

敏感个人信息面面观：概念溯源与域外制度对比

作者：潘永建 | 朱晓阳 | 邓梓珊 | 李佳琪

我国现行法律法规尚未针对敏感个人信息出台具体且明确的识别规则。如[本系列前篇文章](#)所述，现阶段我们可以依据法律法规、各类国标文件中的定义、示例与识别准则，参考行政与司法实践中的认定案例，对敏感个人信息的识别得出相对肯定的结论，但随着数据流通演变与技术发展，实务中的困扰仍将客观长期存在。

鉴于敏感个人信息这一概念本身为“舶来品”，且已在多个国家由法律法规予以特殊保护，我们在本篇文章引入比较法视野，对敏感个人信息的定义逐本溯源，简要梳理并对比分析[欧盟、美国、新加坡、日本与韩国](#)在敏感个人信息定义、范围与保护措施的异与同，帮助大家综合理解敏感个人信息的内涵与外延，并为涉外数据业务提供实务参考。

一. 敏感个人信息的概念溯源

目前，大多数国家与地区倾向采取“一般与特殊”的个人信息二分法，但各国对特殊类型个人信息所用称谓并不一致¹。从定义来看，综合对比内涵与外延，中美对特殊类型个人信息所称“敏感个人信息(Sensitive Personal Information)”近似欧盟所用的“特殊类型个人信息(Special Categories of Personal Data/Information)”²或日本的“需要特殊保护的个人信息(Special Care-Required Personal Information)”，而其概念均来源于欧洲存在较久的“敏感数据(Sensitive Data)”(为免歧义，[下文暂以“敏感个人信息”统一指代以上概念](#))。

.....
如您需要了解我们的出版物，
请联系：

Publication@llinkslaw.com

敏感个人信息概念的演变历程简要梳理如下表所示：

¹ 参考韩新远：敏感个人信息的多维认定与严格保护，载《数字法治》2024 年第 2 期。

² 欧盟 GDPR 正文部分 Art.9 采用“特殊类别的个人信息数据(Special Categories of Personal Data/Information)”的表述，但在其“鉴于条款” Recital 51 又采用“敏感个人数据(Sensitive Personal Data)”的表述。



表 1 敏感个人信息概念的演变历程³

二. 不同国家/地区敏感个人信息范围之异同

从保护原则来说，各国通过界定敏感个人信息，对特殊类型的个人信息予以强化保护。但结合下表所整理的域外敏感个人信息类型对比(本文以中国、欧盟、美国、新加坡、日本、韩国为样本，下同)，可以发现各国/地区所界定敏感个人信息的具体范围**不尽相同**。

³ 参考 Solove, Daniel J., Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data. 118 Northwestern University Law Review 1081 (2024).

☐ 法律法规	☐ 指引性文件	明文列为“敏感”或“特殊”的个人信息类型 (非穷尽列举)											
各国/地区数据领域主要法律或指引性文件		生物识别 ⁴	未成年人 ⁵	特定身份 ⁶	医疗健康	金融账户/财产	行踪轨迹/位置	宗教/哲学信仰	政治观点	种族民族血统	通信内容/记录	性生活/性取向	违法犯罪记录
中国 《个人信息保护法》 《信息安全技术 个人信息安全规范 (GB/T 35273-2020)》		☐	☐	☐	☐	☐	☐	☐			☐	☐	☐
欧盟 《通用数据保护条例(GDPR)》		☐	☐		☐			☐	☐	☐		☐	☐
美国 《加州隐私权法案(CPRA)》《儿童在线隐私保护法(COPPA)》《数据隐私和保护法(ADPPA)》(草案)等 ⁷		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
新加坡 PDPC ⁸ 发布的系列专项指南		☐	☐	☐	☐	☐	☐	☐		☐		☐	☐
日本 《个人信息保护法(個人情報保護法/APPI)》及条例、专项指南				☐	☐	☐		☐		☐			☐
韩国 《个人信息保护法(PIPA)》 PIPC ⁹ 发布的系列专项指南		☐	☐	☐	☐	☐			☐	☐		☐	

表 2 域外敏感个人信息类型对比(以中国、欧盟、美国、新加坡、日本、韩国为样本)

可以发现, 较多国家及地区认为与特定身份、医疗健康、宗教信仰、种族民族、性生活/性取向、刑事犯罪记录以及未成年人相关的个人信息属于敏感个人信息。此类信息的相似处在于, 其或具有唯一识别特定个人的能力(例如特定身份信息中的身份证件号码), 或与社会观念下的人格尊严存在较强联系(例如宗教信仰、性取向)。

⁴ 包括个人基因信息。
⁵ 需注意, 未成年人的个人信息在各国法规下并非一定敏感, 但或出于倾斜保护目的, 部分国家选择将其拟制为法律上的敏感个人信息进行保护。参考韩新远: 敏感个人信息的多维认定与严格保护, 载《数字法治》2024 年第 2 期。
⁶ 包括身份证件号码。
⁷ 美国对敏感个人信息的规制采取分散立法模式。以生物识别信息为例: 在联邦法律层面, 除草案《数据隐私和保护法(ADPPA)》有所规定外, 尚无生效法律将生物识别信息列为敏感个人信息; 而在州层面, 部分州通过单独立法将生物识别信息列为敏感个人信息予以保护, 例如已生效的《伊利诺伊州生物识别信息隐私法(BIPA)》。
⁸ 即, 新加坡个人数据保护委员会(Personal Data Protection Commission)。
⁹ 即, 韩国个人信息保护委员会(Personal Information Protection Commission)。

然而，生物识别信息、地理位置信息、政治观点、通信内容等个人信息的敏感性认定则呈现差异性。其原因或根植于个人信息保护立法模式与敏感个人信息保护法益的国别差异。换言之，因为不同国家个人信息保护制度的形式不同，立法者所认为的现阶段最应优先保护的法益不同、保护特定类型的个人信息所能防控的风险不同，从而综合导致各国从海量个人信息中所挑选出的敏感个人信息的结果不同。

三. 不同国家/地区保护敏感个人信息的原则与具体措施

除了定义与范围不同，敏感个人信息的域外保护模式也各具特色。我们依然以中、欧、美、新、日、韩为样本，简要整理其保护敏感个人信息的原则与具体措施，并在文末以表格形式汇总对比(见文末表 3)。

1. 欧盟

欧盟 GDPR¹⁰原则上禁止企业或组织¹¹处理敏感个人信息，除非满足以下 10 种特定条件之一：

- 处理敏感个人信息已获得个人的明确同意的(某些情况下，法律可能会排除这种选择)；
- 欧盟法律、国家法律或集体协议要求企业或组织处理敏感个人信息，从而遵守其及个人在就业、社会保障和社会保护法领域的义务和权利的；
- 该敏感个人信息主体或在身体或法律上无能力给予同意的个人的重要利益受到威胁的；
- 作为基金会、协会或其他以政治、哲学、宗教或工会为目的的非营利机构，正在处理其成员或与该组织有经常联系的人的敏感个人信息的；
- 显然由个人自行公开其敏感个人信息的；
- 为确立、行使或辩护法律索赔请求而需要处理敏感个人信息的；
- 根据欧盟或国家法律，出于重大公共利益而需要处理敏感个人信息的；
- 根据欧盟或国家法律，或根据卫生专业人员合同，出于预防或职业医学、员工工作能力评估、医疗诊断、提供卫生或社会保健或治疗、或管理卫生或社会保健系统和服务的目的而需要处理敏感个人信息的；
- 根据欧盟或国家法律，出于公共卫生领域的公共利益原因而需要处理敏感个人信息的；
- 根据欧盟或国家法律，出于存档、科学、历史研究目的或统计目的而需要处理敏感个人信息的。

其中，GDPR 还要求企业对基因、生物特征或健康相关敏感个人信息的处理予以更高级别保护，应当由负有法定职业保密义务的人员为某些与健康有关的目的而进行。部分欧盟成员国法律也对此作进一步限制，例如《荷兰 GDPR 实施法(UAVG)》特别允许出于有限的身份验证和安全目的的处理生物识别信息。

¹⁰ 参考 GDPR Article 9 以及 Recitals 51–56.

¹¹ 为便于理解，下文暂以“企业”统一指代类似细分概念，如企业/组织、个人信息处理者/控制者等。

此外，如企业或组织的核心活动涉及大规模处理敏感个人信息的，GDPR 还要求其指定一名数据保护官(DPO)。

2. 美国

如上文所述，由于美国联邦与各州分散立法，且尚未正式出台涉及敏感个人信息保护的联邦法律，美国目前在敏感个人信息保护方面仍呈现地区性差异：

- 美国大多数设有综合性隐私法律的州¹²倾向对敏感个人信息保护采取严格的授权同意模式——企业收集、使用和披露特定类型敏感个人信息(如健康信息、信用财务信息、儿童个人信息、生物识别信息、视频观看偏好信息、地理位置及电信使用情况等)，除需事先以隐私政策等形式向个人披露其收集、使用和披露方式，个人对其个人信息拥有的选择权以及企业的联系信息外，还必须事先获得个人明确的“加入同意(Opt-in Consent)”；
- 加利福尼亚州¹³要求企业向消费者提供限制使用、披露其敏感个人信息的权利；
- 爱荷华州¹⁴和犹他州¹⁵要求企业向消费者提供明确通知以及“拒绝(Opt-out)”处理其敏感个人信息的权利；
- 弗吉尼亚州¹⁶则要求企业在处理敏感个人信息前应进行“数据保护评估(Data protection assessment)”。

3. 新加坡

新加坡《个人数据保护法(PDPA)》虽建立了一般数据保护法律框架，但并未区分敏感个人信息与非敏感个人信息。而实践中¹⁷，新加坡主要通过其个人数据保护委员会(“PDPC”)发布的执法决定与专项指南承认并保护敏感个人信息：

- PDPC 曾在执法决定¹⁸中表示应采取更高标准保护身份证件号码、银行账户、存款信息与交易记录、医疗信息等敏感个人信息；
- PDPC 在其《数据保护条款执法指南(Advisory Guidelines on Enforcement of Data Protection Provisions)》中提出，处理大量敏感个人信息的组织应采取与数据泄露可能造成损害相称的充分保护措施，否则可将此视为罚款的加重情节。

4. 日本

与欧盟模式类似，日本《个人信息保护法(個人情報保護法/APPI)》也在原则上禁止企业获取敏感个人信息，除非符合 9 种例外情形之一，例如出于委托或业务继承原因等。

¹² 除加利福尼亚州、佛罗里达州、爱荷华州和犹他州外。

¹³ CA Civ Code § 1798.121

¹⁴ Iowa Code § 715D.4

¹⁵ Utah Code § 13-61-302

¹⁶ Va. Code Ann. § 59.1-580

¹⁷ In Re Aviva Ltd [2017] SGPDPC 14

¹⁸ 例如，Aviva Ltd [2018] SGPDPC 4, In Re Aviva Ltd [2017] SGPDPC 14 等。

需注意的是, APPI 虽允许对一般个人信息适用“选择退出程序 (オプトアウト方式)”(如图 1 所示意), 但禁止企业通过该程序向第三方提供敏感个人信息。

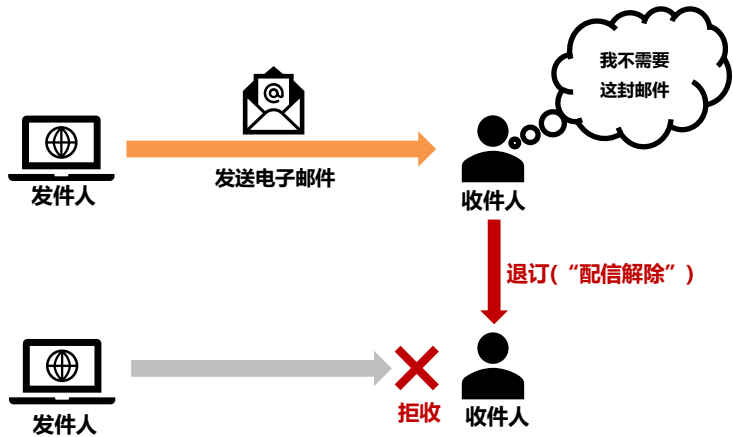


图 1 日本一般个人信息所适用的“选择退出程序 (オプトアウト方式)”

此外, APPI 还要求行政机关履行通报义务¹⁹——行政机关在持有包含敏感个人信息的文件之前, 必须向个人信息保护委员会通报具体情况。

5. 韩国

韩国《个人信息保护法(PIPA)》原则上禁止企业处理敏感个人信息, 除非其已告知个人有关处理其敏感个人信息的特定内容, 并获得该个人对处理敏感个人信息的单独同意。

此外, 企业还应当采取以下保护措施:

- 采取必要的技术、管理和物理措施, 如制定内部管理计划、保存访问记录等。
- 如认为在提供商品或服务过程中披露的信息含有可能隐私侵犯风险的敏感个人信息, 应事先以便于理解的方式告知个人可能披露的情况与其选择不披露的方式。

国家地区	原则上是否允许处理	处理的前提条件/例外情形	额外要求的保护措施 ²⁰
欧盟	否	需符合 GDPR 所规定 10 种例外情形之一。 ➢ 例如, 取得个人 <u>明确的同意</u> 、出于重大公共利益所必需等。	成员国法律可能对 <u>遗传、生物识别或健康相关敏感个人信息</u> 的处理作进一步限制。 ➢ 例如, 《荷兰 GDPR 实施法(UAVG)》特别允许出于有限的身份验证和安全目的处理生物识别信息。
美国	是	需遵守联邦(如有)及各州法律具体规定。	各州法律可能对敏感个人信息的处理作特殊要求:

¹⁹ Article 74, Act on the Protection of Personal Information(個人情報保護法)

²⁰ 即, 敏感个人信息相较一般个人信息保护措施所额外需要的特别措施。

		➢ 例如, 需事先取得个人 <u>明确的“加入同意 (Opt-in Consent)”</u> , 或赋予个人 <u>限制/拒绝权</u> 等。	➢ 例如, 弗吉尼亚州《消费者数据保护法案(CDPA)》还要求企业事先开展“数据保护评估(Data Protection Assessment)”。
新加坡	是	未在法律层面区分“敏感”与“一般”个人信息, 遵守《个人数据保护法(PDPA)》即可处理。	需给予敏感个人信息更高级别的保护, 并实施与其敏感性相适应的保护措施(<u>结合个案场景判断</u>)。 ➢ 例如, 邮寄私人函件应配备标准作业程序(SOP)及安保措施。
日本	否	需事先取得个人 <u>明确的同意</u> 。 ➢ 除非符合《个人信息保护法(個人情報保護法/APPI)》所规定 9 种例外情形之一, 如出于委托或业务继承原因等。	1) 禁止企业以 <u>“选择退出程序 (オプトアウト方式)”</u> 向第三方提供敏感个人信息。 2) 行政机关持有包含敏感个人信息文件前, 需通报个人信息保护委员会。
韩国	否	需事先 <u>告知</u> 个人有关处理其敏感个人信息的特定内容, 并获得个人对该处理的 <u>单独同意</u> 。	如企业认为在提供商品或服务过程中披露的信息含有可能隐私侵犯风险的敏感个人信息的, 还应事先以便于理解方式 <u>告知</u> 个人可能披露的情况与其选择不披露的方式。

表 3 域外敏感个人信息保护模式对比(以中国、欧盟、美国、新加坡、日本、韩国为样本)

如您希望就相关问题进一步交流，请联系：



潘永建
+86 21 3135 8701
david.pan@llinkslaw.com



朱晓阳
+86 21 3135 8683
nigel.zhu@llinkslaw.com

如您希望就其他问题进一步交流或有其他业务咨询需求，请随时与我们联系: master@llinkslaw.com

上海

上海市银城中路 68 号
时代金融中心 19 楼
T: +86 21 3135 8666
F: +86 21 3135 8600

北京

北京市朝阳区光华东里 8 号
中海广场中楼 30 层
T: +86 10 5081 3888
F: +86 10 5081 3866

深圳

深圳市南山区科苑南路 2666 号
中国华润大厦 18 楼
T: +86 755 3391 7666
F: +86 755 3391 7668

香港

香港中环遮打道 18 号
历山大厦 32 楼 3201 室
T: +852 2592 1978
F: +852 2868 0883

伦敦

1/F, 3 More London Riverside
London SE1 2RE
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

本土化资源 国际化视野

免责声明:

本出版物仅供一般性参考，并无意提供任何法律或其他建议。我们明示不对任何依赖本出版物的任何内容而采取或不采取行动所导致的后果承担责任。我们保留所有对本出版物的权利。

© 通力律师事务所 2024