公告內容之方式（例如：須直接向當事人提示公告內容所在位置，並請其閱讀瞭解）始屬之。是以，非公務機關如僅於門市公告或網站公告個資法第8條第1項所定應告知事項，但以現場告知或簡訊告知等各種方式向客戶提示公告內容所在位置，並請其閱讀瞭解，若可達到個別通知使當事人知悉之效果，則可認為符合「明確告知」之意旨。

  （法務部106年10月11日法律字第10603509640號函）

告知「個人資料利用之對象」

- 按個資法第8條第1項之立法意旨在使當事人能充分瞭解其個人資料被他人蒐集之情形，又於告知有關「個人資料利用之對象」（該條項第4款規定）時，以告知時之已知資訊進行適度描述已足，尚無須詳列未知之資訊，亦即，蒐集者應就其利用個人資料之範圍及可能將資料移轉對象之類別，提供合理程度之確定性。
- 如告知客戶利用個資之對象包含「關係企業及合作廠商」，對於利用對象之描述恐過於廣泛，無法合理地界定出個人資料利用對象之類別，尚難認符合本條項立法意旨。

  （法務部106年10月11日法律字第10603509640號函）

臺灣高等法院109年度消上字第12號判決

上訴人主張前述107年9月19日之通知，關於〈為行銷目的使用資料〉之說明不明確...所擬提供並分享用戶個人資訊之官方帳號持有者、廣告商為何？均未明確告知...另前述107年7月2日官方部落格公告，仍未詳盡說明〈為行銷目的使用資料〉，僅略稱用戶資訊僅於「必要最低限度內」分享給「屬於LINE責任範圍」的第三方，第三方包括臺灣連線股份有限公司(LINETaiwanLimited)、連加網路商業股份有限公司（LINEBiz+TaiwanLimited）等，仍未具體就提供用戶之「何範圍」之個資予「何範圍」之對象為說明，難謂被上訴人已依個資法第7條之規定明確告知蒐集個資之目的及同意與否所可能產生的影響...等語。

臺灣高等法院109年度消上字第12號判決

系爭服務契約性質應為雙務契約，即由被上訴人提供LINE通訊軟體使上訴人等用戶使用電腦、手機等智慧型裝置，透過網際網路對他人傳送聲音、圖像、文字、數據、檔案或其他訊息；而上訴人於使用LINE通訊軟體之同時亦提供其個人資料等數據供被上訴人於提供LINE服務範圍內為蒐集及利用，且被上訴人以此方式吸引更多使用者，創造其產品在市場上的領先地位等，據此，被上訴人未向上訴人收費而提供LINE服務，是為吸引更多用戶及蒐集、利用用戶個資，以創造其市場地位，藉以吸引更多廣告商、協力廠商等以營利，則就市場競爭、商業經營牟利與瞬息萬變之商業經濟活動而言，實難要求被上訴人僅與特定範圍之廣告商、協力廠商合作，因此，被上訴人辯稱個資利用之範圍及對象無法在當下確定，目前做不到具體說明利用個資範圍，原來條文的設計就是廣泛的指相關的協力廠商等語，尚難認有逾越合理範圍。上訴人若無法接受此等廣泛的授權，可以選擇退出直接行銷機制或選擇停止繼續使用LINE服務，而選擇其他通訊軟體廠商所提供的類似服務例如WhatsApp、WeChat等，並非只有被上訴人有提供即時通訊軟體服務，因此，難謂有被上訴人未善盡說明義務，妨害上訴人個資自主權之合法權益行使之情事。

(5)

法定情形

法定情形

- 非公務機關對個人資料之蒐集或處理，應符合下列情形之一者：

  一、法律明文規定。

  二、**與當事人有契約或類似契約之關係**，且已採取適當之安全措施。

  三、當事人自行公開或其他已合法公開之個人資料。

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

  五、**經當事人同意**。

  六、為增進公共利益所必要。

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

  八、對當事人權益無侵害。

- 蒐集或處理者知悉或經當事人通知依前項第七款但書規定禁止對該資料之處理或利用時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。（個資法第19條）

非公務機關為與客戶成立契約而蒐集客戶個資（例如：請求客戶填寫基本資料表），如個人資料係於履行契約事務之必要範圍內所蒐集者，是否需再另行取得當事人同意？

- 非公務機關為與客戶成立契約而蒐集客戶個資（例如：請求客戶填寫基本資料表），如上開個人資料係於**履行契約事務之必要範圍內**所蒐集者，則該蒐集行為與個資法第19條第1項第2款**「與當事人有契約或類似契約之關係」規定相符**，而**無須再另行取得當事人同意**（個資法第19條第1項第5款規定）。
- 然如所蒐集者包括**其他與契約履行無關之個人資料**或**並非為履行契約所必需者**，則應依個資法第7條第1項規定，應於契約之外**另行取得當事人同意**，始為合法。
- 非公務機關與個人資料當事人間具有個資法第19條第1項第2款之關係存在時，應優先適用此款，不能再以同條項第5款作為蒐集事由，以避免個人資料當事人立於不對等地位而無法真正作成自主決定（例如：以同意做為契約成立前提）；甚至在已有其他合法事由下，仍尋求當事人同意，更有可能顯失公平。

（法務部106年10月11日法律字第10603509640號函）

同意

- 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。
- 公務機關或非公務機關明確告知當事人應告知事項時，當事人如未表示拒絕，並已提供其個人資料者，推定當事人已表示同意。
- 蒐集者就本法所稱經當事人同意之事實，應負舉證責任。（個資法第7條）
- 公司將**告知書**與**同意書**列於同一書面而未明顯區隔，易造成員工混淆，而為概括同意。為避免員工混淆，於執行個資法第 8 條之告知說明，與同法第19條第5款、第20條第1項第6款需取得當事人書面同意而為特定目的外利用等情形，**宜於不同書面**，或另**於同一書面之適當位置明顯區隔為之**，始為適法。（法務部102年12月5日法律決字第10200683890號）

LINE要點「同意」才能繼續用 退休教授提告求償二連敗

2021/07/20 自由時報

前台灣科技大學鄭姓教授，3年前不滿通訊軟體LINE**要求用戶必須點選「同意」新的隱私權政策，才能繼續使用**，導致他因「不同意」而未點選，無法繼續使用通訊服務，對LINE提告要求提供他先前的通訊紀錄，並求償10萬元，台北地院判他敗訴；鄭男提起上訴，高等法院認定LINE未妨害鄭姓退休教授個資自主權的行使，今仍判他敗訴。

鄭姓退休教授認為，LINE突然在2018年9月19日通知他變更隱私權政策，要求他點選「同意」按鈕，才能繼續使用LINE的服務，沒有讓用戶具有「不同意」的選項，他未點選「同意」按鈕，遭LINE片面停止提供通訊服務，LINE的這項隱私權政策變更，欠缺合理性。

臺灣高等法院109年度消上字第12號判決

被上訴人稱其早在107年6月25日就已經於官網預告即將更新隱私權政策，隨後於107年7月2日在官方部落格公告於「該日」更新隱私權政策，用戶會陸續在手機的LINE中，收到需要用戶同意的通知視窗等，並說明更新隱私權政策相關事項，包括**用戶必須就「LINE隱私權政策變更」與「LINE得為了行銷目的使用及分享本人資訊」等2個選項點選「同意」按鈕，才能繼續使用LINE服務之說明**...同時告知**如果用戶不希望自己的資料被使用於行銷目的，可以在勾選同意後，於繼續使用LINE服務時，進入「設定」選項，選擇退出直接行銷機制**，且被上訴人係在公告變更內容2個月後之107年9月19日向上訴人提出變更系爭隱私權政策之通知，於該通知中，亦有就前述事項再次說明乙情... 足認被上訴人已依系爭應記載事項第9條規定向用戶包含上訴人在內，公告及通知變更之內容、蒐集個資之目的及同意與否所可能產生的影響。

臺灣高等法院109年度消上字第12號判決

上訴人若不希望自己的資料被使用於行銷目的，可以在勾選同意後，於繼續使用LINE服務時，進入「設定」選項，選擇退出直接行銷機制，**並非無「不同意」之選項**，即使操作上較為繁瑣一些，但尚無違反系爭應記載及不得記載事項。從而，上訴人主張被上訴人於107年9月19日所提出變更系爭隱私權政策之通知，須點選「同意」按鈕，才能繼續使用LINE服務，且無「不同意」之勾選框，如不勾選同意即無法繼續使用LINE服務云云，尚難採信。

被上訴人已於107年7月2日公告及107年9月19日通知中告知上訴人，若不同意系爭隱私權政策之變更，仍可在勾選同意後，進入「設定」選項，選擇退出直接行銷機制，已如前述，雖較為繁瑣，然並未影響上訴人之自由意思之程度，**更難謂是「強制」**…。

(6)

特定目的

特定目的

- 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。（個資法第5條）
- 非公務機關對個人資料之蒐集或處理，應有特定目的（個資法第19條）

特定目的外之利用

- 非公務機關對個人資料之利用，應於蒐集之特定目的必要範圍內為之。但有下列情形之一者，得為特定目的外之利用：

  一、法律明文規定。

  二、為增進公共利益所必要。

  三、為免除當事人之生命、身體、自由或財產上之危險。

  四、為防止他人權益之重大危害。

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

  六、**經當事人同意**。

  七、有利於當事人權益。（個資法第20條）

- 同意，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。（個資法第7條）

如行銷與當事人契約或類似契約內容無涉之商品或服務資訊，是否需再另行取得當事人同意？

- 所稱「蒐集之特定目的必要範圍內」，如係依據個資法第19條第1項第2款規定，並基於「行銷」（代號：040）、「契約、類似契約或其他法律關係事務」（代號：069）或「其他經營合於營業登記項目或組織章程所定業務」（代號：181）之特定目的而蒐集個人資料，則**其利用需與原蒐集之要件「與當事人契約或類似契約之關係」有正當合理之關聯，始能屬特定目的內利用**。換言之，非公務機關使用基於契約或類似契約關係下取得之個人資料，對該個人當事人進行行銷，應合乎社會通念下當事人對隱私權之合理期待，故**「行銷行為內容」與「契約或類似契約」二者間，應有正當合理之關聯，始符合個資法第20條第1項本文規定特定目的內利用之範疇，而無需再得「當事人同意」**（同條項但書第6款）。
- 如**行銷與當事人契約或類似契約內容無涉之商品或服務資訊**，則除符合個資法第20條第1項但書第1款至第5款或第7款事由外（例如：為增進公共利益或免除當事人生命、身體、自由、財產上之危險等事由），**應**依同條項但書第6款規定**經當事人同意**（同意方式請依個資法第7條第2項規定），始得為之。

（法務部106年10月11日法律字第10603509640號函）

如行銷與當事人契約或類似契約內容無涉之商品或服務資訊，是否需再另行取得當事人同意？

- 是以，如蒐集客戶個資之目的包含「行銷（含行銷本公司業務及與本公司合作或業務往來之關係企業及合作廠商之商品或服務）」，其中「行銷與本公司合作或業務往來之關係企業及合作廠商之商品或服務」部分，涉及**將客戶個資提供予當事人以外第三人為特定目的外之利用，應符合個資法第 20 條但書規定情形之一，始得為之**。

  （法務部106年10月11日法律字第10603509640號函）

(7)

當事人權利

當事人權利

- 當事人就其個人資料依個資法規定行使之下列權利，不得預先拋棄或以特約限制之：

  一、查詢或請求閱覽。

  二、請求製給複製本。

  三、請求補充或更正。

  四、請求停止蒐集、處理或利用。

  五、請求刪除。（個資法第 3 條）

當事人權利

- 公務機關或非公務機關應依當事人之請求，就其蒐集之個人資料，**答覆查詢**、**提供閱覽**或**製給複製本**。但有下列情形之一者，不在此限：

  一、妨害國家安全、外交及軍事機密、整體經濟利益或其他國家重大利益。

  二、妨害公務機關執行法定職務。

  三、妨害該蒐集機關或第三人之重大利益。（個資法第10條）

- 公務機關或非公務機關受理當事人上述請求，應於**十五日**內，為准駁之決定；必要時，得予延長，延長之期間不得逾**十五日**，並應將其原因以書面通知請求人。（個資法第13條第1項）

- 查詢或請求閱覽個人資料或製給複製本者，公務機關或非公務機關得**酌收必要成本費用**。（個資法第14條）

當事人權利

- 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。
- **個人資料正確性有爭議者**，應主動或依當事人之請求停止處理或利用。但因執行職務或業務所必須，或經當事人書面同意，並經註明其爭議者，不在此限。
- 個人資料蒐集之**特定目的消失**或**期限屆滿**時，應主動或依當事人之請求，刪除、停止處理或利用該個人資料。但因執行職務或業務所必須或經當事人書面同意者，不在此限。
- **違反本法規定蒐集、處理或利用個人資料**者，應主動或依當事人之請求，刪除、停止蒐集、處理或利用該個人資料。
- 因可歸責於公務機關或非公務機關之事由，未為更正或補充之個人資料，應於**更正或補充後，通知**曾提供利用之對象。（個資法第11條）
- 公務機關或非公務機關受理當事人上述請求，應於**三十日**內，為准駁之決定；必要時，得予延長，延長之期間不得逾**三十日**，並應將其原因以書面通知請求人。（個資法第13條第2項）

(8)

行銷

行銷

- 非公務機關利用個人資料行銷者，**當事人表示拒絕接受行銷時，應即停止**利用其個人資料行銷。

- 非公務機關於首次行銷時，**應提供當事人表示拒絕接受行銷之方式**，並**支付所需費用**。（個資法第20條）

首例 廣告電郵擾民 特力屋判賠2.6萬

2014年10月15日 傳送 讚 1,380 G+1 6

郭姓會計師拿著會員卡，指控特力屋違反《個資法》。趙元彬攝

【吳珮如／台北報導】郭姓會計師前年退出大型賣場特力屋會員，並要求刪除個人資料，特力屋回信允諾，但郭男後續半年內仍收到特力屋電子廣告信共五十二封，不堪其擾，怒告特力屋違反《個人資料保護法》求償十萬元。士林地院日前判決特力屋須賠償郭男兩萬六千元。這是《個資法》上路以來，因廣告信擾人判賠首例。

(9)

資料安全措施

資料安全措施

- 非公務機關保有個人資料檔案者，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。（個資法第27條）
- 適當之安全措施，指公務機關或非公務機關為防止個人資料被竊取、竄改、毀損、滅失或洩漏，採取**技術上**及**組織上之措施**。（施行細則第12條）
- 中央目的事業主管機關得指定非公務機關訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。（個資法第27條）
  - **金融監督管理委員會指定非公務機關個人資料檔案安全維護辦法**
  - **製造業及技術服務業個人資料檔案安全維護管理辦法**

36萬筆個資外洩 雄獅旅行社免賠

2019/11/01 中國時報

- 雄獅旅行社電腦主機在2017年遭駭客入侵，從中竊取數萬顧客的身分證等個資，有25位民眾聲稱因此遭詐騙集團來電騙錢，消基會整理被害人資料，發起**國內首宗個資受害團體訴訟**，具體求償450萬9575元，士林地院認為，這是**第3者惡意入侵，雄獅有善盡管理責任**，昨判決消基會敗訴。
- 雄獅強調，個資遭竊後即向檢調報案，另以簡訊、電子郵件、網站聲明、實體通路門市等多重管道，主動提醒客戶，另委託專業資安防護公司，協助修復遭破壞的漏洞，系統也加密升級，有盡善良管理人注意義務，民眾後來被騙，也是詐騙集團所為，與雄獅沒有因果關係。
- 合議庭審酌，本案是第3人惡意入侵，且駭客攻擊時有所聞，現今科技也無法完全避免，雄獅事後立刻報警，並發布重大訊息告知消費者，已採取適當防護行為，避免可能發生的財產損害，且原告無法證明事後被騙，是否與雄獅個資洩漏有關，判決消基會敗訴。全案可上訴。
- 該訴訟案在2020年7月於台灣高等法院民事庭成立調解，消費者也獲得賠償金。

臺灣士林地方法院107年度消字第6號判決

- 被告公司已提出其**個人資料檔案安全維護計畫**（見本院卷一證物袋內），經**與交通部觀光局所發布之旅行業個人資料檔案安全維護計畫範本**...比對後，**內容大致相符**，包含個人資料處理及利用管理措施、事故預防、通報及應變機制、資料安全管理（包含員工、設備）及相關稽核機制等項目，均有明定，其中關於指定員工定期清查所保有之個人資料、設定員工不同權限以分別控管掌握之個人資料，以及輸出入個人資料時均需使用識別密碼、定期變更密碼等方式作為加密機制等，亦符合前揭旅行業個人資料檔案安全維護計畫及處理辦法第4條第1項、第13條第1款、第14條第2款等規定，至於**計畫執行層面，被告公司亦進行內部稽核、資料安全人員職業訓練，並定期變更電腦系統作業密碼**等情，有**被告公司向交通部觀光局提出之內部稽核報告、系統指令頁面、職業訓練等資料**為憑...足見**被告公司為保有所掌握之個人資料檔案，已採行合於個資法所定之安全措施**。

- 況且，兩造均不爭執本件個人資料外洩肇因於第三人入侵被告公司電腦作業系統所為之竊取行為，已如前述，益徵本件個人資料外洩並非被告公司管理不當所致，而鑑於電腦科技雖日新月異，然駭客惡意入侵電腦系統進行攻擊之事仍層出不窮，足見現今科技尚無法提供可完全防堵駭客攻擊之防護技術，自不能僅以被告公司電腦系統遭他人惡意入侵竊取資料一事，遽而推論其違反個資法規定或管理上有所疏失。

(10)

資料外洩通知

資料外洩通知

- 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**。（個資法第12條）
- 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。
- 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**。（施行細則第22條）

資料外洩通知

- 「**即時**」，應指**不得為不必要之拖延**；又具體個案是否構成「不必要之拖延」，應依個案情節，考量公務機關或非公務機關初步查明個資侵害事故，及採取適當措施避免損害擴大所需之合理時間；通知對於當事人及時採取措施以防止立即性損害發生之必要性；以及於相關主管機關介入時，該個資侵害事故之揭露是否可能妨礙主管機關進行調查等因素為判斷。
- 「**個人資料被侵害之事實**」及「**已採取之因應措施**」等通知事項，應包括：**個資外洩之事實**、**業者所採取之因應措施**及**所提供之諮詢服務專線**。又上開規定未限制公務機關或非公務機關提供與個資侵害事故有關之其他訊息...建議公務機關或非公務機關於適當時，宜併提供**當事人應採取措施之具體建議**（例如重新設定密碼、聯繫銀行及信用卡發行公司、警戒可能之詐騙行為），以防止損害之發生或擴大。

（法務部105年4月20日法制字第10502506140號函）

麥當勞遭駭 台灣客戶個資也外洩

臺灣士林地方法院108年度湖小字第558號判決

- 被告於知悉其網站遭不法入侵後，於106年5月27日以主旨為「重要必看！雄獅會員防詐騙說明。保障自身財物安全」電子郵件之通知會員，並於同年月23日及26日寄送如前揭意旨之提醒詐騙之簡訊至原告所有0000000000門號等情，有電子郵件及簡訊內容在卷可佐...並為原告所不爭執，應認**被告知悉其網站遭入侵後亦有採取相當之措施**。

- 本件縱認被告如未疏於維護其公司網站內之原告個人資料，原告不致被詐騙份子詐騙而受財物損失，而認被告之疏失行為可謂原告財產權受損害之不可欠缺之條件。然被告已106年5月23日及26日寄送如前揭意旨之提醒詐騙之簡訊至原告所有手機門號，予以提醒，原告即應對此一詐騙技倆有所警覺，然原告未有所警覺，因其個人疏忽而誤信詐騙份子伎倆，致被詐騙份子詐騙，又衡諸一般情形，客戶資料外洩固係對於客戶隱私權之侵害，然並不必然發生客戶受詐騙且受有財物損失之財產權侵害結果。是以**被告縱令有疏失行為，其與原告之財物損失結果，不得謂有相當之因果關係**，依前揭說明，即難認被告應就原告被詐騙之損失負責。

(11)

跨境傳輸

跨境傳輸

原則允許，例外限制

- 非公務機關為國際傳輸個人資料，而有下列情形之一者，中央目的事業主管機關得限制之：

  一、涉及國家重大利益。

  二、國際條約或協定有特別規定。

  三、接受國對於個人資料之保護未有完善之法規，致有損當事人權益之虞。

  四、以迂迴方法向第三國（地區）傳輸個人資料規避本法。（第21條）

- 國家通訊傳播委員會：限制**通訊傳播事業經營者**將所屬用戶之個人資料傳遞至大陸地區

- **金融機構作業委託他人處理內部作業制度及程序辦法**：須金管會核准

(12)

違法責任

違法責任

- **民事責任（公司及個人）**
  - 非公務機關違反本法規定，致個人資料遭不法蒐集、處理、利用或其他侵害當事人權利者，**負損害賠償責任。但能證明其無故意或過失者，不在此限**。
  - 如被害人**不易或不能證明其實際損害額**時，得請求法院依侵害情節，以每人每一事件**新臺幣五百元以上二萬元以下**計算。
  - 對於同一原因事實造成多數當事人權利受侵害之事件，經當事人請求損害賠償者，其合計**最高總額以新臺幣二億元為限**。但因該原因事實所涉利益超過新臺幣二億元者，以該所涉利益為限。（第28、29條）

違法責任

- 刑事責任（個人）
  - **意圖為自己或第三人不法之利益**或**損害他人之利益**，而違反第六條第一項、第十五條、第十六條、第十九條、第二十條第一項規定，或中央目的事業主管機關依第二十一條限制國際傳輸之命令或處分，足生損害於他人者，處五年以下有期徒刑，得併科新臺幣一百萬元以下罰金。（第41條）
  - **意圖為自己或第三人不法之利益**或**損害他人之利益**，而對於個人資料檔案為非法變更、刪除或以其他非法方法，致妨害個人資料檔案之正確而足生損害於他人者，處五年以下有期徒刑、拘役或科或併科新臺幣一百萬元以下罰金。（第42條）
  - 最高法院109年度台上大字第1869號裁定：個人資料保護法第41條所稱「意圖為自己或第三人不法之利益」，應限於財產上之利益；至所稱「損害他人之利益」，則不限於財產上之利益。

違法責任

- **刑事責任常見情形**
  - 兩人之間因為糾紛涉訟，敗訴的一方心有未甘，把未將個人姓名、住所、職業等個人資料遮蓋的判決書，貼在社群媒體上要大家評評理。
  - 情人之間鬧翻了，就將對方的姓名、手機號碼、車號，甚至兩人間的私密照片、影片、性歷史等放在網路上或散布在LINE群組上公諸於世。
  - 員工竊取、外洩公司的顧客之個人資料。

違法責任

- **行政責任（公司及負責人）**
  - 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府處**新臺幣五萬元以上五十萬元以下罰鍰**，並令限期改正，屆期未改正者，按次處罰之：
    一、違反第六條第一項規定。（敏感個資）
    二、違反第十九條規定。（特定目的、法定情形）
    三、違反第二十條第一項規定。（特定目的外之利用）
    四、違反中央目的事業主管機關限制國際傳輸之命令或處分。（第47條）
  - 非公務機關有下列情事之一者，由中央目的事業主管機關或直轄市、縣（市）政府**限期改正**，屆期未改正者，按次處**新臺幣二萬元以上二十萬元以下罰鍰**：
    一、違反第八條或第九條規定。（告知義務）
    二、違反第十條、第十一條、第十二條或第十三條規定。（當事人權利、資料外洩通知）
    三、違反第二十條第二項或第三項規定。（行銷）
    四、違反第二十七條第一項或未依第二項訂定個人資料檔案安全維護計畫或業務終止後個人資料處理方法。（第48條）

違法責任

- **行政責任（公司及負責人）**
  - 非公務機關之**代表人、管理人**或**其他有代表權人**，因該非公務機關依前三條規定受罰鍰處罰時，**除能證明已盡防止義務者外**，應並受同一額度罰鍰之處罰。（第50條）
  - 非公務機關有違反本法規定之情事者，中央目的事業主管機關或直轄市、縣（市）政府除依本法規定裁處罰鍰外，並得為下列處分：

    一、**禁止蒐集、處理或利用個人資料**。

    二、命令刪除經處理之個人資料檔案。

    三、沒入或命銷燬違法蒐集之個人資料。

    四、公布非公務機關之違法情形，及其姓名或名稱與負責人。（第25條）

3

Data Issues in AI

(1)

Data Issues in Acquiring Training Data

Does the model trainer have a license to the dataset?

- **Datasets are downloaded from the Internet**
  - No license but statement that “This dataset is for non-commercial use only.”
  - Is training a machine learning model a “non-commercial” use?
- **Recommendation:** Exercise caution and review each license in context with its facts, license agreement, if any, and the intended use.

Licensors of datasets made from data scraped from the Internet may have a copyright in the compilation, but may not own or license the underlying data

Data Due diligence is important

- Is the underlying content a copyrightable work of authorship?
- Will copying include the structure and organization of the compilation?
- Promises to remove content from datasets upon request suggests that the datasets include other people's original works

Storing copyrighted content for use in training the data model may be alleged to be acts of “copying” and to support a claim of copyright infringement

Under the Copyright Act, a successful plaintiff may recover:

- actual damages;
- disgorgement of profits attributable to the infringement;
- statutory damages per work infringed, which can be increased if the infringement is willful; and
- an injunction preventing further infringement

(2)

Data Privacy and Security in Machine Learning

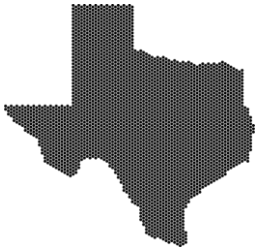
Notice and Consent – State Biometric Laws

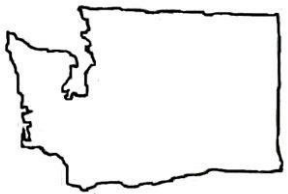
Biometrics Privacy Remedies Available

Illinois: private right of action, class actions allowed, up to $5,000 in liquidated damages per violation

Texas: no private right of action, enforceable only by the Attorney General, up to $25,000 in civil penalties per violation

Washington: no private right of action, enforceable only by the Attorney General under the Consumer Protection Act





Notice and Consent: GDPR Automated Decision-Making

GDPR Article 22 “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”

Exception: Where the decision is based on the data subject’s explicit consent.

Notice and Consent: GDPR Automated Decision-Making

- To lawfully process data for individuals that are subjects of the EU, you must obtain “freely given, specific, informed and unambiguous” consent from the data subject.
- In the context of ML, to obtain such consent you must disclose a variety of things including the existence of any automated decision-making.
- Article 13(2)(f) “[T]he controller shall, at the time when personal data are obtained” provide the data subject with *“meaningful information about the logic involved,* as well as the significance and the envisaged consequences of such processing for the data subject”.

Notice and Consent: CCPA

1798.100 (Right to access) ***A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as*** to the categories of personal information to be collected and ***the purposes for which the categories of personal information shall be used. A business shall not*** collect additional categories of personal information or ***use personal information collected for additional purposes without providing the consumer with notice consistent with this section.***

Notice and Consent: CPRA Automated Decision-Making

The California Privacy Rights Act of 2020 (CPRA) was passed on November 3, 2020. The CPRA will become enforceable on January 1, 2023 with a one-year lookback period.

1798.185 (a)(16) On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including [….] issuing regulations governing access and ***opt-out rights with respect to businesses' use of automated decision-making technology***, including **profiling** and requiring ***businesses' response*** to access requests ***to include meaningful information about the logic involved in such decision-making processes,*** as well as ***a description of the likely outcome of the process with respect to the consumer.***

Delta Sues Chatbot Provider Over Breach

- Delta alleges that chatbot provider [24]7.ai Inc. lacked basic cybersecurity safeguards while running the AI-powered service on Delta's website.
- Hackers accessed [24]7's systems and modified source code using compromised credentials.
- Hackers were able to scrape full credit-card details and other personal information from up to 825,000 customers from Delta's website.
- Delta alleges 24[7] failed to implement basic security controls such as requiring multifactor authentication for employees accessing source code and forbidding staff members from using the same login credentials for all systems.

Q&A

Sean Shih
Partner – Taipei
sean.shih
@bakermckenzie.com

Baker McKenzie.
國際通商法律事務所

bakermckenzie.com