# 外国におけるセンシティブデータの取扱いに関する制度等の調査結果報告書

2023年3月

ベーカー&マッケンジー法律事務所（外国法共同事業）

目次

## 第1章.　総論

### I.　調査体制

本調査では、ベーカー&マッケンジー法律事務所弁護士法人及び同弁護士法人からの再委託先となるベーカー&マッケンジー法律事務所（外国法共同事業）及び調査対象国・地域に所在するその拠点（当該調査対象国・地域に拠点がない場合にはその提携先法律事務所）が連携して、所定の質問票に現地から回答を得る形で各国・地域における制度調査を行い、現地専門家からの回答に基づき、さらにベーカー&マッケンジー法律事務所（外国法共同事業）所属弁護士がオンラインでの調査を実施することにより、本報告書を作成した。

### II.　調査期間

2022 年 12 月より 2023 年 3 月 31 日までの期間、本調査を実施した。

### III.　基準日

回答は、2023 年 1 月 1 日時点で有効な法令を前提としている。ただし、2023 年 1 月 1 日の時点で未だ施行されていないものの、同日時点で成立済みの法令がある場合には、当該法令に関する情報も回答に併記している。なお、米国（連邦）については、2023 年 1 月 1 日の時点の法令案のうち、アメリカデータプライバシー及び保護法（American Data Privacy and Protection Act）を主な調査対象として回答している。

### IV.　調査対象国・地域一覧

本調査の対象となる国・地域は以下のとおりである。

| | | |
|---|---|---|
| 1.EU（欧州連合） | 2.米国（アメリカ合衆国）（連邦・アメリカデータプライバシー及び保護法） | 3.米国（アメリカ合衆国）（カリフォルニア州） |
| 4.中国（中華人民共和国） | 5.インド | 6.ブラジル（ブラジル連邦共和国） |
| 7.オーストラリア（オーストラリア連邦） | 8.韓国（大韓民国） | |

### V.　調査事項

1.　総論

個人情報の保護に関する法令について、包括的な個人情報保護法令がある国・地域の場合には当該法令、そうではない国・地域の場合には、現地専門家の見解に基づき選定された個人情報の保護に関する個別的な法令のうち代表的な法令（以下総称して「本件法令等」という。）を取り上げている。また、本件法令等におけるセンシティブデータに係る規律の趣旨を記載している。

2. センシティブデータの範囲―総論

本件法令等においていかなるデータがセンシティブデータとして指定されているかを示すとともに、センシティブデータを推知させる情報のセンシティブデータの該当性を示している。

3. センシティブデータの範囲―各論

11 の具体的なデータ類型別に、センシティブデータへの該当性やその該非に関する本件法令等の定めの趣旨、追加的規律が存在する場合には当該規律について記載している。このうち健康に関するデータ、遺伝子に関するデータについては、更に細分化した項目毎の該当性を記載している。

4. センシティブデータの取扱いに係る規律（センシティブデータの種類を問わず適用されるもの）

センシティブデータの取扱いに係る規律として、一般的な個人データについて適用される規律とは異なる特有の規律が存在する場合には、センシティブデータの各取扱い（取得、利用、第三者提供、管理、漏えい等、データ主体の権利）に関する規律を記載している。センシティブデータの取扱いに特有の規律が存在しない場合には、その旨及び一般的な個人データについて適用される規律を記載し、規律以外の留意点等があれば該当する事項について記載している。

5. 本人同意、プロファイリング

センシティブデータの取扱いに関連する規律として、本人同意の取得に係る規律、プロファイリング・データ分析に係る規律を記載している。具体的に、本人同意については、センシティブデータの処理にあたって本人同意を得る必要があるか、本人同意の取得に関する要件一般、本人同意を得るにあたって本人に提供する必要がある情報、同意取得の形式、個別同意の必要性（取扱いの目的に応じた個別の同意取得の要否）、同意の撤回の可否について記載している。プロファイリング・データ分析については、プロファイリング・データ分析に適用される規律、プロファイリング・データ分析により生成されるデータのセンシティブデータへの該当性、プロファイリング・データ分析によりセンシティブデータを生成した場合に適用される規律について記載している。

6. センシティブデータの取扱いに係る裁判例・決定等

センシティブデータの取扱いをめぐる各法域における政府・裁判所・データ保護機関が下した決定・処分について、現地専門家から該当する事項として回答のあった事案のうち、本調査の趣旨を踏まえ参考になると考えられる事案の概要を記載している。

## 7. その他

1.総論で取り上げた本件法令等以外に、個人情報の保護に関連する法令として現地専門家により回答のあった法令について記載している。

## 第2章.　EU

### I.　総論

#### 1.　個人情報の保護に関する法令等

個人情報の保護に関する包括的な法令として、個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の（EU）規則 2016/679（一般データ保護規則）（Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC。以下「GDPR」という。）[1]が存在する。GDPR は、公的部門、民間部門の両部門が対象となるが、欧州連合基本条約第 5 章第 2 節（共通外交・安全保障政策）の範囲に含まれる活動、及び公共の安全に対する脅威の保護及び防止を含め、刑事犯罪の防止、捜査、探知若しくは訴追、又は刑事罰の執行を目的とする所轄官庁による活動には適用されない（GDPR 第 2 条（b）及び（d））。

なお、欧州連合の機関、団体、事務所及び当局は、GDPR の対象ではないものの、Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC（以下「規則 2018/1725」という。下記 VII.参照）[2]の対象となる（GDPR 第 2 条第 3 項）。また、指令（directive）は、法律として効力を有するためには EU 加盟国（以下、単に「加盟国」という場合がある。）の国内法に組み込まれる必要がある[3]ものの、公共の安全に対する脅威の保護及び防止を含む、刑事犯罪の防止、捜査、探知又は訴追、又は刑事罰の執行を目的とした、所轄官庁による個人データの処理を対象とする法令として Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA（以下「法施行指令」という。）[4]が存在する（下記 VII.参照）。

このほか、センシティブデータの規律に関連する指令として、Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector（以下「e プライバシー指令」という。）が存在する。この e プライバシー指令も、指令（directive）という法形式をとっているため、法律として効力を有するためには加盟国の国内法に組み込まれる必要がある。本調査においては、GDPR を主に対象として回答を行っており、設問上、追加的あるいは関連する規律が存在する場合、必要に応じて GDPR 以外の法令の規律に言及している。

#### 2.　センシティブデータの取扱いに対する規制の趣旨

##### (1)　GDPR

センシティブデータは、GDPR では「特別な種類のデータ」（special categories of personal data）として規定されており、その性質上、基本的な権利と自由に関連して特にセンシティブであり、その処理の過程で基本的権利と自由に対する重大なリスクが生じ得るため、特別な保護に値する個人データとされている（GDPR 前文第 51 項）。

---

[1] https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725
[3] https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504

欧州データ保護委員会（EDPB）の前身である第 29 条作業部会は、特別な種類のデータに関する勧告文書（Advice paper on special categories of data）[5]で以下のとおり示している。

> 「特定の種類のデータを異なる方法で規制する根拠は、これらのデータの誤用が、他の『通常の」個人データの誤用よりも、プライバシー権や差別を受けない権利等、個人の基本的権利に深刻な結果をもたらす可能性があると推定されるからである。健康データ又は性的指向のようなセンシティブデータの悪用は（例えば、公にされた場合）、不可逆的であり、本人だけでなくその社会環境にも長期的な影響を与える可能性がある。このため、条約及び指令は、その性質上センシティブとみなされるデータの処理を、他の個人データの処理に関する条件より厚い、一定の保護措置及び条件によって行うことを義務付けている。」（4-5 頁）

(2) e プライバシー指令

センシティブデータ又は GDPR 上の「特別な種類のデータ」の概念とは異なるが、e プライバシー指令は、電子通信の過程で収集されたトラフィックデータ及び位置データの処理の過程を規制するものである。

e プライバシー指令の前文第 26 項によると、このような規制を設ける理由は、「接続を確立し情報を送信するために電子通信ネットワーク内で処理される加入者に関するデータは、自然人の私生活に関する情報を含み、通信を尊重する権利に関わり、法人の合法的利益に関わる」ためである。

## II. センシティブデータの範囲―総論

センシティブデータに該当するのは、個人データのうちの特別な種類の個人データ等として規定されている次のデータである（GDPR 第 9 条第 1 項、同第 10 条、規則 2018/1725 第 10 条、同第 11 条、法施行指令第 10 条）。

- 以下のいずれかに該当する個人データ
  - 人種又は民族的出自
  - 政治的意見
  - 宗教的又は哲学的な信条
  - 労働組合への加盟
- 遺伝子データ
  - 自然人の先天的又は後天的な遺伝的特性に関する個人データであって、当該自然人の生理学又は健康に関する固有の情報を与え、かつ、特に当該自然人からの生体サンプルの分析から生じるもの（GDPR 第 4 条第 13 項、規則 2018/1725 第 3 条第 17 項、法施行指令第 3 条第 12 項）。
- 自然人を一意的に識別するための生体データ
  - 自然人の身体的、生理的又は行動的特徴に関連する特定の技術的処理の結果生じた個人データであって、顔画像又は指紋データ等、当該自然人の固有の識別を可能にし又は当該自然人を確認するもの（GDPR 第 4 条第 14 項、規則 2018/1725 第 3 条第 18 項、法施行指令第 3 条第 13 項）。但し、これは「生体データ」の定義であり、このうち「自然人を一意的に識別するための」ものがセンシティブデータに該当する（GDPR 第 9 条第 1 項、規則 2018/1725 第 10 条、法施行指令第 10 条）。
- 健康に関するデータ

[5] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf

- ヘルスケアサービスの提供を含む、自然人の身体的又は精神的健康に関連する個人データで、その健康状態に関する情報を明らかにするもの（GDPR 第 4 条 15 項、規則 2018/1725 第 3 条第 19 項、法施行指令第 3 条第 14 項）。
- 自然人の性生活又は性的指向に関するデータ
- 前科及び犯罪に関する個人データ（GDPR 第 10 条、規則 2018/1725 第 11 条）

また、e プライバシー指令では、センシティブデータとして規定されているわけではないものの、次のデータが特定の保護を受けるデータとして定められている。

- トラフィックデータ
  - 電子通信ネットワーク上での通信の伝達又はその課金を目的として処理されるあらゆるデータ（e プライバシー指令第 2 条（b））。
- 位置データ
  - 電子通信ネットワーク又は電子通信サービスにおいて処理される、公衆利用可能な電子通信サービスの利用者の端末機器の地理的位置を示すあらゆるデータ（e プライバシー指令第 2 条（c））。

1. センシティブデータの範囲一覧

当局の公表している主要な資料において、現時点でセンシティブデータ全般及び特定の種類のセンシティブデータに関するガイダンス文書として公表されたものは特に見当たらない。もっとも、関連する資料として、特定の文脈におけるセンシティブデータの処理に関する次のようなガイダンスが EDPB より公表されている。EDPB は、欧州連合全体におけるデータ保護法令の一貫した適用に貢献し、EU のデータ保護当局間の協力を推進する欧州の独立した機関であり、EU 加盟国のデータ保護当局、欧州委員会及び欧州データ保護観察機関（EDPS）の代表者によって構成される。その任務には、手続きに関するガイドライン、勧告及びベストプラクティスの公表が含まれる。EDPB のガイダンスは、特に全加盟国のデータ保護当局の意見を代表していることから、個人情報の保護に関する分野では権威あるものとみなされている。

- 法執行領域における顔認識技術の利用に関するガイドライン：05/2022[6]
- 仮想音声アシスタントに関するガイドライン：02/2021[7]
- ソーシャルメディアユーザーのターゲティングに関するガイドライン：08/2020[8]
- コネクテッドビークル及びモビリティ関連アプリケーションにおける個人データの処理に関するガイドライン：01/2020[9]
- ビデオデバイスを通じた個人データの処理に関するガイドライン：03/2019[10]
- 規則 2016/679 に基づく同意に関するガイドライン：05/2020[11]
- COVID-19 の発生に関連した科学的研究を目的とした健康に関するデータの処理に関するガイドライン：03/2020[12]

[6] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en
[7] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en
[8] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-82020-targeting-social-media-users_en
[9] https://edpb.europa.eu/system/files/2021-03/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf
[10] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf
[11] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en
[12] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

さらに、EDPB の前身である第 29 条作業部会は、以下の関連する権威あるガイドラインを採択している（第 29 条作業部会のガイドラインは、同会が EDPB の前身であることから EDPB のガイドラインと同様の理由で権威があるものと一般に解されている）。

- 規則 2016/679 の目的のための自動化された個人の意思決定及びプロファイリングに関するガイドライン[13]
- 特別な種類のデータ（「センシティブデータ」）に関するアドバイスペーパー[14]
- 電子健康記録（EHR）における健康に関連する個人データの処理に関するワーキングドキュメント[15]

また、EU の公的機関及び団体が行うデータ処理に関する監督官庁である EDPS が公表した以下の文書によっても、いくつかの有用かつ権威あるガイダンスが示されている。

- EDPS からのオリエンテーション：COVID-19 危機における EU 機関による体温測定について[16]

その他の資料として、欧州連合基本権機関の「欧州データ保護法ハンドブック」（2018 年）[17]にも追加のガイダンスが掲載されている。

なお、一般的に、学者、専門家及び実務家が発表する文書は、EDPB の公表するガイドラインよりも影響力が弱い傾向にあるが、一例としては以下の文書が挙げられる。

- オーラ・リンスキー『EU データ保護法の基礎』オックスフォード大学出版局、2015 年
- ヨス・デュモルティエ、ピーテル・グリフロイ、ルーベン・ロエックス、ユン・シン・ヴァン・デル・サイプ『プライバシーとテクノロジー法』ウォルターズ・クルワー、2022 年
- ポール・クイン、ジャンクラウディオ・マルジェリ「センシティブデータの定義の難しさ-EU データ保護フレームワークにおけるセンシティブデータの概念」ドイツ法研究、2021、22（8）、1583-1612

2. センシティブデータを推知させる情報（推知情報）について

特定の状況下では、センシティブデータを推知できる情報は、センシティブデータに該当すると解される。

まず GDPR 第 9 条第 1 項は、人種又は民族的出自、政治的意見、宗教的又は哲学的信条、労働組合への加入について、それらを明らかにする（reveal）個人データが、センシティブデータとなる旨を規定しており、推知の程度が「明らかにする」に相当するような場合には、その文言の解釈として、人種又は民族的出自、政治的意見、宗教的又は哲学的信条、労働組合への加入を明らかにする情報もセンシティブデータに該当すると解することができる。

[13] https://ec.europa.eu/newsroom/article29/items/612053
[14] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf
[15] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf
[16] https://edps.europa.eu/sites/default/files/publication/01-09-20_edps_orientations_on_body_temperature_checks_in_the_context_of_euis_en.pdf
[17] https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf

また、GDPR 前文第 35 項は、健康に関するデータに関して、健康に関する個人データには、本人の過去、現在または将来の身体的または精神的健康状態に関連する情報を明らかにする、本人の健康状態に関連するすべてのデータが含まれるとしている。また、そのような情報の具体例として、「遺伝子データ及び生物学的サンプルを含む、身体の一部又は身体物質の検査又は調査から得られる情報（...）が含まれる」としている。

さらに、EDPB の複数のガイドライン及び欧州司法裁判所の判例は、データ主体についてセンシティブなデータが推測され得るデータが、GDPR 第 9 条の意味における「特別な種類のデータ」に該当する可能性があることを次の通り確認している。

(3) ソーシャルメディアユーザーのターゲティングに関するガイドライン：8/2020

- 「121. 特別な種類のデータに関する仮定又は推知、例えばリベラルな意見を説くページを訪問した後にある政党に投票する可能性が高いといった情報も、特別な種類の個人データに該当する。」
- 「122. 例えば、ある宗教的信条を持つ人々がよく訪れる場所をユーザーが（一度又は数回）訪問したことを明らかにする単なる記述又は単一の位置データ若しくはそれに類するものの処理自体は、一般に特別な種類のデータの処理とはみなされない。ただし、これらのデータが他のデータと組み合わされる場合、又はデータが処理される脈絡若しくは利用される目的によっては、特別な種類のデータの処理とみなされる可能性がある。」
- 「例 11：ノヴァク氏のソーシャルメディアアカウントのプロフィールには、氏名や居住地といった一般的な情報しか記載されていないが、近況についてのアップデートから、彼が頻繁に教会を訪れ、宗教礼拝に出席していることが判明した。また、これより後に、教会が訪問者に対しキリスト教信者の入会を促すため宗教的なメッセージのターゲットにしようと考えたとする。このような状況において、ターゲティング目的のために、ノヴァク氏の近況アップデートに含まれる個人データを使用することは、特別な種類の個人データの処理に相当する。」
- 「123. ソーシャルメディアプロバイダ又はターゲター（targeter）が、観測されたデータを利用してユーザーを特定の宗教的、哲学的又は政治的信念を持っていると分類する場合、その分類が正しいか否かにかかわらず、このユーザーの分類は、この文脈では明らかに特別な種類の個人データの処理とみなされなければならない。カテゴライズによって特別な種類のデータに基づくターゲティングが可能になる限り、そのカテゴリーがどのようにラベル付けされているかは問題ではない。」

(4) 第 29 条作業部会、規則 2016/679 の目的のための自動化された個人の意思決定及びプロファイリングに関するガイドライン

このガイドラインは、プロファイリングによりセンシティブデータに該当するデータが作成されうることを指摘している。その内容については、下記 V2(2)参照。

(5) COVID-19 の発生に関連した科学的研究を目的とした健康に関するデータの処理に関するガイドライン

このガイドラインは次のように記載し、様々な情報源から派生した情報がセンシティブデータに該当しうることを述べている。

「8. 健康に関するデータは、次の例のように、様々な情報源から派生して生じることがある。

…

4. 特定の文脈で使用されることにより健康データとなる情報（例えば、COVID-19 の感染地域への最近の旅行又は滞在に関する情報を医療従事者が診断するために処理したもの）。」

(6) コネクテッドビークル及びモビリティ関連アプリケーションにおける個人データの処理に関するガイドライン

「63. 自動車及び機器の製造者、サービスプロバイダー及びその他のデータ管理者は、個人データを収集する際、位置データがとりわけデータ主体の生活習慣を明らかにすることを念頭に置くべきである。移動は、職場及び居住地、並びに運転者の関心のある分野（レジャー）を推知することができるという点で非常に特徴的であり、礼拝所を通じて宗教、又は訪問先を通じて性的指向等のセンシティブな情報が明らかになる可能性がある。」

当該記載は、センシティブなデータを推測させ得るデータも、GDPR 第 9 条の「特別な種類のデータ」に該当する可能性があることを示唆する記載と考えられる。

(7) ビデオデバイスを通じた個人データの処理に関するガイドライン

「62. ビデオ監視システムは、通常、大量の個人データを収集し、これにより、高度に個人的な性質のデータ及び特別な種類のデータさえも明らかにすることができる。実際、もともとビデオで収集された一見すると重要でないデータが、別の目的を達成するために他の情報を推知するために利用されることがある（例えば、個人の習慣をマッピングするため等）。しかし、ビデオ監視は、必ずしも特別な種類の個人データの処理とはみなされない。」

「64. ただし、ビデオ映像が特別な種類のデータを推論するために処理される場合は、第 9 条が適用される。」

(8) 2022 年 8 月 1 日欧州司法裁判所（CJEU）判決、Case C-184/20 （ECLI:EU:C:2022:601）[18]

この事件は、EU 加盟国であるリトアニアの汚職防止法が、公的資金を受け取った人の利益申告書をオンラインで公表することを義務付けていたことに関連する。これらの申告には、申告者及びその配偶者、同居人、パートナーの氏名が含まれていた。欧州司法裁判所は、自然人の性生活又は性的指向を間接的に開示する可能性のあるこのようなデータの公表が、特別な個人データの処理（GDPR 第 9 条）に該当するか否かについて判決を下す必要があった。このため、欧州司法裁判所は、比較又は推論を含む知的操作によって自然人の性的指向を明らかにすることができるデータが、特別な種類の個人データに該当するか否かを判断した（第 120 段落）。欧州司法裁判所は、「特別な種類のデータ」及び「センシティブデータ」という用語の広範な解釈を採用し、「自然人の性的指向を間接的に開示する可能性のある個人データの公表」は、GDPR 第 9 条にいう「特別な種類の個人データの処理に該当する」と判断した（第 125 段落及び 128 段落）。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

[18] https://curia.europa.eu/juris/document/document.jsf;jsessionid=E6494702AD1E00A0D3CA8273080E0F28?text=&docid=263721&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1403330

健康に関するデータは、センシティブデータに該当する（GDPR 第 9 条第 1 項、同第 4 条第 15 号）。GDPR 第 4 条第 15 号は、健康に関するデータを、「ヘルスケアサービスの提供を含む、自然人の身体的又は精神的健康に関連する個人データであって、当該自然人の健康状態に関する情報を明らかにするものをいう」と定義する。

「健康に関するデータ」の概念は、欧州司法裁判所によって「個人の健康に関する身体的及び精神的な全ての側面に関する情報を含む」とされ、広く解釈されている（2003 年 11 月 6 日欧州司法裁判所（CJEU）判決、Case C-101/01 （ECLI:EU:C:2003:596）（リンドクヴィスト判決）[19]、 第 50 段落）。

(i)　医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する（GDPR 前文第 35 項、第 4 条 15 項）。GDPR 前文第 35 項は、以下のように規定する。

> 「健康に関する個人データには、データ主体の過去、現在又は将来の身体的又は精神的健康状態に関連する情報を明らかにする、データ主体の健康状態に関連する全てのデータを記載する必要がある。これには、欧州議会及び理事会指令 2011/24/EU （1）で言及されているヘルスケアサービスの登録又はその提供の過程で収集された自然人に関する情報、健康目的のために自然人を一意に識別するために自然人に割り当てられた番号、記号又は特定事項、及び遺伝子データ及び生体試料を含む、身体の一部又は身体物質の検査又は検討から得られた情報、例えば、医師その他の健康に関する専門家、病院、医療機器、体外診断用検査等、情報源とは無関係なデータ主体の疾患、障害、疾患リスク、病歴、臨床治療、生理学又は生物医学的状態に関するあらゆる情報が含まれる。」

一般に、本設問のような検査結果は、自然人の身体的又は精神的健康状態に関連し、これを明らかにすることから、健康に関するデータ（GDPR 第 4 条第 15 項）に該当すると解され、その処理については GDPR が適用される。

(ii)　事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果は、センシティブデータに該当する。

個人データが GDPR 第 4 条 15 項の意味における「健康に関するデータ」に該当するためには、その定義上、医師等によって実施された検査の結果であることは要件とされておらず、そのため、医師等のような特定のデータ管理者によって収集される必要はない。問題となる個人データが「健康に関するデータ」の定義を満たす限り、当該データを収集した管理者に関係なく、健康に関するデータに該当する。

(iii)　消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果がセンシティブデータに該当する。

個人データが GDPR 第 4 条 15 項の意味における「健康に関するデータ」に該当するためには、その定義上、医師等によって実施された検査の結果であることは要件とされておらず、そのため、医師等のような特定のデータ管理者によって収集される必要はない。問題となる個人データが「健康に関するデータ」の定義を満たす限り、当該データを収集した管理者に関係なく、健康に関するデータに該当する。

(iv)　消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する。

個人データが GDPR 第 4 条第 15 項の意味における「健康に関するデータ」に該当するためには、その定義上、医師等によって実施された検査の結果であることは要件とされておらず、そのため、医師等のような特定のデータ管理者によって収集される必要はない。問題となる個人データが「健康に関するデ

[19] https://curia.europa.eu/juris/liste.jsf?num=C-101/01

ータ」の定義を満たす限り、当該データを収集した管理者に関係なく、健康に関するデータに該当する。

なお、EDPB は、COVID-19 の発生に関連した科学的研究を目的とした健康に関するデータの処理に関するガイドラインにおいて、健康に関するデータを得られる可能性がある具体例として以下の例を挙げており、医療従事者の判断や市販の検査機器を使わずに消費者が自分で判断した健康状態も、健康に関するデータとして認められる可能性があることを示している。

> 「8. 健康に関するデータは、例えば、次のような様々な情報源から得られることがありうる。例：（…）3.データ主体が健康に関する質問に（症状を述べる等により）答える「セルフチェック」調査からの情報。」

(v) 予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか)

予防接種の有無関する情報は、健康に関するデータとして、センシティブデータに該当する。

疾病、障害、病歴および臨床治療に関連するあらゆる情報は一律に健康に関するデータとみなされ（2015 年 2 月 5 日付、第 29 条作業部会議長、欧州委員会あて書簡[20]及びその別紙[21]）、予防接種に関する情報もそれらに「関連するあらゆる情報」の範疇に含まれることを明記する資料は本件調査の限りでは見当たらないがその解釈としてこれに含まれることを否定すべき事情もないため、データ主体の種類やその他の条件にかかわらず「健康に関する情報」に該当することとなると解される。

(2) 趣旨

健康に関する個人データは、その性質上、基本的な権利及び自由との関係で特にセンシティブであると考えられ、従って、その処理の過程が基本的な権利及び自由に対して重大なリスクを作成する可能性があるため、特別の保護に値するとされている（GDPR 前文第 51 項）。

第 29 条作業部会は、特別な種類のデータ（「センシティブデータ」）に関するアドバイスペーパー[22]において、「深刻なプライバシー侵害に関連する処理を行う健康データを、濫用（患者データの商業利用等）から保護するために、特別な措置が必要である。」（10 頁）という点を明確にしている。

(3) 追加的規律（該当する場合）

一点目として、GDPR は、加盟国が健康に関するデータの処理に関して、制限を含むさらなる条件を維持又は導入することを認めている（GDPR 第 9 条第 4 項）。

したがって、健康に関するデータに適用される追加の規定は、GDPR を施行する EU 加盟国の国内法において規定されている可能性がある[23]。

---

[20] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf
[21] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf
[22] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2011/2011_04_20_letter_artwp_mme_le_bail_directive_9546ec_annex1_en.pdf
[23] 例えば、ベルギーでは、2018 年 7 月 30 日法律第 9 条は、次のように GDPR 第 9 条 4 項を施行している：
「第 9 条 規則[GDPR]の第 9 条 4 項の施行において、遺伝子データ、生体情報データ又は健康に関するデータを処理する管理者は、以下の追加措置も講じるものとする。
1°管理者又は必要のある処理者は、個人データにアクセスできる者の種類を指定し、当該データの処理に関してその能力を詳細に説明しなければならない。2°管理者又は必要のある処理者は、そのように指定された種類の人物のリストを管轄

二点目として、GDPR 第 88 条「雇用の過程における処理」に基づき、EU 加盟国は、法律又は労働協約により、特に、採用、法律又は労働協約により定められた義務の履行を含む雇用契約の履行、労働の管理、計画及び組織、職場における平等及び多様性、労働における健康及び安全、雇用者又は顧客の財産の保護並びに雇用に関連する権利及び利益の個人的又は集団的な行使及び享受並びに雇用関係の終了のために、雇用の過程における従業員の個人データの処理に関する権利及び自由の保護を確保するためのより具体的な規律を定めることができるとされている。

したがって、雇用における健康に関する従業員のデータの処理に適用される特定の規律（例えば、健康診断、薬物検査等に関する特定の規律）については、EU 加盟国の国内法を参照する必要がある。

三点目として、健康に関するデータは、幅広い法令の影響を受ける可能性がある。以下はその一例である。ただし、これらの法令は健康に関するデータの処理について必ずしも明確に規定しているわけではないことに留意が必要である。

- 障害（Disability）（GDPR 前文第 35 項の定める通り健康に関するデータにも該当する。）は、EU 基本権憲章第 21 条[24]で次のように定められており、禁止されている差別事由の一つになる。

  「性別、人種、肌の色、民族的又は社会的出自、遺伝的特徴、言語、宗教又は信念、政治的又はその他の意見、国内少数派の一員、財産、出生、障害、年齢、性的指向等のあらゆる理由に基づく差別は禁止される。」

- 2000 年 11 月 27 日付「雇用と職業における平等な待遇のための一般的枠組みを確立する理事会指令」（2000/78/EC）[25]では、雇用と職業に関する差別の禁止事由として、障害を挙げている。

- 2016 年 7 月 6 日付「EU 全域のネットワーク及び情報システムのセキュリティに共通する高いレベルの措置に関する指令」（2016/1148）[26]（以下、「NIS 指令」という。）では、加盟国は、病院、私立診療所、その他の医療現場等の必須サービス（指令 4 条 4 項）の運営者に対して、加盟国法でセキュリティ要件とインシデント通知要件を課す必要がある（指令附属書 II）。なお、NIS 指令は、2023 年 1 月 16 日に発効する「規則 No 910/2014 および指令 2018/1972 を改正し、指令 2016/1148 を廃止する EU 全域のサイバーセキュリティに共通する高いレベルの措置に関する指令（NIS 2 指令）」（以下、「NIS 2 指令」という。）（2022/2555）[27]により、2024 年 10 月 18 日の廃止が予定されている。NIS 2 指令は、NIS 指令の対象よりもセキュリティ要件を強化し、より広範な事業者・部門にこれを課している。

- 2022 年 12 月 14 日付欧州議会及び欧州理事会指令（2022/2557）[28]は、重要事業者の耐障害性に関するもので、Council Directive 2008/114/EC を廃止し、2023 年 1 月 16 日に発効する予定である。本指令によると、加盟国は、医療機関、EU 基準研究所、医薬品の研究開発活動を行う事業者、基礎医薬品・製剤の製造業者、公衆衛生上の緊急時に重要と考えられる医療機器の製造業者、医薬品流通事業者等の重要事業者（指令付属書）につき、以下を確保する必要がある。
  - リスクアセスメントの実施
  - 技術的、セキュリティ的、組織的に適切な対策を講じた耐障害性の確保
  - 重要なサービスの提供を著しく妨げるような事象の通知

---

の監督当局が自由に利用できるように保管するものとする。3°管理者は、指定された人物が法的義務又は同等の契約上の規定により、当該データの機密性を尊重するよう拘束されることを保証しなければならない。」

[24] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[25] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0078&from=EN

[26] http://data.europa.eu/eli/dir/2016/1148/oj

[27] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148. https://eur-lex.europa.eu/eli/dir/2022/2555

[28] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2557/oj

このほか、EU 加盟国の国内法には、医療機密に関する規律、患者の権利に関する法律、保険会社による特定の健康・遺伝子データの処理を禁止又は制限する保健分野の法律等において、健康に関するデータに適用される特定の規律も含まれている[29]。

2. 遺伝子に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、センシティブデータに該当する（GDPR 第 9 条第 1 項、GDPR 第 4 条第 13 項）。GDPR 第 4 条第 13 項は、遺伝子に関するデータを、「自然人の先天的又は後天的な遺伝的特性に関する個人データであって、当該自然人の生理学又は健康に関する固有の情報を与え、特に当該自然人に由来する生物学的試料の分析に起因するものをいう。」と定義しており、これに該当する限り、GDPR 上の遺伝子データに該当し、よって、センシティブデータに該当する。

GDPR 前文第 34 項では、次の通り言及されている。

> 「遺伝子データは、自然人の生物学的サンプルの分析、特に染色体、デオキシリボ核酸（DNA）又はリボ核酸（RNA）分析、又は同等の情報を得ることができる他の要素の分析から得られる自然人の遺伝的特性又は後天的に獲得した特性に関する個人データとして定義されるべきである」。

(i) 医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。

(ii) 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する。

個人データが「遺伝子データ」に該当するためには、医師等のような特定のデータ管理者によって収集される必要はない（GDPR 第 4 条第 13 項）。問題となる個人データが「遺伝子データ」の定義を満たす限り、当該データを収集した管理者に関係なく、遺伝子データとして認定される。

(iii) 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、当該情報が、生物学的試料の分析又はそれと同等の情報を得ることを可能にする他の要素の分析から生じる限りにおいて、センシティブデータに該当すると解される（GDPR 第 4 条第 13 項、同前文第 34 項）。

個人データが「遺伝子データ」に該当するためには、医師等のような特定のデータ管理者によって収集される必要はない（GDPR 第 4 条第 13 項）。問題となる個人データが「遺伝子データ」の定義を満たす限り、当該データを収集した管理者に関係なく、遺伝子データとして認定される。但し、GDPR の前文第 34 項は、「遺伝データは、自然人の先天的または後天的な遺伝的特徴に関する個人データであって、当該自然人の生物学的試料、特に染色体、デオキシリボ核酸（DNA）またはリボ核酸（RNA）の分析、または同等の情報を得ることができる他の要素の分析から得られるものと定義されるべきである。」としている。消費者が医師の判断や遺伝子検査キット等を介さずに自ら判断した遺伝に関する情

[29] 例えば、ベルギーでは、職業上/医療上の秘密保持に関する違反は、ベルギー刑法（http://www.ejustice.just.fgov.be/eli/loi/1867/06/08/1867060850/justel）第 458 条に基づき刑事罰の対象となるほか、健康に関する個人データの通信には、一定の例外を除き、原則として情報セキュリティ委員会の社会保障・健康部会の承認が必要である（健康に関する諸々の規定を含む 2006 年 12 月 13 日ベルギー法（http://www.ejustice.just.fgov.be/eli/loi/2006/12/13/2006023386/justel）第 42 条 2 項）といった規律が存在する。

報は、この前文第 34 項の定める内容に相当しないことから遺伝子データに該当しないとされる可能性もあると解される。

(2) 趣旨

遺伝子データは、その性質上、基本的権利及び自由との関係で特にセンシティブなものと考えられており、その処理の過程で基本的権利及び自由に対する重大なリスクが生じうるため、特別の保護に値する（GDPR 前文第 51 項）。

(3) 追加的規律（該当する場合）

GDPR は、加盟国が遺伝子データの処理に関して、制限を含むさらなる条件を維持又は導入することを認めている（GDPR 第 9 条第 4 項）。

したがって、遺伝子データに適用される追加の規定は、GDPR に基づく EU 加盟国の国内法において規定されている可能性がある。また、GDPR 第 88 条「雇用の過程における処理」に基づき、EU 加盟国は、雇用の文脈からより具体的な規律を定めることができるとされている。さらに、NIS 指令、NIS 2 指令、指令（EU） 2022/2557 の規律の対象となりうる。その内容については、上記設問 III. 1 (3)に対する回答参照。

また、遺伝的特徴については、EU 基本権憲章第 21 条が「性別、人種、皮膚の色、民族的又は社会的出自、遺伝的特徴、言語、宗教又は信念、政治的又はその他の意見、国内少数派の一員であること、財産、出生、障害、年齢、性的指向等の理由に基づくあらゆる差別は、禁止される。」と定めており、明確に禁止されている差別の理由の一つである。

このほか、EU 加盟国の国内法には、保健分野の法律等においても、遺伝子データに適用される特定の規律が含まれている可能性がある。

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する（GDPR 第 9 条第 1 項）。

(2) 趣旨

性生活及び性的指向に関するデータは、その性質上、基本的権利及び自由との関係で特にセンシティブなものと考えられており、したがって、その処理の過程が基本的権利及び自由に対して重大なリスクが生じうるため、特別な保護に値する（GDPR 前文第 51 条）。

(3) 追加的規律（該当する場合）

性的指向は、EU 基本権憲章第 21 条で禁止されている差別事由の一つである。
「性別、人種、肌の色、民族的又は社会的出自、遺伝的特徴、言語、宗教又は信念、政治的又はその他の意見、国内少数派の一員、財産、出生、障害、年齢、性的指向等のあらゆる理由に基づく差別は、禁止される。」

雇用と職業における平等な待遇のための一般的枠組みを確立する理事会指令では、雇用と職業に関する差別の禁止事由の一つとして性的指向が挙げられている（同指令第 2 条第 1 項、同第 2 項(b)）。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する（GDPR 第 9 条第 1 項）。

(2) 趣旨

労働組合への加入を明らかにするデータは、その性質上、基本的な権利と自由との関係において特にセンシティブであると考えられ、したがって、その処理の過程で基本的な権利と自由に対する重大なリスクが生じうるため、特別な保護に値する（GDPR 前文第 51 項）。

(3) 追加的規律（該当する場合）

GDPR 上、労働組合の組合員であることを明らかにするデータに関する追加的な規律は特に見当たらない。

もっとも、GDPR 第 88 条「雇用の過程における処理」に基づき、EU 加盟国は、雇用の文脈からより具体的な規律を定めることができるとされている。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、センシティブデータに該当する（GDPR 第 9 条第 1 項）。

生体データとは、「顔画像や指紋データ等、自然人の身体的、生理的又は行動的特徴に関連する特定の技術的処理の結果、その自然人の一意の識別が可能となる又は確認できる個人データ」（GDPR 第 4 条第 14 項）と定義される。

また、GDPR 前文第 51 項では、「自然人の一意の識別又は認証を可能にする特定の技術的手段によって処理される場合にのみ生体データの定義に含まれるため、写真の処理は体系的に特別な種類の個人データの処理とみなされるべきではない。」と規定されている。

EDPB のビデオ機器による個人データの処理に関するガイドライン[30]は、生体データの GDPR 第 9 条の下でのセンシティブなデータとしての概念をさらに次の通り明確にしている。

> 「74. GDPR に定義された生体データとして認定されるには、自然人の身体的、生理的又は行動的特徴等の生データの処理が、これら特徴の分析を意味するものである必要がある。生体データはこのような分析の結果であるため、GDPR はその第 4 条第 14 項で、『[...] 自然人の身体的、生理的又は行動的特徴に関する特定の技術的処理の結果であって、その自然人の固有の識別を可能にし又は確認するもの [...]』と定めている。しかし、個人のビデオ映像は、個人の識別に資する

[30] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

ために特別に技術的に処理されていない場合、それ自体では第 9 条の生体データとは見なされない。」

「75. 特別な種類の個人データ（第 9 条）の処理と見なされるためには、生体データが『自然人を一意に識別する目的で』処理されることが必要である。」

「76. 要約すると、第 4 条第 14 項と第 9 条に照らして、3 つの基準を考慮する必要がある。

- データの性質: 自然人の身体的、生理的又は行動的特徴に関するデータであること

- 処理の手段及び方法:『特定の技術的処理から生じる』データであること

- 処理の目的:自然人を一意に識別する目的で利用されるデータであること」

さらに、法執行の分野における顔認識技術の利用に関する EDPB のガイドライン[31]は、以下のように定める。

「7. FRT（顔認証技術）は、より広い意味での生体認証技術の種類に属する。生体認証は、物理的、生理的又は行動的特徴（指紋、虹彩構造、音声、歩行、血管パターン等）を定量化することによって個人を認識するために利用されるすべての自動化されたプロセスを含む。これらの特徴は、その個人を一意に識別することを可能にし、又は確認するため、『生体データ』と定義される。」

「8. これは、人の顔の場合であり、より具体的には、顔認識装置を利用した技術的処理である。顔の画像（写真又はビデオ）を撮影することにより、生体認証『サンプル』と呼ばれる顔の明確な特徴のデジタル表現（これを『テンプレート』という。）を抽出することが可能である。」

EDPB の仮想音声アシスタントに関するガイドライン（02/2021）[32]では、さらに以下のように規定される。

「31.音声データは本質的には生体認証された個人データである。その結果、当該データが自然人を一意に識別する目的で処理される場合、又は本質的に特別な種類の個人データであると判断される場合、その処理は第 6 条に基づく有効な法的根拠を有し、GDPR 第 9 条に基づく免除を伴う必要がある。」

脚注 31「GDPR は、「写真の処理 (...) は、自然人の固有の識別又は認証を可能とする特定の技術的手段を通じて処理される場合にのみ、生体認証データの定義の対象となる」（前文第 51 項）ため、データの性質のみでは、必ずしもデータが特別な種類に該当するか否かを決定するのに十分ではないと考える」と規定する。音声にも同じ理由付けが妥当する。

また、EU 加盟国のデータ保護当局の中には、生体データの処理に関する具体的なガイドラインを発表しているところもある[33]。

(2) 趣旨

生体データは、その性質上、基本的な権利と自由との関係で特にセンシティブなデータと考えられており、その処理の過程で基本的な権利と自由に対する重大なリスクを生じうるため、特別の保護に値する（GDPR 前文第 51 条）。

[31] https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en
[32] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_en
[33] 例えば、ベルギーデータ保護庁の生体データに関する勧告 1/2021 参照。

(3) 追加的規律（該当する場合）

2004 年 12 月 13 日付「加盟国が発行するパスポートおよび旅券のセキュリティ機能および生体認証に関する基準についての理事会規則」（No 2252/2004）[34]は、EU 加盟国のパスポート及び渡航文書について、生体認証識別子を含むセキュリティ機能の基準を定める。

加盟国は、生体データの処理に関して、制限を含むさらなる条件を維持又は導入することが可能である（GDPR 第 9 条第 4 項）。この点、複数の EU 加盟国が実際に、職場における生体アクセス制御システムにおける生体データの処理を規制・許可するための特定の法的規定を施行している。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータは、センシティブデータに該当しない。これらの種類のデータは、GDPR 第 9 条第 1 項の「特別な種類の個人データ」の定義において該当するものがない。これは、このようなデータが特別な配慮を要しない、あるいは（一般的な個人データと比して）特別な保護と特定の規則による保護を受けるべきではない、ということを意味するものではない。このことを示す例として、例えば、EDPB からは、さらなるオンライン取引を促進することのみを目的としたクレジットカードデータの保存の法的根拠に関する勧告（02/2021）[35]が公表されている。

(2) 趣旨

GDPR の提案に付随する欧州委員会スタッフワーキングペーパー[36]の影響評価において、EU の立法者がセンシティブデータの種類を「金融メッセージデータ、信用履歴、信用調査会社の「スコアリング」システムに含まれる金融支払能力（不良債権リスト）データ」等の金融データに拡大することを検討していたことが窺える（52 頁）。

しかし、センシティブデータの対象拡大は、「データ管理者がその手続きや技術システムを、当該データの処理に関するより厳しい規律に適合させる必要があるため、多大なコストを伴う」との懸念も示され（73 頁）、特に金融データについては、「（個人データの特別な種類に）金融データを含めると、その処理を一般的に新しいデータ保護要件に適合させなければならない金融セクターへの影響を考えると、一層の議論を招くだろう」とも述べられている（114 頁）。欧州委員会は、このような経緯から、GDPR 法案において、金融データを個人データの特別な種類の範囲に含めなかったことが推察される。

(3) 追加的規律（該当する場合）

EU 法及び EU 加盟国の国内法のもとでは、多くの法律や規制が金融データに適用され、影響を及ぼすことに留意されたい。一例として、関連する例を以下に挙げる。

- 2015 年 11 月 25 日付の欧州議会及び欧州理事会指令（2015/2366）[37]：この指令は、EU で決済サービスを提供する決済サービスプロバイダのための法的規制の枠組みを定める。特に、この指令には、決済口座へのアクセスや決済口座情報の利用に関する規律が含まれる（同指令第 66 条及び第 67 条）。また、加盟国は、決済詐欺の防止、調査、検出を保護するために必要な場合、

[34] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02004R2252-20090626
[35] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022021-legal-basis-storage-credit-card_en
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN
[37] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L2366

決済システム及び決済サービスプロバイダによる個人データの処理を許可できる。さらに、この指令は、決済サービスプロバイダは、決済サービス利用者の明確な同意を得た上で、決済サービスの提供に必要な個人データにのみアクセス、処理、保持しなければならないことを明確に定めている（同指令第 94 条）。なお、EDPB は、第二次支払サービス指令（Second Payment Services Directive）と GDPR の相互作用に関するガイドライン（06/2020）[38]を公開している。

- 金融セクターのデジタル・オペレーショナル・レジリエンスに関する規則（2022/2544）[39]は 2022 年 12 月 14 日に採択され、2023 年 1 月 16 日に発効する予定である。ICT のリスク管理、ICT 関連インシデントの報告・通知、ICT サービス事業者と金融事業者間の契約要件等、金融セクターにおけるネットワークや情報システムのセキュリティに関する要件を定めている。
- NIS 1 指令と NIS 2 指令：両指令は生活に不可欠なサービスの事業者に適用され、その中には信用機関も含まれる（NIS 1 指令の付属書 II と NIS 2 指令の付属書 I）。詳細については、上記 III. 1(3)に対する回答参照。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータは、センシティブデータに該当しない。この種類のデータは、GDPR 第 9 条第 1 項の「特別な種類の個人データ」の定義において該当するものがない。

ただし、EDPB は、第二次支払サービス指令と GDPR の相互作用に関するガイドラインにおいて、以下のように述べている。

> 「金融取引は、特別な種類の個人データに関連するものを含め、データ主体個人に関するセンシティブな情報を明らかにすることができる。例えば、取引の内容によっては、政党や政治団体、教会や小教区への寄付によって、政治的意見や宗教的信条が明らかになる可能性がある。労働組合への加入は、銀行口座から年会費が引き落とされることで判明する可能性がある。健康に関する個人データは、データ主体が医療専門家（例えば、精神科医）に支払った医療費を分析することで収集できる可能性がある。最後に、特定の購入品に関する情報は、その人の性生活や性的指向に関する情報を明らかにする可能性がある。これらの例に示されるように、単一の取引であっても、特別な種類の個人データを含むことがある。さらに、口座情報サービスは、GDPR 第 4 条 4 項に定義されるプロファイリングに依拠する可能性がある。EDPB によって承認された『規則 2016/679 のための自動化された個人の意思決定とプロファイリングに関する第 29 条作業部会のガイドライン』で以前述べたように、『プロファイリングは、それ自体では特別な種類のデータではないが、他のデータと組み合わされることでそうなるデータからの推論によって特別な種類のデータを生成できる』。つまり、金融取引の集計を通じて、様々な種類の行動パターンが明らかになり、その中に特別な種類の個人データが含まれる可能性がある。したがって、データ主体の金融取引に関する情報を処理するサービスプロバイダーが、特別な種類の個人データを処理する可能性はかなり高い。」

(2) 趣旨

上記 III. 6(2)に対する回答参照。

[38] https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202006_psd2_afterpublicconsultation_en.pdf
[39] https://eur-lex.europa.eu/eli/reg/2022/2554/oj

(3) 追加的規律（該当する場合）

上記 III. 6(3)に対する回答参照。

信用データの処理については、自動的な意思決定の対象とならない権利（right not to be subject to automated decision-making）（GDPR 第 22 条）も特に留意を要する。GDPR 前文第 71 項は、「データ主体は、自分に関する個人的側面を評価し、自動処理のみに基づき、自分に関する法的効果を生じさせ、又は同様に自分に著しい影響を与えるような決定（措置を含む）を受けない権利を有するべきである」と規定している（例えば、クレジットのオンライン申込の自動拒否や人手を介さない e リクルートの実践等）。このような処理には、自然人に関する個人的側面を評価する、あらゆる形式の自動処理からなる「プロファイリング」が含まれ、特に、本人に関する法的効果が生じるか、同様に大きな影響を及ぼす、データ主体の仕事上のパフォーマンス、経済状況、健康、個人的嗜好又は興味、信頼性や行動、場所又は移動に関する側面を分析又は予測する。（...）」とする。この権利の詳細は、下記 V. 2 参照。

また、EU 加盟国の国内法には、消費者の信用データ、特に消費者信用契約に関して経済的信用力を評価するための処理に用いられうる種類のデータについて、特に要件を課しているものがありうる。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。この種類のデータは、GDPR 第 9 条第 1 項の「特別な種類の個人データ」の定義において該当するものがない。

(2) 趣旨

GDPR の起案作業において、政府から財政的保護や援助を受けている事実に関するデータを特別な種類の個人データに含めるよう議論されたという記述は見当たらない。したがって、EU の立法者は、このようなデータを基本的な権利と自由との関係（GDPR 前文第 51 項）で特にセンシティブなものとは考えていなかったと思われる。

(3) 追加的規律（該当する場合）

政府から経済的保護や財政援助を受けている事実に関するデータについて、適用されうる規律は特に見当たらない。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、その内容によっては、センシティブデータに該当すると解される。このようなデータは、GDPR 第 9 条第 1 項の定める「特別な種類の個人データ」の範囲には明示的に含まれていないものの、センシティブデータを推知できるデータは、センシティブデータに該当すると解される（上記設問 II. 2 に対する回答参照）。このため、成年後見制度により保護されている事実に関する情報であって、それにより健康状態に関するデータ（障害を含む）が推知できるものであれば、成年後見制度の保護を受けている事実もセンシティブデータに該当する。

(2) 趣旨

健康に関するデータがセンシティブデータとして保護される趣旨について、上記 III 1 (2)に対する回答参照。

(3) 追加的規律（該当する場合）

健康に関するデータがセンシティブデータに適用される追加的規律について、上記 III. 1 (3)に対する回答参照。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報がセンシティブデータに該当するかは、場合による。

GDPR 第 9 条では、「特別な種類の個人データ」として「児童に関するデータ」を列挙していないため、児童に関するデータのすべてがセンシティブな個人データに該当するわけではない。ただし、児童に関するデータが GDPR 第 9 条に列挙された個人データの特定の種類に関連する限り、これらのデータは児童の年齢に関係なく、センシティブデータ（例：児童の健康状態に関するデータ）として保護される。さらに、未成年者は「脆弱な（vulnerable）」データ主体と解されている（前文第 75 項参照）ことは、注目に値する。

加えて、情報社会サービス（information society services）の提供に関連する児童の同意の有効性に関しても、特定の規律が適用される（下記 V. 1 (7)に対する回答参照）。

(2) 趣旨

GDPR の提案に付随する欧州委員会スタッフワーキングペーパーの影響評価において、EU の立法者がセンシティブデータの種類を「児童に関するデータ」まで拡大することを検討していたことが窺える（52 頁）。

しかし、センシティブデータの対象拡大は、「データ管理者は、その処理や技術システムを、当該データの処理に関するより厳しい規律に適合させる必要があるため、多大なコストを伴う」との懸念も示され（73 頁）。欧州委員会はこれを踏まえ、GDPR 法案において、児童に関する情報を個人データの特別な種類に記載しなかったものと解される。

(3) 追加的規律（該当する場合）

情報社会サービスの提供における児童の同意の有効性については、特定の規律が適用される（下記 V. 1 (7)に対する回答参照）。

処理の法的根拠に関して、正当な利益という法的根拠に依拠する場合、管理者は「正当な利益のバランステスト」を行い、管理者の正当な利益が、特にデータ主体が児童である場合、データ主体自身の利益及び基本的権利と自由によって覆されないことを証明しなければならない（第 6 条 1 項（f））。

また、GDPR 第 13 条及び第 14 条で言及されている、予定された処理に関する情報、並びにデータ主体の権利及びデータ侵害通知に関する情報をデータ主体に提供する場合、管理者は、特に児童に特に宛てられた情報（GDPR 第 12 条 1 項）について、明確かつ平易な言葉を用いて、簡潔、透明、理解可能かつ容易にアクセス可能な形式でそのような情報を提供するための適切な措置を講じなければならない。

さらに、GDPR 前文第 58 項は、「（…）児童が特別な保護に値することを考えると、児童に向けた処理が行われる場合のあらゆる情報とコミュニケーションは、児童が容易に理解できるような明確でわかりやすい言語であるべき」と明記している。

データ主体は、自分に関する個人データの消去を管理者から不当に遅延なく得る権利を有し、管理者は、特定の状況、特に第 8 条第 1 項が言及する情報社会サービスの提供に関連して収集された個人データ（情報社会サービスの文脈における児童の同意、詳細については下記 V. 1 (7)参照）を、不当に遅延なく消去する義務を負う。

そして、前文第 65 項は次のように規定する。

> 「（この権利は、データ主体が児童の頃に同意を与えたが、処理に伴うリスクを十分に認識しておらず、後に、特にインターネット上で当該個人データの削除を希望する場合に特に関連するものである。」

プロファイリングを含む自動的な意思決定の対象とならない権利（第 22 条）に関しては、当該意思決定が、管理者が従うべき EU 法又は加盟国法によって許可され、かつデータ主体の権利と自由及び正当な利益を保護するための適切な措置が規定されている場合には、適用がない。ただし、GDPR の前文第 71 項は、「当該措置は児童に関係するものであってはならない」と明記している。

## 11. オンライン行動履歴に関する情報

### (1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報がセンシティブデータに該当するかは、場合による。

上記のように、GDPR 第 9 条では、「特別な種類の個人データ」としてオンライン行動履歴に関するデータを列挙していないため、オンライン行動履歴に関するデータのすべてがセンシティブな個人データに該当するわけではない。

もっとも、センシティブデータはオンライン行動履歴に関するデータから推論される可能性がある[40]。このような推論されたデータは、GDPR 第 9 条のもとでセンシティブなデータとして保護される。

### (2) 趣旨

GDPR の起草段階において、オンライン行動履歴に関するデータを個人データの特別な種類に含めることを議論した文献は見当たらない。立法者は、このようなデータを基本的な権利と自由との関係（GDPR 前文第 51 項）で特にセンシティブなものとは考えていなかったと思われる。

### (3) 追加的規律（該当する場合）

[40] EDPB のソーシャルメディアユーザーのターゲティングに関するガイドライン（8/2020）のうち、特に、8.1.2 Inferred and combined special categories of data

オンライン行動履歴に関するデータは、クッキーを通じて収集することができ、これに応じたeプライバシー指令第5条第3項のクッキーについての規律に基づく保護の対象となる。eプライバシー指令第5条第3項では、加入者又はユーザーの端末機器への情報の保存や、すでに保存されている情報へのアクセスは、特に処理の目的について指令95/46/ECに従って明確かつ包括的な情報を提供された上で、当該加入者又はユーザーが同意を与えた場合にのみ認められることを加盟国が保証しなければならないことを定める。ただし、電子通信ネットワークを介したコミュニケーションの送信を唯一の目的とする技術的な保存又はアクセスに必要な場合、又は情報社会サービスのプロバイダーが、加入者若しくはユーザーが明示的に要求したサービスを提供する際に厳に必要な場合は、この限りではない。

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

#### (4) GDPR

##### (i) データ保護影響評価

GDPR第35条1項によると、特に新技術を利用した処理の種類が、自然人の権利と自由に対して高いリスクをもたらす可能性がある場合、管理者は処理に先立って、想定される処理作業が個人データの保護に及ぼす影響の評価（データ保護影響評価。以下「DPIA」という。）を実施しなければならない。DPIAを実施する義務は通常の個人データとセンシティブデータいずれにも適用されうるが、センシティブデータが関係する場合は適用される可能性がより高い。

DPIAは、以下の場合に必要となる（GDPR第35条第1項、第3項及び第4項）。

- プロファイリングを含め、自動的な処理に基づくものであり、かつ、それに基づく判断が自然人に関して法的効果を生じさせ又は本人に同様の重大な影響を及ぼす、自然人に関する人格的側面の体系的かつ広範囲な評価の場合
- 第9条に規定する特別な種類のデータ、又は第10条に規定する前科及び犯罪に関連する個人データの大規模な処理である場合
- 一般に公開された地域を、システムを用いて大規模に監視する場合
- その他自然人の権利と自由に対して高いリスクをもたらす可能性がある場合
- 各加盟国の監督当局が作成する、DPIAが必要となる個人情報の処理のリストに記載された処理に該当する場合

なお、各加盟国の監督当局は、DPIAが不要な場合の一覧を作成することができるとされている（GDPR第35条5項）。

また、法的義務の遵守や、公共の利益・管理者に帰属する公的権限の行使のために実施される業務の遂行に処理が必要な場合、DPIAは不要である（GDPR第35条10項）。

第29条作業部会のDPIAに関するガイドライン[41]は、DPIAが必要かどうかを評価するために考慮すべき9つの基準として以下の項目を示している。

- 評価又は採点（データ主体の勤務状況、掲載状況、健康、個人的な嗜好、信用性、場所などの側面に基づくプロファイリングなど）
- 法的又は類似の重要な効果を有する自動的な意思決定
- システムによる監視

[41] https://ec.europa.eu/newsroom/article29/items/611236

- センシティブデータ又は極めて個人的な性質を有するデータ
- 大規模に処理されたデータ
- データセットの照合又は結合
- 脆弱なデータ主体に関するデータ
- 革新的な利用、又は新しい技術的若しくは組織的なソリューションの適用
- 処理自体が、データ主体が権利を行使したり、サービスや契約を利用したりすることを妨げる場合

通常、DPIA は 2 つの基準が満たされる場合に必要となるが、1 つの基準のみ該当する処理にも DPIA が必要となる場合もある。

(ii) 特別な種類の個人データ及び前科・犯罪に関連するデータの処理が許可される場合

特別な種類の個人データの処理は、以下のいずれかに該当する場合を除き、原則として禁止されている（GDPR 第 9 条第 1 項及び第 2 項）。

(a) データ主体が、1 つ又は複数の特定された目的のためのその個人データの取扱いに関し、明確な同意を与えた場合

  - 例外：EU 又は加盟国の国内法が、データ主体の同意によりセンシティブデータ収集の禁止を解除できないことを定めている場合

(b) EU 法若しくは加盟国の国内法により認められている範囲内、又は、データ主体の基本的な権利及び利益のための適切な保護措置を定める加盟国の国内法による団体協約によって認められる範囲内で、雇用及び社会保障並びに社会的保護の法律の分野における管理者又はデータ主体の義務を履行する目的のため、又は、それらの者の特別の権利を行使する目的のために取扱いが必要となる場合

(c) データ主体が物理的又は法的に同意を与えることができない場合で、データ主体又はその他の自然人の生命に関する利益を保護するために処理が必要である場合

(d) 政治、思想、宗教又は労働組合の目的による団体、協会その他の非営利組織による適切な保護措置を具備する正当な活動の過程において、当該処理が、その組織の構成員若しくは元構成員、又は、その組織の目的と関係してその組織と継続的に接触をもつ者のみに関するものであることを条件とし、かつ、データ主体の同意なくその個人データが当該組織の外部に開示されないことを条件として処理が行われる場合

(e) 処理が、データ主体によって明示的に公開されている個人データに関連するものである場合

(f) 法的請求の確立、行使、防御のため、又は裁判所が司法上の権能を行使する際に処理が必要となる場合

(g) 求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための適切かつ個別の措置を定める EU 法又は加盟国の国内法に基づき、重要な公共の利益を理由とする取扱いが必要となる場合

(h) EU 法又は加盟国の国内法に基づき、又は、医療専門家との契約により、かつ、GDPR 第 9 条第 3 項に定める条件及び保護措置に従い、予防医学若しくは産業医学の目的のために、労働者の業務遂行能力の評価、医療上の 診断、医療若しくは社会福祉又は治療の提供、又は、医療制度若しくは社会福祉制度及びそのサービス提供の管理のために取扱いが必要となる場合

  - 第 9 条第 3 項は、特別な種類の個人データが、①EU 若しくは加盟国の法律又は各国の所轄

機関が定めた規律に基づき職業上の秘密保持義務を負う専門家により処理される場合若しくはその責任の下で処理される場合、又は②同じく EU 法若しくは加盟国の法律又は各国の所轄機関が定めた規律に基づく秘密保持の義務を負う他の者によって処理される場合、上記の目的のために処理されうることを規定する。

(i) データ主体の権利と自由を保護するための適切かつ具体的な措置、特に職業上の秘密を規定する EU 法又は加盟国の法律に基づく、健康に対する国境を越えた深刻な脅威からの保護、又はヘルスケア及び医薬品又は医療機器の高い品質と安全性の確保等、公衆衛生の分野における公益上の理由から処理が必要である場合

(j) 求められる目的と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的 な権利及び利益の安全性を確保するための適切かつ個別の措置を定める EU 法又は加盟国の国内法に基づき、第 89 条第 1 項に従い、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取扱いが必要となる場合

- 第 89 条第 1 項には、公共の利益における保管の目的、科学調査若しくは歴史調査の目的又は統計の目的のための処理は、GDPR に従い、データ主体の権利及び自由のための適切な保護措置に従うものとすると規定している。それらの保護措置は、とりわけデータの最小化の原則に対する尊重を確保するために、技術的及び組織的な措置を設けることを確保する。それらの措置は、それらの目的がそのような態様で充足されうる限り、仮名化を含むことができる。データ主体の識別を許容しない又は許容することのない別の目的による取扱いによってそれらの目的が充足されうる場合、それらの目的は、その態様によって充足される。

また、加盟国の法律は、遺伝子データ、生体データ、健康に関するデータの処理に関して、制限を含むさらなる条件を維持又は導入することができる旨定められている（GDPR 第 9 条 4 項）。

前科及び犯罪に関する個人データは、公的機関の管理下においてのみ処理することができ、また、データ主体の権利及び自由に対する適切な保護措置を定めた EU 法又は加盟国の法律によって処理が許可された場合にのみ処理できる（GDPR 第 10 条）。前科の包括的な記録は、公的機関の管理下においてのみ保管されるものとする（同条）。したがって、前科及び犯罪に関する個人データを処理する場合は、犯罪や前科に関連する個人データがどのような条件で処理されるかを規定する加盟国の国内法を参照する必要がある。

(5) 法施行指令

法施行指令第 10 条は、データ主体の権利と自由に対する適切な保護措置のもとで、次に掲げるいずれかに該当し厳密に必要な場合にのみ、特別な種類の個人データの処理を許可するものと定めている。

- EU 法又は加盟国の法律により許可されている場合
- データ主体又は他の自然人の生命的利益を保護する場合
- 当該処理が、データ主体によって明示的に公開されているデータに関連する場合

2. 利用

上記 IV. 1 参照。

3. 第三者提供

通常の個人データ、センシティブデータいずれについても、第三者提供に関する同様の規律が適用される。

4. 管理

上記 IV. 1 参照。

データ保護責任者（以下「DPO」という。）とは、データ保護法及び実務に関する専門的な知識を有し、管理者又は処理者による本規則の遵守を監視することを支援する者である（GDPR 前文第 97 項）。通常の個人データ及びセンシティブデータのいずれとの関係でも DPO の任命が必要とされうるが、センシティブデータが関係する場合は DPO の任命が必要とされる可能性がより高い。

具体的には、GDPR 第 37 条第 1 項に基づき、以下の場合、DPO を任命しなければならない。

- 処理が公的機関又は団体によって実施される場合（ただし、司法上の権能を行使する裁判所を除く）
- 管理者又は処理者の中核的活動が、大規模でデータ主体を定期的かつ体系的に監視する必要のある処理業務で構成されている場合
- 管理者又は処理者の中核的活動が、特別な種類のデータ（第 9 条）及び前科及び犯罪に関する個人データ（第 10 条）の大規模な処理で構成されている場合

GDPR 前文第 97 項は、ここでいう「中核的活動」（core activities）とは（付随的な活動ではない）「主要な活動」（primary activities）を指すことを明確にしている。

その他の場合、管理者若しくは処理者、又は管理者若しくは処理者の属性を代表する協会及びその他の団体は、データ保護責任者を任命することが可能であり、EU 法若しくは加盟国の法律によって要求される場合には、任命しなければならない（GDPR 第 37 条 4 項）。

5. 請求権

通常の個人データとセンシティブな個人データには、同じデータ主体の権利が適用される。これらの権利は以下の通りである。

- 同意を撤回する権利（GDPR 第 7 条）
- 個人データの収集と利用について情報を得る権利（GDPR 第 12 条、第 13 条及び第 14 条）
- 個人データにアクセスする権利（GDPR 第 15 条）
- 不正確又は不完全な個人データを修正する権利（GDPR 第 16 条）
- 消去する権利（GDPR 第 17 条）
- 個人データの処理を制限する権利（GDPR 第 18 条）
- データポータビリティの権利（GDPR 第 20 条）
- 異議を申し立てる権利（GDPR 第 21 条）
- プロファイリングを含む自動処理のみに基づく決定の対象とならない権利（GDPR 第 22 条）
- 管轄のデータ保護当局に苦情を申し立てる権利

センシティブな個人データについては、上述の権利に関し特定の規律が存在するものがある。これらの具体的な規律については、以下の通りである。

(1) 消去する権利（GDPR 第 17 条）

消去する権利は、第 9 条第 2 項（h）及び（i）並びに第 9 条第 3 項に従い、公衆衛生の分野における公益上の理由から処理が必要である場合には適用されない（GDPR 第 17 条 3 項）（これらの条文の内容については、上記 IV. 1 参照）。

(2) データポータビリティの権利（GDPR 第 20 条）

データポータビリティの権利は、センシティブデータについては、データ主体の明示的な同意が処理の法的根拠となっている場合にのみ利用可能である（GDPR 第 9 条 2 項（a））（GDPR 第 20 条 1 項（a））。

(3) プロファイリングを含む自動処理のみに基づく決定の対象とならない権利（GDPR 第 22 条）

データ主体は、原則として、プロファイリングを含む自動処理のみに基づく決定で、自分に関する法的効果を生じさせるか、同様に自分に重大な影響を与えるものの対象とならない権利を有する（GDPR 第 22 条 1 項）。

この権利には、以下の決定である場合に例外が存在する（GDPR 第 22 条 2 項）。

- データ主体者とデータ管理者との間の契約の締結又は履行に必要な決定
- 管理者が従う EU 法又は加盟国法によって許可され、データ主体の権利と自由及び正当な利益を保護するための適切な措置が定められている決定
- データ主体からの明示的な同意に基づく決定

ただし、GDPR 第 22 条 2 項で言及されている決定は、以下の場合を除き、センシティブデータに基づくものであってはならない。

- センシティブデータについて、（i）データ主体の明示的な同意がある場合、又は（ii）本質的な公益上の理由による必要性に基づいて、追求される目的に比例し、データ保護の権利の本質を尊重し、データ主体の基本的権利及び利益を保護するための適切かつ特定の措置を規定する EU 法又は加盟国の法律に基づき取得される場合
- データ主体の権利と自由及び正当な利益を保護するための適切な措置がとられている場合

## V. 本人同意、プロファイリング

### 1. 本人同意

(1) センシティブデータ規制（上記III）との関係

本人同意は、「自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思の表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの取扱いの同意を表明するもの」（GDPR 第 4 条 11 項）と定義される。

本人同意は、GDPR 第 6 条 1 項及び 9 条 2 項に基づくセンシティブデータの処理が許可される処理及び状況として考えられる法的根拠の一つに過ぎないと整理されている。第 9 条 2 項（a）によれば、センシティブデータについては、データ主体の「明示的同意」であることが必要である。

(2) 要件一般

同意は、以下を満たすものでなければならないとされている（GDPR 第 4 条第 11 項及び規則 2016/679 に基づく同意に関するガイドライン）。

- 自由に与えられたものであること
- 具体的であること
- 情報が提供されたこと
- 曖昧でないこと

また、データ管理者は、データ主体からの同意を証明できるようにしなければならない（GDPR 第 7 条第 1 項）。

さらに、規則 2016/679 に基づく同意に関するガイドラインは、以下も要求する。

- 自由に与えられた同意（GDPR 第 7 条 4 項）

  データ主体は、同意するか否かを決定する際に、実質的に選択肢が与えられていなければならない。データ主体が実質的には選択肢を与えられておらず、同意を強制されたと感じたり、同意しないことによって好ましくない結果を甘受しなければならないことになる場合は、自由に与えられた同意は存在しないとされる。

  例えば、雇用の状況や公的機関との関係において、管理者とデータ主体との間に明らかな力の不均衡が存在する場合、実質的に選択肢は与えられていない。また、例えば、契約の履行に必要でないデータの処理にデータ主体が同意しなければ契約が履行されない場合等、同意がサービスの提供に結びついている場合も、自由に与えられた同意とはいえない。さらに、データ主体が処理目的をまとめて受け入れなければならない場合にも、実質的な選択肢は与えられていない。あるサービスが複数の目的のために複数の処理操作を伴う場合、データ主体は、どの目的に同意するかを自由に選択できなければならない。

- 具体的であること

  下記（5）参照。

- 情報が提供されたこと

  下記（3）参照。

- 曖昧でないこと

  ある処理に対するデータ主体の同意は、明確でなくてはならないとされている。

- 文書化された同意であること

  前文第 42 は、「処理がデータ主体の同意に基づく場合、管理者は、データ主体が処理操作に同意したことを証明できなければならない。」と規定する。したがって、管理者は、有効な同意を得たことを文書化しなければならない。

GDPR は、データ主体の同意をどのように証明するかについては記述していない。規則 2016/679 に基づく同意に関するガイドラインは、さらに「管理者が有効な同意を得たことを証明する義務は、それ自体が過剰な量の追加のデータ処理につながるべきではない。つまり、管理者は、（同意が得られたことを

示すため）処理との関連性を示すのに十分なデータを持つべきだが、必要以上の情報を収集すべきではない。」ことを明らかにしている（第 106 段落）。

この要件に準拠する方法の具体例として、受け取った同意の陳述にかかる記録を残すことが、同ガイドラインにあげられている。

(3) 情報提供

有効な同意とは、通常の個人データもセンシティブな個人データについても、具体的な情報の提供を受けた上での同意（informed consent、インフォームドコンセント）を意味する（GDPR 第 4 条第 11 項参照）。標準的な実務としては、公正かつ透明な処理を確保するために必要なすべての情報を提供する必要がある（GDPR 第 13 条及び 14 条- 透明性の義務に関しては、IV. 1.参照）。

規則 2016/679 に基づく同意に関するガイドラインの第 64 段落によると、情報提供される同意に必要な最低限の内容は以下のとおりである。

- 管理者の身元と連絡先
- 同意が求められる処理業務のそれぞれの目的
- 収集・利用されるデータの種類
- 該当する場合、データの受領者（の種類）
- 同意を撤回する権利の存在（ただし、撤回前の同意に基づく処理の合法性には影響しない）。
- 関連する場合、自動的な意思決定（GDPR 第 22 条 2 項（c））のためのデータの利用に関する情報
- 十分性認定や適切な保護措置がないために国際的なデータ移転に関して起こりうるリスク（GDPR 第 46 条）

(4) 形式

GDPR 第 6 条に基づく法的根拠としての同意と、センシティブデータの処理が許容される場合としての明示的な同意の両方について、GDPR 第 4 条第 11 号は、同意を「（...）データ主体が、陳述又は明確な肯定的行動により、自身に関連する個人データの処理に同意したことを示す意思表示」と定義しており、いかなる推定的又は黙示的な同意も除外されている。

また、GDPR 前文第 32 項は、「この（肯定的な）同意には、インターネットのウェブサイトを訪問する際にボックスにチェックを入れること、情報社会サービスの技術設定を選択すること、又はこの文脈でデータ主体が個人データに関し提案される処理を受け入れることを明確に示す別の陳述又は行為が含まれ得る」ことを明確にしている。

同意の要求は、他の事項から明確に区別できる方法で、明確で平易な言語を用いて、分かりやすく、容易にアクセスできる形で提示されなければならない（GDPR 第 7 条第 2 項）。管理者は、データ主体が同意していることを証明できなければならず（GDPR 第 7 条第 1 項）、同意を与えることも同意を撤回することと同じくらい容易でなければならない（GDPR 第 7 条第 3 項）。

規則 2016/679 に基づく同意に関するガイドラインによれば、次の通りとされている。

- GDPR 第 6 条に基づく同意
    - 「66. GDPR は、インフォームドコンセントの要件を満たすために情報を提供しなければならない形態や形状を規定していない。つまり、有効な情報は、書面や口頭での発言、音声や

映像のメッセージ等、さまざまな方法で提示される可能性がある。（...）」

- 「71. 同意が電子的手段で要求される場合、前文第 32 に従い、同意の要求は別個のものでなければならず、単に利用規約の中の一項とすることはできない。小さな画面や情報を表示するスペースが制限されている状況に対応するため、ユーザーエクスペリエンスや製品設計を過度に妨げないよう、適切な場合には情報を重層的に表示する方法も考えられる。」

- GDPR 第 9 条に基づく明示的な同意
  - 「92. GDPR は、『陳述又は明確な積極的行動』が『通常の』同意の前提条件であると規定している。しかし、より厳しい要件であるデータ主体による明示的な同意を得るために、特別な努力が必要とされる。」
  - 「93. 明示的という用語は、データ主体が同意を明示的に表明する必要があることを意味する。同意が明示的であることを確認する明確な方法は、書面による同意を明示的に確認する方法である。適切な場合、管理者は、将来起こりうる疑義や証拠不足の可能性をすべて取り除くために、書面による陳述にデータ主体が署名していることを確認することができる。」
  - 「94. しかし、このような署名入りの陳述は、明示的な同意を得る唯一の方法ではなく、GDPR が、有効な明示的同意を必要とするすべての状況において、書面及び署名入りの陳述を規定しているとは言い切れない。例えば、デジタル又はオンラインの状況では、データ主体は、電子フォームへの記入、電子メールの送信、データ主体の署名が入ったスキャン文書のアップロード、又は電子署名の利用によって、必要な陳述を提供することができる可能性がある。理論的には、口頭による陳述の利用も、有効な明示的同意として十分な表現となり得るが、陳述の記録時に有効な明示的同意の条件がすべて満たされていたことを管理者が証明することは困難な場合がある。」
  - 「95. 組織は、選択に関する情報が公正で分かりやすく明確であり、データ主体による具体的な確認を求める（例えば、ボタンを押す、口頭で確認する等）ことを条件に、電話での会話を通じて明示的な同意を得ることもできる。」
  - 「98. 同意の二段階認証は、明示的な同意が有効であることを確認するための方法にもなり得る。例えば、データ主体が、管理者から医療データを含む記録を処理する意図を通知する電子メールを受け取ったとする。ここで、管理者はその電子メールで、特定の目的のために特定の情報セットを利用することに同意を求める旨説明する。データ主体がこのデータの利用に同意した場合、管理者は『同意する』という文言を含む電子メールの返信を求める。返信が送信された後、データ主体は、同意を確認するために、クリックしなければならない検証リンク、又は検証コードを含む SMS メッセージを受け取る。」

(5)　個別同意の必要性

一般的な個人データとセンシティブデータの両方について、同意は具体的でなければならない（第 4 条第 11 項参照）。

GDPR 第 6 条第 1 項（a）及び第 9 条第 2 項（a）は、データ主体の同意が「1 つ又は複数の特定の」目的に関してなされなければならず、データ主体がそれぞれの目的に関して選択できることを規定している。

さらに、前述のとおり、インフォームドコンセントのために最低限提供すべき情報には、同意を求める各処理業務の目的に関する情報も含まれる（上記(3)参照）。

上記及び規則 2016/679 に基づく同意に関するガイドライン[42]（第 58 段落）から、データ主体が特定の処理目的ごとに同意できるようにする必要があるため、複数の処理目的に対して行われる同意は許されな

[42] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en

いと考えられる。また、同ガイドライン第 60 段落において、EDPB は、「様々な異なる目的に対して同意を求める管理者は、ユーザーが特定の目的に対して特定の同意を与えることができるように、各目的に対して個別のオプトイン（の機会）を提供すべきである」ことを特に明らかにする。

さらに、同ガイドライン第 61 段落では、「管理者は、データ主体に異なる選択肢による影響を認識させるために、目的ごとに処理されるデータについて、個別の同意の要求とともに具体的な情報を提供すべきである。こうして、データ主体は具体的な同意を与えることができるようになる。」としている。

(6) 同意撤回

一般な個人データとセンシティブデータの両方について、同意はいつでも撤回することができる（GDPR 第 7 条第 3 項）。同意を与える前に、データ主体にはその旨が通知されるものとする（GDPR 第 13 条第 2 項(c)及び第 14 条第 2 項(d)）。データ主体が同意を撤回することは、同意を与えたときと同様に容易でなければならない（GDPR 第 7 条第 3 項）。ただし、同意の撤回は、撤回前の同意に基づく処理の適法性に影響を与えない（GDPR 第 7 条第 3 項）。

(7) その他留意事項

情報社会サービスに関する児童の同意に関する具体的な要求事項がある。すなわち、GDPR 第 8 条第 1 項によると、情報社会サービス（以下に示す定義の電子的サービスを指す）が児童に直接提供される場合、児童の個人データの処理は、児童が 16 歳以上（ただし、加盟国はこの年齢を 13 歳を下回らない年齢に引き下げる可能性がある）である場合に適法となる。児童が 16 歳未満である場合、当該処理は、児童の親としての責任を有する者から同意が得られる場合、又はその範囲においてのみ適法となる。

管理者は、このような場合、利用可能な技術を考慮し、同意が児童に対する親としての責任を有する者によって与えられたこと、又は承認されたことを確認するために、合理的な努力をするものとする（GDPR 第 8 条第 2 項）。

ただし、児童に直接提供される予防的サービス又はカウンセリングサービスの文脈では、親権者の同意は必要ない（GDPR 前文第 38 項）。

GDPR 前文第 38 項は、「児童は、個人データの処理に関連するリスク、結果及び関係する保護措置、並びに、自らの権利について十分に認識できないかもしれないため、その個人データに関して特別の保護を享受する。特に、マーケティングの目的、その子どもに関するパーソナリティ若しくは個人プロファイルの作成の目的での子どもについて の個人データの使用、及び子どもに対して直接に提示されるサービスを利用する際の子どもの個人データの収集に対して、そのような特別の保護が適用されなければならない」と説明する。

情報社会サービスとは、以下のサービスを指す（GDPR 第 4 条 25 号が指令 2015/1535[43]第 1 条第 1 項（b）の定義を参照している）。

> 「遠隔地で、電子的手段により、サービスの受領者の個別の要求に応じて、通常は報酬を得て提供されるあらゆるサービス。
>
> この定義における用語については、それぞれ以下のとおり意味を有する（指令 2015/1535 第 1 条第 1 項 （b））。
>
> (i) 『遠隔地』とは、当事者が同時に存在することなくサービスが提供されることを意味する。

[43] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015L1535&from=EN#d1e245-1-1

(ii) 『電子的手段』とは、データの処理（デジタル圧縮を含む）及び保存のための電子機器により、サービスが最初に送信され、その宛先で受信されること、並びに有線、無線、光又はその他の電磁的手段により完全に送信、伝達及び受信されることを意味する。

(iii) 『サービスの受領者の個別の要求に応じて』とは、個別の要求によるデータの送信を通じてサービスが提供されることを意味する。」

## 2. プロファイリング

### (1) プロファイリング・データ分析に対する規律

データ主体は、原則として、プロファイリングを含む自動処理のみに基づく決定で、自らに関する法的効果を生じさせるか、同様に自らに重大な影響を与えるものの対象とならない権利を有する（GDPR 第 22 条第 1 項）。

この権利は、当該決定が以下の各号に該当する場合には適用されない（GDPR 第 22 条第 2 項）。

(a) データ主体及びデータ管理者間の契約の締結又は履行に必要である場合
(b) 管理者がそれに服し、かつ、データ主体の権利及び自由並びに正当な利益の安全性を確保するための適切な措置も定める EU 法又は加盟国の国内法によって認められている場合
(c) データ主体の明示的な同意に基づく場合

上記の第(a)号及び第(c)号の場合、データ管理者は、データ主体の権利及び自由並びに正当な利益を保護するための適切な措置を実施し、少なくとも管理者側の人的介入を得る権利、自分の意見を表明する権利、決定に異議を申し立てる権利（GDPR 第 22 条第 3 項）をデータ主体に与えなければならない。

センシティブデータに基づく自動化された決定は、以下の双方を満たす場合のみ GDPR 第 22 条第 2 項にいう自動化された決定となる（GDPR 第 22 条第 4 項）。

- センシティブな個人データが、（i）データ主体の明示的な同意、又は（ii）本質的な公益上の理由による必要性に基づいて、追求される目的に比例し、データ保護の権利の本質を尊重し、データ主体の基本的権利及び利益を保護するための適切かつ具体的措置を規定する EU 法又は加盟国の法律に基づき取得されている
- データ主体の権利と自由及び正当な利益を保護するための適切な措置がとられている

### (2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリング・データ分析により生成されたデータは、センシティブデータに該当しうる。

第 29 条作業部会の自動化された個人の意思決定及びプロファイリングに関するガイドライン[44]は以下の通り述べている。

> 「管理者は、（GDPR）第 9 条 2 項に規定された条件の 1 つと第 6 条の条件を満たすことができる場合にのみ、特別な種類の個人データを処理できる。これには、プロファイリングから由来又は推知された特別な種類のデータが含まれる。
>
> プロファイリングは、それ自体は特別な種類のデータではないが、他のデータと組み合わされると特別な種類のデータになるデータから推知して、特別な種類のデータを作成できる。例えば、

[44] https://ec.europa.eu/newsroom/article29/items/612053/en

食品の品質及びエネルギー含有量に関するデータと組み合わせた食品購入の記録から、ある人の健康状態を推測できる可能性がある。

個人の健康状態、政治的信条、宗教的信条、又は性的指向について何かを示す相関関係が発見される可能性がある（...）」（15 頁）

また、上記 II,2 で言及したソーシャルメディア利用者のターゲティングに関するガイドラインの第 123 段落の例も、プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうることを示していると言える。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

第 29 条作業部会の自動化された個人の意思決定及びプロファイリングに関するガイドラインはさらに、次の通り規定する。

「プロファイリングからセンシティブな嗜好や特性が推測される場合、管理者は次のことを確認する必要がある。

- その処理が本来の目的と矛盾しないこと
- 特別な種類のデータの処理に関する合法的な根拠を特定したこと
- データ主体に処理について通知したこと」（15 頁）

同ガイドラインは次のことを明らかにする。

「特別な種類の個人データを含む自動的な意思決定（第 22 条 1 項に記載）は、次の重複的な場合（第 22 条 4 項）にのみ許される。

- 第 22 条第 2 項の例外規定が適用される場合
- 第 9 条第 2 項のポイント（a）又は（g）が適用される場合

（...） 上記のいずれの場合も、管理者は、データ主体の権利と自由及び正当な利益を保護するための適切な措置を講じなければならない。」（24 頁）

## VI. センシティブデータの取扱いに係る裁判例・決定等

センシティブデータに関するいくつかの事件は、予備的判決（EU 法の解釈に関連し EU 各国の裁判所から送られてくる照会）のために司法裁判所に付託され、現在係争中である。本調査の趣旨を踏まえ現地カウンセルにより選定された事案について、以下概略を示す。

- 付託 C-446/21[45]は、性的指向のデータに関する事件である。具体的には、GDPR 第 9 条第 2 項（e）の下、パネルディスカッションの目的で個人が自身の性的指向について発言した場合、個人向け広告のためにデータを集約し分析する目的による、性的指向に関する他のデータの処理が許されるか否かというものである。
- 付託 C-667/2146は、健康に関するデータに関する事件である。主な問題は、GDPR 第 9 条第 2 項

[45] https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-446%252F21&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%2 52C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&page=1&lg=&cid=468060

[46] https://curia.europa.eu/juris/documents.jsf?nat=or&mat=or&pcs=Oor&jur=C%2CT%2CF&num=C-667%252F21&for=&jge=&dates=&language=en&pro=&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%2

（h）の下、健康保険基金の医療サービスが、従業員の労働能力評価の前提条件となる健康に関するデータを処理することが禁止されるか否かというものである。

- 付託 C-115-22[47]は、スポーツに関するもので、いくつかの論点からなるが、その中の一つとして次の点が問題となる。
  - ある人物が特定のドーピング違反を犯し、その結果、その人物が（国内及び海外の）競技会への参加を禁止されたという情報は、健康に関するデータであるか否か。
  - ある人物が特定のドーピング違反を犯し、その結果、その人物が（国内及び海外の）競技会への参加を禁止されたという情報の開示が、前科及び犯罪に関する個人データの処理に該当するかどうか（第 10 条）。この質問に対し、該当するという回答がなされた場合、独立仲裁委員会が GDPR 第 10 条の意味における公的機関（前科についての個人データの処理が認められる機関）であるか。
- 付託 C-252/21[48]は、Facebook による、マッチングアプリ、ゲイの出会い系サイト、政党のウェブサイト、又は健康関連のウェブサイトに関連するパーソナライズされたコンテンツ、広告、ソーシャルメディアプラグインの実装に関する複数の論点が含まれており、特に以下の質問が挙げられている。
  - インターネット利用者が、マッチングアプリ、ゲイの出会い系サイト、政党のウェブサイト、健康関連のウェブサイト等、GDPR 第 9 条第 1 項の基準が関係するウェブサイトやアプリを単に訪問したり、登録時や注文時等に情報を入力したりするだけで、Facebook Ireland のような別の事業者が、それらのウェブサイトやアプリに統合された 「Facebook ビジネスツール」のようなインターフェース、又はインターネット利用者のコンピュータやモバイルデバイスに配置された Cookie や類似のストレージ技術を使用して、それらのウェブサイトやアプリへの訪問やユーザーが入力した情報に関するデータを収集し、それらのデータをユーザーの Facebook.com アカウントのデータとリンクさせて使用する場合、この収集や関連付け、使用には、同項の意味でのセンシティブデータの処理が含まれるか否か。
  - もし含まれるのならば、それらのウェブサイトやアプリを訪問・情報を入力し、もしくは Facebook Ireland 等の事業者がそれらに統合したボタン（「いいね」「シェア」「Facebook ログイン」「アカウントキット」等のソーシャルプラグイン）をクリック又はタップすることは、GDPR 第 9 条第 2 項（e）の意味において、訪問そのものあるいはユーザーが入力した情報に関するデータの（データ主体による）明示的な公開になるか否か。
  - GDPR 第 6 条 1 項（a）及び第 9 条第 2 項（a）の意味における同意は、Facebook Ireland のような独占的事業者に対してであっても、有効に、かつ GDPR 第 4 条第 11 項等に従い任意で、与えられることができるか。

## VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

EU の法制度動向として、第一に、欧州委員会は、欧州健康データ空間（EDHS）に関する規制案[49]を提示した。その目的は、ヘルスケアをデジタル化し、健康に関するデータを巡る経済の可能性を最大限に引き出すことにある。そのため、EDHS は医療従事者と個人間のデータ交換だけでなく、研究者、政策立案者、企業とのデータ交換にも重点を置くことになる。データアクセス機関が発行する許可に基づき、特定の目的のためのデータ交換のみを許可し、安全な処理環境を要求することで、GDPR の原則が守られる予定である。

52C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&oqp=&td=%3BALL&avg=&lgrec=en&page=1&lg=&cid=471265

[47] https://curia.europa.eu/juris/liste.jsf?num=C-115/22&language=en

[48] https://curia.europa.eu/juris/liste.jsf?num=C-252/21&language=en

[49] https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en

第二に、欧州委員会は、データに関する欧州の戦略を通じて、データの単一市場を作成することを目指している。この戦略では、2022 年 5 月 30 日に採択された欧州データガバナンスに関する 2022 年 5 月 30 日付欧州議会及び理事会規則（EU）2022/868 及び規則（EU）2018/1724 の改正とデータ法案[50]という、2 つの主要な立法構想が取り上げられている。データ法案は、個人データと非個人データの両方に適用され、GDPR と大きな相互作用がある。データ法案第 1 条によると、「製品又は関連サービスの利用によって生成されたデータをその製品又はサービスの利用者が利用できるようにすること、データ保有者はデータ受領者がデータを利用できるようにすること、及び公益のために行われる業務の遂行のために、例外的必要がある場合にデータ保有者が公共部門機関又は連合の機関若しくは団体にデータを利用できるようにすることについて調和のとれた規則を定める。」とされている。

第三に、2017 年以降、クッキーの規律を含む e プライバシー指令を更新・廃止する新しい e プライバシー規則の議論が進んでいる。欧州委員会は 2017 年 1 月 10 日、e プライバシー規則の第 1 次草案を提示した。当初、e プライバシー規則は、一般データ保護規則（GDPR）とともに 2018 年 5 月 25 日から適用される予定であった。しかし、EU 加盟国はまだこの規制案について合意できていない。それ以来、さまざまな提案が発表されている。e プライバシー規則は、特に、クッキーや類似技術の利用に適用される規律をさらに調和させる必要がある。一方、欧州のデータ保護当局は、GDPR に対応したクッキーの同意要件の解釈に関し、以下のようなガイドラインを発表している。

- EDPB は、2023 年 1 月 17 日、「クッキー・バナー・タスクフォースによる作業報告書」を採択した[51]。この報告書は、e プライバシー指令および GDPR の規定のうち、特に事前チェックボックスとバナーデザインに関してクッキーに適用されるものについての欧州データ保護当局の共通解釈を示す。
- ベルギーデータ保護当局は、ダイレクトマーケティング目的の個人データ処理に関する勧告 01/2020 を発表した[52]。これにはクッキーの使用に関する規定が多数含まれている。また、ウェブサイトにおいてもクッキーに関するガイダンスを公表した[53]。
- フランスデータ保護局は、クッキーおよびその他のトラッカーに関するガイドラインおよびクッキーおよびその他のトラッキング技術に関する勧告を公表した[54]。
- アイルランドデータ保護局は、クッキーおよびその他のトラッキング技術に関するガイダンスノートを発行した[55]。

また、米国に関する十分性認定案について、2022 年 12 月 13 日、欧州委員会は、米国の法的枠組みを評価し、EU と同等のセーフガードを提供していると結論づける十分性認定案[56]を発表した。十分性認定案は、今後、採択手続きに入る。この認定案は、欧州データ保護委員会（EDPB）に送付され、同委員会は 2023 年 2 月 28 日に意見を公表した[57]。その後、十分性認定案は、EU 加盟国の代表者で構成される委員会によって承認されなければならない。欧州議会はさらに、十分性認定に関する精査の権利を有する。この手続きが完了した後、欧州委員会は最終的な十分性認定を採択することができる。

その他センシティブデータに処理に関連する規律として、以下のような法令が存在する。

- EU 基本権憲章第 21 条：「性別、人種、肌の色、民族的又は社会的出自、遺伝的特徴、言語、宗教又は信念、政治的又はその他の意見、国民的少数者の一員、財産、出生、障害、年齢又は性的指向等のいかなる理由に基づく差別も禁止される。」
- 2000 年 6 月 29 日付理事会指令（2000/43/EC）[58]は、民族的出自に関係なく人を平等に扱うという

[50] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2022%3A68%3AFIN
[51] https://edpb.europa.eu/system/files/2023-01/edpb_20230118_report_cookie_banner_taskforce_en.pdf
[52] https://www.autoriteprotectiondonnees.be/publications/recommandation-n-01-2020.pdfvvvvvvvv
[53] https://www.autoriteprotectiondonnees.be/professionnel/themes/cookies
[54] https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf
[55] https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance note on cookies and other tracking technologies.pdf
[56] https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en
[57] https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-52023-european-commission-draft-implementing_en
[58] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0043&from=EN

原則を施行するもので、人種や民族的出自を理由とする差別と闘うための枠組みを定めるものである。本指令は、かかる理由に基づく直接的又は間接的な差別を禁止する（第 2 条）。この指令は、公共団体を含む官民両部門に関して、次の事項について、すべての人に適用される（第 3 条）。

- 選考基準及び採用条件を含む、雇用、自営業、職業へのアクセスに関する条件（昇進を含む）
- 職業指導、職業訓練、高等職業訓練及び再訓練（実務経験を含む）のすべての種類への及び水準のアクセス
- 解雇及び賃金を含む、雇用及び労働条件
- 労働者又は雇用者の組織、又は特定の職業を営む者を構成員とする組織への加入及び関与（かかる組織により提供される便益を含む）
- 社会保障及び医療を含む、社会的保護
- 社会的利益
- 教育
- 住宅を含む、公衆が利用できる財及びサービスへのアクセス及び供給

本指令第 4 条により、加盟国は、「人種的又は民族的出自に関連する特性に基づく待遇の相違は、当該特定の職業活動の性質又はそれらが実施される文脈を理由として、当該特性が本質的かつ決定的な職業上の要件となる場合、目的が正当で要件が比例的であることを条件に、差別とはならないと定めることもできる」。

- 雇用と職業における平等な待遇のための一般的枠組みを確立する理事会指令は、雇用と職業に関して、宗教又は信念、障害、年齢、性的指向を理由とする差別と闘うための一般的枠組みを規定する（第 1 条）。また、雇用と職業に関して、上記の理由に基づく直接的又は間接的な差別を禁止する（第 2 条）。この指令は、「公共団体を含む官民両部門に関して、次の事項に関して、すべての人に適用される（第 3 条）。
  - 選考基準及び採用条件を含む、雇用、自営業、職業へのアクセスに関する条件（昇進を含む）
  - 職業指導、職業訓練、高等職業訓練及び再訓練（実務経験を含む）のすべての種類への及び水準のアクセス
  - 解雇及び賃金を含む、雇用及び労働条件
  - 労働者又は雇用者の組織、又は特定の職業を営む者を構成員とする組織への加入及び関与（かかる組織により提供される便益を含む）
  - 社会保障及び医療を含む、社会的保護
  - 社会的利益
  - 教育
  - 住宅を含む、公衆が利用できる財及びサービスへのアクセス及び供給」

  本指令第 4 条により、加盟国は、「人種的又は民族的出自に関連する特性に基づく待遇の相違は、当該特定の職業活動の性質又はそれらが実施される文脈を理由として、当該特性が本質的かつ決定的な職業上の要件となる場合、目的が正当で要件が比例的であることを条件に、差別とはならないと定めることもできる」。

また、個人情報の保護に関する法令として、GDPR を含め以下のような法令が挙げられる。

| 当該法令の名称 | URL | 公的部門と民間部門のいずれを対象とするか |
|---|---|---|
| 欧州連合基本権憲章 | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT | EU の機関、団体、事務所及び当局、並びに加盟国が EU 法を実施する場合にのみ適用される（第 51 条）。 |
| 個人データの取扱いと関連する自然人の保護に関する、及び、そのデータの自由な移転に関する、並びに、指令 95/46/EC を廃止する欧州議会及び理事会の 2016 年 4 月 27 日の（EU）規則 2016/679（GDPR） | http://data.europa.eu/eli/reg/2016/679/2016-05-04 | 両部門が対象となるが、以下の活動は例外となる（第 2 条（b）及び（d））<br>• 欧州連合基本条約第 5 章第 2 節（共通外交・安全保障政策）の範囲に含まれる活動。<br>• 公共の安全に対する脅威の保護及び防止を含め、刑事犯罪の防止、捜査、探知若しくは訴追、又は刑事罰の執行を目的とする所轄官庁による活動（下記参照）。<br><br>EU の機関、団体、事務所及び当局は、GDPR の対象ではないものの、規則 2018/1725（下記参照）の対象となる。 |
| 欧州連合の機関、団体、事務所及び当局による個人データの処理に関する自然人の保護及び当該データの自由な移動に関する 2018 年 10 月 23 日の欧州議会及び理事自動化された規則（EU）2018/1725、並びに規則（EC）No 45/2001 及び決定 No 1247/2002/EC の廃止 | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018R1725 | EU の機関、団体、事務所及び当局のみを対象としている。 |
| 刑事犯罪の防止、捜査、探知、訴追又は刑事罰の執行を目的とする所轄官庁による個人データの処理に関する自然人の保護及び当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会及び理事会指令（EU）2016/680、並びに理事会枠組み決定 2008/977/JHA の廃止（施行指令） | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016L0680-20160504 | 公共の安全に対する脅威の保護及び防止を含む、刑事犯罪の防止、捜査、探知又は訴追、又は刑事罰の執行を目的とした、所轄官庁による個人データの処理を対象とするものである。<br><br>なお、指令は直接適用されるものではなく、加盟国の国内法に組み込む必要がある。 |
| 電子通信分野における個人データの処理及びプライバシー保護に関する 2002 年 7 月 12 日付欧州議会及び理事会指令 2002/58/EC（以下「e プライバシー指令」という。） | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219 | 両部門を対象とする。<br><br>なお、指令は直接適用されるものではなく、加盟国の国内法に組み込む必要がある。 |
| テロ犯罪及び重大犯罪の防止、探知、捜査及び訴追のための旅客名記録（PNR）データの利用に関す | https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L0681 | 両部門を対象とする。 |

| | | |
|---|---|---|
| る 2016 年 4 月 27 日付欧州議会及び理事会指令（EU）2016／681 | | なお、指令は直接適用されるものではなく、加盟国の国内法に組み込む必要がある。 |
| 欧州データガバナンスに関する 2022 年 5 月 30 日付欧州議会及び理事会規則（EU）2022/868 及び規則（EU）2018/1724 の改正 | https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0868 | 両部門を対象とする。 |

# 第3章.　米国（連邦）

## I.　総論

### 1.　個人情報の保護に関する法令

米国では、連邦レベルでの個人情報の保護に関する包括的な法令は存在しない。以下、本章では、2022年6月に下院に草案が提出された、アメリカデータプライバシー保護法 （American Data Privacy and Protection Act, H.R.8152.）[59]（以下「ADPPA」という。）におけるセンシティブデータに関する規律について、報告書作成時点において公表されている ADPPA の草案に基づき検討していく。以下、本章においては、断りのない限り条項についての言及は ADPPA の条項を指すものとする。各論点につき、必ずしも解釈が確立していないため、今後の議論の進展に伴い異なる解釈が裁判所や当局等により採用される可能性があることにも留意されたい。

ADPPA は民間部門を対象としており、公的部門は適用対象から除外されている（第 2 条(9)(B)）。

### 2.　センシティブデータの取扱いに対する規制の趣旨

ADPPA において特にセンシティブデータについて特に規制を加える趣旨を明確に論じる資料は本調査の限りでは見当たらないが、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があるというのが規制が検討された趣旨と考えられる。

## II.　センシティブデータの範囲―総論

### 1.　センシティブデータの範囲一覧

ADPPA の適用対象となるデータ を「対象データ」（covered data）と定義し、そのうえで、その中でも一定のデータを「対象センシティブデータ」（sensitive covered data）と定義している。それぞれの具体的な内容は以下の通りである。

対象データとは、単独で又は他の情報と組み合わせて、個人[60]又は機器[61]であって個人を識別し若しくは個人と合理的に関連付けられうるものを、識別し又はそれらと関連付けられ若しくは合理的に関連付けられうる情報をいい、派生データ（derived data）[62]及び永続的な固有の識別子も含まれうると規定している（第 2 条(8)(A)）。但し、次の情報は対象データに含まれない（第 2 条(8)(A)）。

(i)　非識別化されたデータ

(ii)　従業員データ

(iii)　一般に公開されている情報

(iv)　複数の独立した公開情報源からのみ作成された推知情報（inference）であって対象センシティブデータを明らかにしないもの

---

[59] https://www.congress.gov/bill/117th-congress/house-bill/8152/text
[60] 米国居住の自然人をいう (第 2 条(19))。
[61] 一人又は複数の個人が利用する、対象データを取得、処理、又は移転することができる電子機器をいう (第 2 条(18))。
[62] 個人又は個人の機器に関する事実、証拠又は別の情報源若しくはデータから、情報、データ、仮定、相関関係、推論、予測又は結論を派生させることによって作成される対象データをいう(第 2 条(13))。

対象センシティブデータは、次のいずれかに該当する情報をいうと規定されている（第 2 条(28)(A)）。

(i) 社会保障番号、パスポート番号、運転免許証番号などの政府発行の識別子であって、公の場で表示することが法律上義務付けられていないもの

(ii) 個人の過去、現在若しくは将来の身体的健康、精神的健康、障害、診断、医療状態若しくは治療について記述し、又はこれらを明らかにする情報

(iii) 金融口座番号、デビットカード番号、クレジットカード番号又は個人の所得水準若しくは銀行口座残高を記述し、又はこれらを明らかにする情報。ただし、デビットカード番号又はクレジットカード番号の下 4 桁は、センシティブデータにはあたらない。

(iv) 生体情報

(v) 遺伝子情報

(vi) 正確な地理的位置情報

(vii) ボイスメール、電子メール、テキスト、ダイレクトメッセージ、郵便物などの個人の私的通信又は当該通信の当事者を特定する情報、音声通信、ビデオ通信及び当該通信の送信に関連する情報（通話した電話番号、通話元の電話番号、通話した時間、通話時間、通話当事者の位置情報など）であって、対象事業者又は対象事業者を代理するサービス供給者 （①対象事業者又は連邦、州、部族、地域若しくは地方政府機関のために、その指示により、対象データを取得し、処理し又は移転する個人若しくは団体、又は、②対象事業者又は連邦、州、部族、地域、若しくは地方政府機関から、又はその代理として、対象データを受信する個人又は団体をいう（第 2 条(29)(A)）。以下同じ。）が送信者又は送信者が意図する通信の受領者ではないもの。ただし、雇用主が当該通信にアクセスする可能性があることを明確に通知している場合は、雇用主が従業員に提供するデバイスから、又は当該デバイスとの間で通信が行われるとき、その通信はここでいう「私的通信」にはあたらない。

(viii) アカウント又はデバイスのログイン認証情報、セキュリティコード又はアクセスコード

(ix) 当該情報の取得、処理又は提供に関する個人の合理的な期待に反した方法で、個人の性的行動を特定する情報

(x) 個人の私的利用のために保持されるカレンダー情報、アドレス帳情報、電話又はテキストログ、写真、オーディオ録音又はビデオ。これらの情報が個人のデバイスに保存されているか、デバイスからアクセスでき、別の場所にバックアップされているかは問わない。ただし、これら情報は、雇用主がこれら情報にアクセスする可能性があることを明確に通知している場合は、雇用主が従業員に提供するデバイスから又は当該デバイスに送信されるときは、センシティブデータにはあたらない。

(xi) 個人の裸又は下着姿の私的領域を示す写真、フィルム、ビデオ録画、又はその他の類似のもの

(xii) 第 102 条 (4)に記載されるサービス供給者ではない対象事業者が取得した、個人が要求又は選択したビデオコンテンツを明らかにする情報。ここには、独立したビデオ測定のための提供のためだけに利用される対象データは含まれない。

(xiii) 対象事業者又はサービス供給者が、個人が未成年者であることを認識している場合の、その個人に関する情報

(xiv) 個人の人種、肌の色、民族性、宗教又は労働組合員であること

(xv) 個人のオンライン活動を特定する情報であって、時をまたぎ、第三者のウェブサイトやオンラインサービス間を横断するもの

(xvi) (i)から(xv)で挙げられた種類のデータを特定する目的で取得、処理、又は移転されるその他の対象データ

なお、上記(vii)に言う対象事業者は、原則として、非商業的な文脈で行動する個人を除く、単独又は他者と共同で対象データの収集、処理、転送の目的及び手段を決定する企業又は個人であって、以下のいずれかを満たす者を指し、対象事業者を支配する者、対象事業者に支配される者、又は対象事業者と共通の支配下にあるものを含むと定義されている（第 2 条(9)(A)）。

(i) Federal Trade Commission Act の対象である

(ii) 1934 年 Communications Act、その改正又は補足となる法令の対象となるキャリアである、又は

(iii) 自己又はその構成員の利益のために事業を行うために組織されたものではない組織である

また、上記(xii)にいう、「第 102 条(4)に記載されるサービス供給者」とは、放送テレビサービス、ケーブルサービス、衛星サービス、ストリーミングメディアサービス、又は 1934 年通信法第 713 条(h)(2)(47 U.S.C. 613(h)(2))に記載のその他のビデオ番組サービスをいうと規定され、1934 年通信法第 713 条(h)(2)(47 U.S.C. 613(h)(2))に記載のその他のビデオ番組サービスとは、テレビ放送局による番組、又はテレビ放送局によって提供される番組と一般的に同等とみなされる番組（ただし、消費者生成メディアは含まない）と規定されている。同号にいう「独立したビデオ測定」は ADPPA において特に定義されておらず、その語義は解釈に任されることとなる。

更に、「連邦取引委員会は、合衆国法典 5 編 553 条に基づき、対象データの取得、処理又は移転の新しい方法の結果として、第 2 条(28)(A)(i)から(xvi)までに掲げる対象データと同様のレベルの保護を必要とし得る、他の種類の対象データを対象センシティブデータに含めるための規則を制定できる」との規定も設けられている（第 2 条(28)(B)）。

なお、本調査の限りでは、当局の公表している主要な資料、あるいは学者・有識者・実務家の資料（論文・記事等）において対象センシティブデータの上記のカテゴリーごとに分けてその例、趣旨や範囲等についての個別に具体的に説明した内容は特に見当たらない。

2. センシティブデータを推知させる情報（推知情報）について

センシティブデータを推知させる情報は、センシティブデータに該当する可能性がある。

ADPPA 上、対象データには、他のデータからの推論により生じた派生データ（derived data）も含まれうる（第 2 条(13)。上記 II. 1 参照）。さらに、第 2 条(8)(B)(iv)では、複数の独立した公開情報源からのみ作成された推論のうち、対象センシティブデータを明らかにしないものは、対象データに該当しないと規定している。すなわち、対象センシティブデータに該当する内容を明らかにする推論は、対象データに該当しないものから明確に除外されており、対象センシティブデータを明らかにする推論が対象データに該当することが明らかにされている。本調査の限りではそのような推論が対象センシティブデータに該当するか否かを示す資料等は見当たらなかったが、条文の解釈としては、対象センシティブデータにも該当する可能性があるものと解される。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。

対象センシティブデータを定義する第 2 条(28)(A)は、その(ii)において次の情報が対象センシティブデータに該当することを規定しており、健康に関するデータは通常、この定義に該当するものと解される。

> 「個人の過去、現在若しくは将来の身体的健康、精神的健康、障害、診断、医療状態若しくは治療について記述し、又はこれらを明らかにする情報」

(i) 医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当すると考えられる。

医師等による検査結果は、健康に関する情報の最も典型的な種類といえ、対象センシティブデータの定義に含まれるものと解される。

(ii) 事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する可能性がある。

第 28 条(A)(ii)に定める健康に関するデータについての対象センシティブデータの定義上、健康に関するデータは広くセンシティブデータにあたると解され、その入手方法や入手経路による除外は特に規定されていない。したがって、医師等の判断を介していない、事業者による検査結果が保護の対象外であるとする明文の規定は存在せず、そのような情報もセンシティブデータとして保護される可能性がある。

(iii) 消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する可能性がある。

第 28 条(A)(ii)に定める健康に関するデータについての対象センシティブデータの定義上、健康に関するデータは広くセンシティブデータにあたると解され、その入手方法や入手経路による除外は特に規定されていない。したがって、医師等の判断を介していない、消費者による検査結果が保護の対象外であるとする明文の規定は存在せず、そのような情報もセンシティブデータとして保護される可能性がある。

(iv) 消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する可能性がある。

第 28 条(A)(ii)に定める健康に関するデータについての対象センシティブデータの定義上、健康に関するデータは広くセンシティブデータにあたると解され、その入手方法や入手経路による除外は特に規定されていない。したがって、消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態に関する情報が保護の対象外であるとする明文の規定は存在せず、そのような情報もセンシティブデータとして保護される可能性がある。

(v) 予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無に関する情報がセンシティブデータに該当する可能性がある。

予防接種の接種有無に関する情報が最も関係すると思われるセンシティブデータに関する定義の規定は第 28 条(A)(ii)であるが、そこに挙げられた各項目（身体的健康、精神的健康、障害、診断、医療状態若しくは治療）のいずれかに該当する可能性がある。

(2) 趣旨

ADPPA において特に健康に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、健康に関するデータについては、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

ADDPA においては特に見当たらない。

なお、健康情報について一定の保護に関する規定を設けている他の連邦法が存在する。

例えば、米国保険福祉省は、1996 年医療保険の携行性と責任に関する法律（HIPAA）に基づきプライバシーについての規則を発行している。当該規則は、HIPAA の対象事業者又はその業務提携者が、電子、紙、口頭を問わず、あらゆる形式又は媒体で保有又は移転する一切の「個人特定可能健康情報」（individually identifiable health information）を保護の対象として、個人の健康情報の利用及び開示についての規則を定めている。HIPAA 及び保健福祉省の規則によれば、HIPAA の対象事業者は、同規則が特に認める場合又は本人が書面で許可する場合を除き、保護の対象となる個人特定可能健康情報を使用又は開示することはできないこととされているほか、本人に対するプライバシーに関する一定の事項の通知、並びに本人による開示、修正及び利用制限の請求への対応が必要とされる。保護の対象となる個人特定可能健康情報は、統計データを含む、次に関連する情報であって、個人を特定し、又は個人を特定するために用いられると信じる合理的な根拠があるものをいい、具体的には名前、住所、生年月日、社会保障番号等を含む、多くの一般的な識別子が対象となる（45 CFR § 160.103[63]）。

- 個人の過去、現在又は将来の身体的又は精神的な健康状態又は体調
- 個人に対するヘルスケアの提供
- 個人に対するヘルスケアの提供についての過去、現在又は将来の支払

2. 遺伝子に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、センシティブデータに該当する。

対象センシティブデータを定義する第 2 条(28)では、遺伝子情報（genetic information）がセンシティブデータに含まれることが明記されているところ、この遺伝子情報について、第 2 条(18)が次の通り定義している。

> 「『遺伝子情報』は、その形式にかかわらず、個人の遺伝的特徴に関係するすべての対象データを意味し、以下のものを含む。
>
> (A) 個体の完全な又は抽出されたデオキシリボ核酸 (DNA)の一部の配列決定から得られる生の配列データ
>
> (B) (A)に規定された生の配列データを解析した結果得られる遺伝子型情報及び表現型情報。」

したがって、この定義に該当する遺伝子に関するデータは広くセンシティブデータに該当すると解される。

[63] https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-160

(i)　医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する可能性が高い。

厳密には第 2 条(28)の定義に該当するか否かにより判断されるが、多くの場合、同項の(B)にいう、「解析した結果得られる遺伝子型情報及び表現型情報」に該当すると考えられる。

(ii)　消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する可能性がある。

厳密には第 2 条(28)の定義に該当するか否かにより判断されるが、医師等の判断を介していない、消費者自身による検査の結果であっても、検査の結果といえる限りは、同項の(B)にいう、「解析した結果得られる遺伝子型情報及び表現型情報」に該当すると考えられる。医師等の判断を介していないことから保護の対象外であるとする明文の規定は存在しない。

(iii)　消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当する可能性がある。

厳密には第 2 条(28)の定義に該当するか否かにより判断されるが、医師等の判断や遺伝子検査キットを介していない、消費者自身による検査の結果であっても、検査の結果といえる限りは、同項の(B)にいう、「解析した結果得られる遺伝子型情報及び表現型情報」に該当すると考えられる。医師等の判断や遺伝子検査キットを介していないことから保護の対象外であるとする明文の規定は存在しない。

(2)　趣旨

ADPPA において特に遺伝子情報をセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、遺伝子情報については、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたものと考えられる。

(3)　追加的規律（該当する場合）

ADPPA においては特に見当たらない。

遺伝情報に関する追加的な規律を定める他の連邦法として遺伝子情報差別禁止法（Genetic Information Nondiscrimination Act。以下、「GINA」という。）[64]があり、GINA は遺伝情報の利用等を規制している。なお、GINA における遺伝情報には、個人の遺伝子検査及び個人の家族の遺伝子検査に関する情報並びに個人の家族の疾患又は障碍の発現に関する情報（すなわち家族の病歴）が含まれている（GINA 第 201 条(4)）。これは、家族の病歴は、ある人が将来疾患、障害、身体異常となるリスクが高いか判断するためによく使われることに基づくものであると解される。そのほか、GINA における遺伝情報には、個人による遺伝サービスの要求又は受領、個人又はその家族の遺伝サービスを含む臨床研究への参加、個人又はその家族である妊婦が身ごもった胎児の遺伝情報、生殖保持技術を使用して個人又はその家族が合法的に保有する胚の遺伝情報も含まれる。

[64] https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008

GINA は遺伝情報に基づく差別に焦点を当てて規制を設けており、原則として、対象事業者が遺伝情報を取得することは同法上違法とされ、その禁止に対する限定的な例外として、次の 6 つを規定している（GINA 第 202 条(b)）。

- 遺伝情報の不注意による取得（マネージャーやスーパーバイザーが、誰かが家族の病気について話すのを立ち聞きしたような状況を指す。）
- 使用者（従業員を雇用する者）が任意で提供する健康又は遺伝サービスの一環として入手した遺伝情報（家族の病歴など）
- 従業員が深刻な健康状態にある家族の世話をするために申請する休暇（Family and Medical Leave Act 第 103 条又はそれに類似の州法若しくは州法に基づく、若しくは就業規則に基づく休暇）の認定手続の一環として取得した家族の病歴
- 商業的に公開された文書を通じて取得された遺伝情報。但し、使用者が遺伝情報を発見する目的でそれらの情報源を検索し、又は遺伝情報を取得する可能性のある情報源にアクセスした場合は除く。
- 職場における有害物質の生物学的情報を監視するモニタリングプログラムが法律で義務付けられ、又はそのプログラムが任意であるように慎重に定義された条件の下で行われる場合、そのプログラムを通じて取得された遺伝情報
- 法医学研究所として法執行のために、又は遺体特定のために DNA 検査を行う使用者が獲得した従業員の遺伝情報

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する場合がある。

対象センシティブデータを定義する第 2 条(28)(A)は、その(ix)において次の情報が対象センシティブデータに該当することを規定しており、性生活や性的指向に関するデータも、この定義に該当する限りにおいて、センシティブデータに該当する。

> 「当該情報の取得、処理又は移転に関する個人の合理的な期待に反した方法で、個人の性的行動を特定する情報。」

(2) 趣旨

ADPPA において特に性生活・性的指向に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、性生活・性的指向に関するデータについては、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

特に見当たらない。

なお、連邦法（1964 年公民権法[65]第 7 編等）は、性的志向に基づく差別を一般的に禁ずる。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性 どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する。

第 2 条(28)(A)(xiv)において、個人の労働組合員であることに関するデータが対象センシティブデータに該当することが明確に規定されている。

(2) 趣旨

ADPPA において特に労働組合への加入に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、労働組合への加入に関するデータについて、特に労働組合員であることに関するデータについては、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

特に見当たらない。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性 どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、以下に述べる生体データの定義に該当する限り、センシティブデータに該当する。

対象センシティブデータを定義する第 2 条(28)では、生体データがセンシティブデータに含まれることが明記されているところ、生体データについては、第 2 条(3)が次の通り定義し、生体データに該当するデータと該当しないデータを規定している。

> 「(A) 原則 生体データとは、技術的処理から生成される対象データであって、個人に特有の生物学的、身体的、又は生理学的特徴の、個人とリンクしているか合理的にリンク可能なものを意味し、指紋、声紋、虹彩又は網膜スキャン、顔又は手のマッピング、配置又はテンプレート、及び歩き方又は個人を特定できる身体動作を含む。
>
> (B) 例外 生体データには、デジタル又はフィルム写真、録音又は録画、これらから生成されたデータであって、個人を特定するために使用できないものは含まれない。」

これに従い、自然人を一意に識別することを目的とする生体データは、上記のうち(A)に該当し、かつ(B)に該当しないと解されるため、生体データを構成し、センシティブデータに該当する。

[65] https://www.govinfo.gov/content/pkg/STATUTE-78/pdf/STATUTE-78-Pg241.pdf

(2) 趣旨

ADPPA において特に生体データをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、生体データのうちセンシティブデータに指定されているものは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

特に見当たらない。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータの一部は、センシティブデータに該当する。

対象センシティブデータを定義する第 2 条(28)(A)は、その(iii)において次の情報が対象センシティブデータに該当することを規定しており、金融口座番号、クレジットカード番号等の金融・財産に関するデータは通常、この定義に該当するものと解される。

> 「金融機関の口座番号、デビットカード番号若しくはクレジットカード番号を記述し、又はこれらを明らかにする情報。ただしデビットカード番号又はクレジットカード番号の各下 4 桁は、センシティブデータとはみなされないものとする。」

(2) 趣旨

ADPPA において特に金融・財産に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、金融・財産に関するデータのうちセンシティブデータに指定されているものは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

ADPPA 上は特に見当たらない。

他の連邦法として、グラム・リーチ・ブライリー法としても知られる 1999 年金融サービス現代化法[66]がある。同法第 5 章には、銀行、証券会社、保険会社等の金融機関その他金融商品及びサービスを提供する会社に、顧客の金融のプライバシーを保護するための措置をとることを義務付けている（同法第 5 章 A 節）ほか、個人や企業が偽計を用いて金融機関の顧客情報（金融機関によって、又は金融機関のために維持されるあらゆる情報のうち、金融機関と金融機関の顧客との間の関係に由来し、かつ顧客と識別されるもの。同法第 527 条(2)）へアクセスすること等禁止されている（同法第 5 章 B 節）。同法を執行する連邦機関の一つに米国連邦取引委員会があり、同委員会は、金融分野におけるプライバシーに関する規則を定めている。同規則では、顧客の個人情報をどのように収集及び開示するべきかが定められて

[66] https://www.govinfo.gov/content/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

いる。また、同委員会が公表するセーフガード規則では、金融機関に、顧客情報を保護するためのセーフガード（安全管理措置）の維持を義務付ける。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータのうち、個人の所得水準又は口座残高についての情報は、センシティブデータに該当する。第 2 条(28)(A)(iii)において、個人の所得水準又は口座残高についての情報が、明確にセンシティブデータの定義に含まれている。

(2) 趣旨

ADPPA において特に信用に関する情報をセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、信用に関するデータは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

ADPPA 上は特に見当たらない。

但し、公正信用報告法（FCRA）[67]は信用情報機関、医療情報会社、入居審査サービスなど、一定の情報収集機関によって収集された個人の信用に関する情報の保護について定めている。信用に関する情報の入手方法についても定めており、具体的には、対象となる情報収集機関は、原則として、消費者報告（consumer report、個人の与信や保険、雇用等への適格性の判断の目的で利用される、個人の信用度等を報告するもの。口頭による報告も含まれる。FCRA 第 603 条(d)）に記載された情報を、与信、保険や雇用といった、同法に明記された目的以外の目的で第三者に提供することはできない（FCRA 第 604 条(a)）。また、対象となる情報収集機関が、使用者等に、その従業員又は求職者の消費者報告を提供できる条件についても、その情報の取得について本人にあらかじめ通知がなされていることといった要件を課している（同条(b)）。

さらに、債権回収に関しては、公正債権回収法（Fair Debt Collection Practices Act。債権回収者による多くの詐欺的、不誠実、不公正、不合理な債権回収行為を禁止する法律）[68]が、信用調査機関への伝達等のいくつかの限られた例外を除き、債権回収業者による債権回収に関する情報の第三者への開示を禁止している（同法第 805 条(b)）。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。

[67] https://uscode.house.gov/view.xhtml;jsessionid=E1A1F8C0E8A0AD512BB47D8A2F966223?req=granuleid%3AUSC-prelim-title15-chapter41-subchapter3&saved=%7CKHRpdGxlOjE1IHNlY3Rpb246MTY4MWEgZWRpdGlvbjpwcmVsaW0p%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim
[68] https://www.ftc.gov/legal-library/browse/rules/fair-debt-collection-practices-act-text#805

(2) 趣旨

ADPPA において特に政府等の金銭的保護を受けている事実に関するデータをセンシティブデータとして保護しないことの趣旨を明確に論じる資料は本調査の限りでは見当たらないが、政府等の金銭的保護を受けている事実に関するデータは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高いとまではいえず、他の対象データと同程度の規制を及ぼせば足りると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

ADPPA においては特に該当する追加的規律はない。

家族教育権及びプライバシー法（FERPA）[69]は、連邦の資金提供を受ける機関が、学生の書面による明確な同意なしに、教育記録に含まれる個人を特定できる情報の他者への開示を一般的に禁止している（FERPA 第 99.30 条）。ただし、経済援助の適格性、援助の額及び援助条件を決定するため、又は援助の規約の執行のために必要な場合等は例外とされている（同法第 99.31 条(a)(4)）。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、センシティブデータに該当しない。ただし、精神的健康など、健康に関するデータ（上記 III. 1）を推論させるものとして、センシティブデータに該当する可能性はある（上記 II. 2 参照）。

(2) 趣旨

ADPPA において特に成年後見制度の保護を受けている事実に関する情報をセンシティブデータとして保護しないことの趣旨を明確に論じる資料は本調査の限りでは見当たらないが、成年後見制度の保護を受けている事実に関するデータは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高いとまではいえず、他の対象データと同程度の規制を及ぼせば足りると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

該当する追加的規律は特に見当たらない。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

[69] https://studentprivacy.ed.gov/node/548/

児童に関する情報は、センシティブデータに該当する。但し、対象事業者又はサービス供給者が、個人が「対象未成年者」（17 歳未満の個人をいう（第 2 条(11)）。以下同じ。）であることを認識している場合における、その個人に関する情報に限る（第 2 条(28)(A)(xiii)）。

ここにいう「認識」とは、事業者の種類に応じて、以下の通り定義されている（第 2 条(20)(A)）。

「(i) 影響力の大きいソーシャルメディア企業（定義は下記の通り）に関しては、その事業者が、その個人が対象未成年者であることを知っていたか、又は知るべきであった状態

(ii) 大規模データ保有者（定義は下記のとおり。以下同じ。）であり、かつ影響力の大きいソーシャルメディア企業ではない対象事業者又はサービス供給者に関しては、対象事業者が、その個人が対象未成年者であるという事実を知っていたか、故意に無視して行動していた状態

(iii) (i)又は(ii)の要件を満たさない対象事業者又はサービス供給者については、実際に知っていた状態」

影響力の大きいソーシャルメディア企業は、以下の通り定義されている（第 2 条(20)(B)）。

「インターネットでアクセス可能なプラットフォームを提供する対象事業者であって、

(i) その年間収入が 300 万ドル以上であり

(ii) 当該プラットフォームは、当該対象事業者のオンライン製品又はサービスにおいて、過去 12 ヶ月のうち 3 ヶ月以上、月間アクティブユーザーが 3 億人以上であり、かつ

(iii) 当該プラットフォームが、主にユーザーがユーザー生成コンテンツにアクセス又は共有するために使用するオンライン製品又はサービスであること。」

大規模データ保有者は、以下の通り定義されている（第 2 条(21)）。

「(A) 原則。大規模データ保有者とは、直近の暦年において、以下に該当する対象事業者又はサービス供給者をいう。

(i) 年間総収入が 2 億 5,000 万ドル以上であり、かつ、

(ii) 以下の対象データを取得、処理又は移転するもの。

(I) 500 万人以上の個人又は 1 人以上の個人の識別、関連付け若しくは合理的な関連付けが可能な機器の対象データ。ただし、個人により要求された製品又はサービスの開始、提供、請求、最終決定、完了又はその他の支払回収を目的としてのみ取得及び処理される対象データを除く。

(II) 20 万人以上の個人又は 1 人以上の個人の識別、関連付け又は合理的な関連付けが可能な機器のセンシティブデータ

(B) 例外。大規模データ保有者には、対象事業者又はサービス供給者が、以下のいずれかを取得又は処理することのみを理由として大規模データ保有者に該当するような場合は含まれない。

(i) 個人の電子メールアドレス

(ii) 個人の電話番号

(iii) 個人又は機器が、対象事業者又はサービス供給者が管理するアカウントにログインするための、個人又は機器のログイン情報」

(2) 趣旨

ADPPA において特に児童に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、児童に関するデータは、その漏えいや不正利用が生じた場合、児童に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

ADPPA 上、児童及び未成年者の対象データ（対象センシティブデータを含む）について適用される追加的な規律として、データ保護措置（第 205 条）がある。その具体的な内容は以下の通りである。

(a) 児童及び未成年者へのターゲティング広告の禁止 - 対象事業者は、対象事業者が個人が対象未成年者であることを認識している場合、そのようないかなる個人に対してもターゲティング広告を行ってはならない。

(b) 対象未成年者に関連するデータの移転のための要件

(1) 原則　対象事業者は、以下の場合、対象未成年者の対象データを第三者に移転又はその指示をしてはならない。

(A) 個人が対象未成年者であることを認識しており、かつ、

(B) 対象未成年者又は対象未成年者の親若しくは後見人から積極的な明示的同意[70]を得ていない場合。

(2) 例外　対象事業者又はサービス供給者は、法執行機関又は行方不明児童又は児童からの搾取に関する問題に関して被害者、家族、児童サービス専門家及び一般市民に支援を提供するために議会で指定された非営利の全国リソースセンター並びにクリアリングハウスに児童の被害に関する情報を提出するためにのみ、対象事業者又はサービス供給者が 18 歳未満と認識している個人の対象データを取得、処理及び移転できる。

ADPPA のほかに、1998 年児童オンラインプライバシー保護法（COPPA）[71]は、13 歳未満の児童向けのウェブサイト又はオンラインサービスの運営者その他 13 歳未満の児童からオンラインで個人情報を収集していることを知っているウェブサイト又はオンラインサービスの運営者に対し、一定の義務を課している。具体的には以下のような規定が COPPA 及びその規則（Children's Online Privacy Protection Rule、以下「COPP 規則」という。）[72]において定められている。

- COPPA の対象となる事業者は、13 歳未満の児童からオンラインで収集する個人情報をどのように取り扱うかを明確かつ包括的に記述したプライバシーポリシーを掲示しなければならない（COPPA 第 6502 条(b)(1)(A)(i)）。
- COPPA の対象となる事業者は、児童から情報を収集する前に、事業者の情報取扱いについて保護者に直接通知しなければならない（COPP 規則第 312.4 条(b)）。
- 児童の個人情報を収集し、利用し、又は開示する前に、COPPA の対象となる事業者は、保護者の検証可能な同意を取得しなければならない（COPPA 第 6502 条(b)(1)(A)(ii)）。

[70] 「積極的な明示的同意」とは、一定の要件を満たす対象事業者からの具体的な要請に応じ、情報提供を受けた後に、ある行為又は慣行について、個人が自由に与えた（freely given）、特定の（specific）、かつ不明確ではない(unambiguous)承認を明確に伝える、個人による積極的な行為をいう（第 2 条(1) (A) ）。

[71] http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter91&saved=%7CZ3JhbnVsZWlkOlVTQy1wcmVsaW0tdGl0bGUxNS1zZWN0aW9uNjUwMQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim

[72] https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312

- COPPA の対象となる事業者は、要求する保護者に対し、児童から収集した個人情報を確認する方法、同意を取り消し児童の個人情報の将来の利用及び収集を拒否する方法並びに児童の個人情報を削除する方法を提供しなければならない（COPP 規則第 312.3 条(c), 同 312.6 条(a)(2)）。
- COPPA の対象となる事業者は、児童から収集した個人情報の機密性、セキュリティ及び完全性を保護する合理的な手続を確立し、維持しなければならない（COPPA 第 6502 条(b)(1)(D)）。

11. オンライン行動履歴（ウェブサイトの閲覧履歴等）に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴（ウェブサイトの閲覧履歴等）に関する情報は、センシティブデータに該当する場合がある。具体的には、個人のオンライン行動を特定する、長期的かつ第三者のウェブサイト又はオンラインサービスにわたる情報が該当することが、対象センシティブデータの定義（2 条(28)(A)(xv)）により明らかにされており、これに該当する限りはセンシティブデータに該当する。

(2) 趣旨

ADPPA において特にオンライン行動履歴に関するデータをセンシティブデータとして保護する趣旨を明確に論じる資料は本調査の限りでは見当たらないが、オンライン行動履歴に関するデータは、その漏えいや不正利用が生じた場合、個人に重大な損害が生じる可能性が高く、他の対象データに比べより強度な規制を及ぼす必要があると判断されたからだと考えられる。

(3) 追加的規律（該当する場合）

本調査の限りでは特に見当たらない。

IV.　センシティブデータの取扱いに適用される規律

1. 取得

ADPPA 上、データの最小化の原則が規定されており、対象データについては、データ主体からの要求に基づく商品やサービスの提供又は ADPPA 第 101 条(b)に定められる所定の目的に合理的に必要かつ適切な場合（reasonably necessary and proportionate）、対象データを取得、処理又は移転できる（第 101 条(a)）。

さらに対象センシティブデータについては、その対象センシティブデータが、データ主体である個人が要求した特定の製品又はサービスの提供又は維持のために不可欠な場合、又は以下のいずれかの目的（第 101 条(b)(1)から(12)、(14)及び(15)）を実現するために確実に必要（strictly necessary）な場合にのみ、取得又は処理ができる（第 102 条(2)）。

「第 101 条(b)

(1) 請求、発送、配送、保管や会計など、関連する日常的な管理、運営、アカウントサービス活動を含む、個人によって要求された特定の製品又はサービスに関する取引の開始、管理、完了又は注文の履行

(2) 過去に本法律に従い取得された対象データについては、 (1)の例外にかかわらず、以下の目的

(A) システムの保守又は診断を行うために必要なデータの処理

(B) そのデータが取得された製品又はサービスの開発、維持、修理又は強化

(C) そのデータが取得された製品又はサービスを改善するための内部調査又は分析

(D) 在庫管理又は合理的なネットワーク管理の実施

(E) スパム対策

(F) そのデータが取得された製品若しくはサービスの機能を損なうエラーのデバッグ又は修復

(3) 製品又はサービスの利用者認証

(4) 製品又はサービスの保証の履行

(5) セキュリティインシデントの防止、検出、保護又は対応。本号において、セキュリティとは、不法占有、不法侵入及び医療に関する警告、火災警報並びにアクセスコントロール及びアクセスセキュリティを含む、ネットワークセキュリティ、物理的セキュリティ及び生命に関する安全性をいう。

(6) 詐欺、ハラスメント又は違法行為の防止、検出、保護又は対応のため。本号において、違法行為とは、重罪又は軽犯罪として処罰される連邦法、州法又は地方法の違反であって、直接的に危害を加えることができるものをいう。

(7) 連邦法、部族法、地方法若しくは州法により課された法的義務の遵守、又は対象事業者若しくはサービス供給者が関わる法律上の請求についての調査、立証、準備、行使、又は防御

(8) 個人若しくは個人の集団が、死亡、重大な身体的傷害又はその他の重大な健康上の危険にさらされていると対象事業者又はサービス供給者が誠実に判断する場合に、個人又は個人の集団がそれら損害を被ることの防止

(9) 連邦法又は州法に基づく製品のリコールの実施

(10) (A) 公的又は査読付きの科学的、歴史的又は統計的研究プロジェクトの実施で以下を両方を満たすもの

(i) 公益に資するものであること

(ii) 被験者保護のための規制を含む、その研究に適用されるすべての関連法令を遵守しているか、又は施設内倫理委員会の基準が免除されていること

(B) （翻訳省略。連邦取引委員会が将来的にガイドラインを発行すべきことを定める規定）

(11) 個人に対する、広告ではないコミュニケーション。ただし、そのコミュニケーションが、個人と対象事業者との相互作用の文脈の中で、個人によって合理的に予想されるものである場合に限る。

(12) 個人とそれ以外の者との間におけるコミュニケーションであって、その個人の指示によるもの

(13) 略（企業の合併や倒産処理等を目的とする対象データの移転を定めるものであるが、第102条(2)において本号が引用されていない。但し、第三者提供に関し、下記3を参照）

(14) 第208条規定の、対象データのデータセキュリティ及び完全性の確保。

(15) 過去に本法律に従い取得された対象データに関して、法令で許される範囲内において、政府の指示により活動するサービス供給者又は対象事業者が政府機関に提供するサービスによる、不法侵入、自然災害又は国家安全保障上の事件を含む公共安全上の事件の防止、検

出、保護又は対応。ただし、本条項は、政府に対する支払又はその他の有償的対価のために、対象データを移転することを許すものではない。

2. 利用

対象センシティブデータを取得するにあたって適用される規律と同じ規律が適用される(上記設問 IV. 1 参照)。

3. 第三者提供

対象センシティブデータは、第 102 条(3)に定める場合にのみ、第三者に提供することができる。この規律は、上記 1 において述べた規律に加えて適用される。

第 102 条(3)に定める場合とは、以下の通りである。

(A) 個人の積極的な明示的同意に基づき移転が行われる場合

(B) 連邦法、部族法、地方法若しくは州法により課された法的義務の遵守、又は対象事業者若しくはサービス供給者が関わる法律上の請求についての調査、立証、準備、行使又は防御のために移転が必要である場合

(C) 対象事業者の誠実な考えによれば、個人が死亡、重大な身体的傷害又は重大な健康上の危険にさらされており、個人をそれらの差し迫った危険から守るために移転が必要である場合

(D) 過去に本法律に従い取得された対象データに関して、法令で許される範囲内において、政府の指示により活動するサービス供給者又は対象事業者が政府事業者に提供するサービスによる、不法侵入、自然災害又は国家安全保障上の事件を含む公共安全上の事件の防止、検出、保護又は対応のために移転が必要である場合。ただし、本条項は、政府に対する支払い又はその他の有価的対価のために、対象データを移転することを許すものではない。

(E) パスワードを提供する場合であって、指定されたパスワードマネージャーを使用する必要があるとき、又はサイトやアカウント間をまたいで繰り返し利用されているパスワードを特定することのみを目的とし対象事業者に移転されるとき

(F) 遺伝子情報の移転の場合であって、個人から特に要求された医学的診断又は治療を行うとき、又は第 101 条(b)(10)の規定に従って医学的研究を行うために必要であるとき

(G) 第 101 条(b)(13)に記載された方法で資産を譲渡する場合

第 101 条(b)(13)は、次の通り定めている。

合併、買収、破産、又は類似の取引において、第三者が対象事業者の資産の全部又は一部を管理することになった場合における、資産の第三者への移転であって、対象事業者がそのような移転の前に合理的な時間内に、影響を受ける各個人に以下の両方を提供する場合

(A) 第 202 条に記載されているように、自身の対象データを受け取る事業者又は団体の名称及びそのプライバシーポリシーを含む、当該移転を説明する通知

(B) 個人の対象データに関連する本法に基づく積極的な明示的同意の要件に従って、以前に与えられた同意を撤回する合理的な機会、及び第 203 条に記載されている通り自身の対象データの削除を要求する合理的な機会

4. 管理

センシティブデータの管理に関する特有の規律は見当たらない。

5. 漏えい等

センシティブデータに関する特有の規律は見当たらない。

6. 請求権

センシティブデータに関する特有の規律は見当たらない。

## V. 本人同意、プロファイリング

### 1. 本人同意

#### (1) センシティブデータ規制（上記III）との関係

センシティブデータ規制（上記III）との関係では、対象センシティブデータの移転について、本人同意が必要とされている。

ADPPA 上、センシティブデータの取得又は処理は原則として禁止されており（第 102 条柱書）、例外として、そのセンシティブデータが、データ主体たる個人が要求した特定の製品又はサービスの提供又は維持のために不可欠な場合、又は法令上列挙された目的を実現するために不可欠な場合にのみ許容される（第 102 条 (2)、上記設問 IV. 1 参照）。センシティブデータの移転については、さらに加えて、個人の積極的な明示的同意（affirmative express consent）が必要となる（第 102 条(3)(A)）。

#### (2) 要件一般

ADPPA 上の同意に関する定めとしては、「積極的な明示的同意」についての定義規定が存する。「積極的な明示的同意」とは、一定の要件を満たす対象事業者からの具体的な要請に応じ、情報提供を受けた後に、ある行為又は慣行について、個人が自由に与えた（freely given）、特定の（specific）、かつ不明確ではない（unambiguous）承認を明確に伝える、個人による積極的な行為をいう（第 2 条(1) (A)）（上記設問 III. 10 (3) 参照）。

#### (3) 情報提供

センシティブデータを取り扱うにあたってデータ主体たる個人の同意を取得する必要がある場合、その同意の要求に際し、対象事業者は以下の情報を提供する必要がある（第 2 条(1)(B)(ii)ないし(vii)）。

> 第 2 条(1)(B)
>
> (ii) 個人の同意が求められる処理目的の説明、及び、
>
> (I) 処理目的を実現するために必要な、対象事業者が取得、処理、移転する対象データの種類の明示

(II) 目立つ見出しを含み、合理的な個人が、同意を求める処理目的及びその処理目的のために対象事業者が取得、処理又は移転する対象データを特定し理解できるような分かりやすい記載

(iii) 同意に関連し、個人に付与される権利についての明確な説明

(iv) その要求が、障害者にとり合理的な方法でアクセスでき、使用可能な方法でなされていること

(v) その要求が、承認（authorization）を求める製品又はサービスが提供される各対象言語により利用できるようにされていること

(vi) 同意を拒否するという選択肢が、少なくとも同意するという選択肢と同程度に目立つものとされ、同意を拒否するという選択にかかるステップが、同意するという選択にかかるステップと同じステップ数かそれ以下のステップ数であること

(vii) 積極的な明示的同意に基づき取得された対象データを、明示的同意が得られた処理目的とは異なる処理目的で処理又は移転する場合は、その異なる処理目的について改めて積極的な明示的同意を得ていること

(4) 形式

形式につき、第 2 条(ii)及び(iv)から(vi)において一定の要件が定められている（上記設問 V. 1 (3)参照）。

また、以下のとおり、黙示的な同意及び推定された同意は許容されない（第 2 条(C)）。

(C) 明示的同意の必要性 - 対象事業者は、個人の不作為又は対象事業者が提供するサービス又は製品の個人による継続的利用から、その個人がある行為又は実務に明示的同意を与えたと推定することができない

さらに、以下のような方法による、偽りの同意（pretextual consent）も許容されない（第 2 条(D)）。

(D) 偽りの同意の禁止 - 対象事業者は、以下の方法で個人の積極的な明示的同意を得ること、又は得ようとすることができない

(i) 虚偽、架空、詐欺又は著しく誤解を招く記述や表現の利用

(ii) 合理的な個人の自律性、意思決定若しくは当該同意や対象データを提供するための選択を難解にし、混乱させる若しくは損なう目的又は実質的な効果を有するユーザーインターフェースの設計、修正又は操作

(5) 個別同意の必要性

ADPPA 上は必ずしも明らかではない。ただし、「積極的な明示的な同意」については特定性（specific）の要件があるほか、同意取得に際し提供する必要がある情報（上記設問 V. 1 (3)）及び同意取得の形式（上記設問 V. 1 (4)） の規定によれば、明示性、アクセシビリティ、理解容易性、操作の簡便性が実現されることも必要であり、仮に一括して同意を取得する場合でもこれらの要件が満たされる必要がある。

(6) 同意撤回

ADPPA 上、次のように同意の撤回をする手段を本人に提供することが対象事業者に義務付けられており、同意の撤回が認められている（第 204 条）。

(a) 同意の撤回 - 対象事業者は、ある個人の対象データの処理又は移転に関して、その個人によって以前に提供された積極的な明示的同意を撤回するための明確かつ目立つ簡便な手段であって、同意を提供する手段と同様に合理的な個人にとって簡便な手段を、その個人に提供するものとする。

(7) その他留意事項

その他留意すべき規定として、次のような規定が挙げられる。

第 204 条

(b) 第三者への対象データ移転時のオプトアウト権

(1) 原則

(A) 個人が移転に反対する場合、個人の対象データを第三者に移転してはならず、移転を指示してもならない。

(B) 第 210 条に定めるとおり、オプトアウトメカニズムにより、個人がその移転に反対することを認めるものとする。

(2) 例外 –第 206 条(b)(3)(C)に定める場合（連邦取引委員会が ADPPA に基づき設けることとされている「Do Not Collect」登録簿と呼ばれる、個人が一定の対象データの消去等を容易に求めることができる仕組みの対象となる場合を指す）を除き、対象事業者は、第 101 条(b)(1)から(15)の例外（上記 IV.1 参照）に従って行われる対象データの取得、処理又は移転については、その個人によるオプトアウトを許す必要はない。

2. プロファイリング

(1) プロファイリング・データ分析に対する規律

以下のとおり、プロファイリングその他のデータ分析という処理行為は、大規模データ保有者による、「対象アルゴリズム」（covered algorithm）の利用として、次の規律が適用される可能性がある（第 2 条）。

第 2 条(7) 対象アルゴリズム - 「対象アルゴリズム」とは、機械学習、自然言語処理、人工知能技術又は類似若しくはそれ以上の複雑性を有する他の計算処理技術を利用し、製品又はサービスの提供を決定するため、又は個人に対する情報の配信若しくは表示のランク付け、順序付け、促進、推奨、強化など、対象データに関して決定を行う、又は人間の意思決定を容易にする計算プロセスをいう。

第 207 条(c) 対象アルゴリズムの影響及び評価

(1) 対象アルゴリズムの影響

(A) 影響評価 ― 本法律の他の規定にかかわらず、本法律の制定日から 2 年以上経過してから、その後毎年、個人又は個人の集団に結果的に損害を与えるリスクをもたらす方法で対象アルゴリズムを利用し、対象データを取得、処理、移転するために、当該対象アルゴリズムを単独又は部分的に利用している大規模データ保有者は、(B)に従って当該アルゴリズムの影響評価を実施するものとする。

(B) 影響評価の範囲 — (A)に基づき必要とされる影響評価では、以下のものを提供するものとする。

(i) 対象アルゴリズムの設計プロセス及び方法論の詳細な記述

(ii) 対象アルゴリズムの目的及び提案される利用についての記述

(iii) 入力として処理されるデータの種類、及び該当する場合、対象アルゴリズムが依拠するモデルの訓練に使用されるデータを含む、対象アルゴリズムが利用するデータの詳細な記述

(iv) 対象アルゴリズムが生成する出力の説明

(v) 対象アルゴリズムの必要性と比例性についての、その記載された目的との関連における評価

(vi) 大規模データ保有者が、対象アルゴリズムが個人又は個人の集団に及ぼす潜在的な危害を軽減するために講じた、又は講じる予定の措置の詳細な説明(以下の関連事項を含むものとする)

(I) 対象未成年者

(II) 住宅、教育、雇用、医療、保険又は信用機会のための広告の作成若しくは促進又は利用の決定若しくは制限

(III) 公共宿泊施設へのアクセス又は利用制限の決定。特に、これらによる損害が、人種、肌の色、宗教、国籍、性別又は障害を含む個人の保護されるべき特質に関連するものであること

(IV) 個人の人種、肌の色、宗教、国籍、性別又は障害の状態に基づく格差のある影響

(V) 個人の所属政党に基づく不利な影響

(2) アルゴリズム設計の評価 — 本法律の他の規定にかかわらず、本法律の制定日から遅くとも 2 年以内に、結果的な決定を促進するために対象データを取得、処理、又は移転するために、単独又は部分的に設計された対象アルゴリズムを意図的に開発する対象事業者又はサービス供給者は、対象アルゴリズムを州をまたぐ商取引に展開する前に、対象アルゴリズムの開発に利用されたあらゆる訓練データを含む当該アルゴリズムの設計、構造、入力を、(1)(B) で特定した潜在的危害のリスクを低減するために評価しなければならない。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリング・データ分析により生成されたデータは、それが対象データであれば、センシティブデータに該当する可能性は否定できない。

センシティブデータを特定する目的で取得、処理、又は移転されるその他の対象データもセンシティブデータに含まれる（上記 II. 2 参照）。この「取得」（collection）は、購入、貸与、収集、取得（obtaining）、受信、アクセス、その他あらゆる手段による対象データの入手をいう（第 2 条(4)）。このため、評価結果データの生成も「取得」に含まれ、プロファイリング・データ分析により生成されたデータもセンシティブデータに該当する可能性がある。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

上記 V. 2 (2)記載のとおり、プロファイリング・データ分析により生成されたデータもセンシティブデータに該当する可能性がある。該当する場合は、センシティブデータの取得に係る規律（上記 IV. 1）が適用されるものと考えられる。

## VI. センシティブデータの取扱いに係る裁判例・決定等

ADPPA は 2023 年 1 月 1 日時点において成立もしくは施行されていないため、注目すべき裁判例や政府の決定は存在しない。なお、本調査時点では、ADPPA 自体の法案成立に向けた進捗は乏しく、制定は未知数である。

なお、ADPPA を巡る議論状況としては、本調査時点では、超党派の支持を得ているものの、センシティブデータの取扱いとの関係では、ADPPA が原則として州法以下の法令に優越すること（第 404 条(b)(1)。なお、反対に州法が ADPPA に対して優越する事例については、同条(b)(2)の例外規定による。）に懸念を示す声がある。カリフォルニア州の検事総長は、他の 9 つの州の検事総長との連名の書簡を議会に送り、ADPPA がプライバシー権に「底」ではなく「天井」を設定するものであると批判した。これらの州の検事総長は、州が独自のプライバシー法を採用することを認めるべきであり、それによって技術や実務の変化に対応した立法を行うことができると主張している。

現在、米国におけるプライバシー及びデータセキュリティ領域の規制については、連邦取引委員会（Fair Trade Commission （FTC）、アメリカにおける消費者保護及び競争法の執行権限を与えられた連邦機関）に大きく依っている。FTC の主要な執行手段は、FTC 法第 5 条（15 U.S.C. § 45(a)(1)）を根拠としている。FTC 法はセンシティブデータ自体について特に議論又は規律するものではないものの、同法に基づき、個人情報の処理が FTC 法の違反に該当するとして巨額の罰金が課されたり、違反について一定の対応をとるべき内容の合意が FTC と事業者の間でなされる実例も見られている。

加えて、司法省（DOJ）もサイバーセキュリティ領域の規制を行う。DOJ は、連邦刑法に違反した者を訴追する権限を有する。データ漏洩事案を隠蔽することで司法妨害及び重罪隠匿に関する法律に違反したとの嫌疑で、米国企業の前最高セキュリティセキュリティ責任者に対して DOJ が刑事訴追を行った事案もある。

## VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

個人情報の保護に関する包括的な連邦法の代わりに、特定の産業に適用されるプライバシーに関連する法令が多数存在する。もっとも、これらの法律は、上記の FTC による規律と同様に、「センシティブデータ」そのものを議論又は規律していない。以下では、個人情報の保護又はサイバーセキュリティに関連する義務を課す規定を有する連邦法とそれに基づき施行された規則の例を示している。

| **法令の名称及び URL** | **URL** | 適用対象（公的部門・民間部門） |
|---|---|---|
| 消費者オンラインプライバシー法案(Consumer Online Privacy Rights Act) (COPRA) | https://www.congress.gov/bill/117th-congress/senate-bill/3195/text<br><br>対象事業者は、事前の積極的明示的同意なしに、センシティブデータを処理又は移転してはならず、個人にその同意を撤回するための簡便な手段を提供しなければならない。 | [適用対象：民間部門]<br>ADPPA による規律は他の連邦法による規律に影響を及ぼさない(ADPPA 404 条(a)(1) (C))。<br>したがって、ADPPA による規律は COPRA による規律に影響を及ぼさないものと考えられる。 |
| 医療保険の携行性と責任に関する法律(Health Insurance | https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf | [適用対象：民間部門及び公的部門]<br>ADPPA による規律は、208 条を除く ADPPA の要件を充足する限り、 |

| | | |
|---|---|---|
| Portability and Accountability Act of 1996) (HIPAA) | データ保持者は、保護対保健情報(PHI)につき、プライバシールールにより許容若しくは要求される場合、又はその個人が書面により許可を得た場合にのみ開示又は使用できる。また、合理的かつ適切な行政的、技術的及び物理的措置により、電子化された PHI を保護しなければならない。 | HIPAA による規律に影響を及ぼさない (ADPPA 404 条(a) (3))。 |
| 遺伝情報差別禁止法（Genetic Information Non-discrimination Act of 2008） (GINA) | https://www.eeoc.gov/statutes/genetic-information-nondiscrimination-act-2008<br><br>雇用者が雇用、解雇、配置、昇降格を決定する際、個人の遺伝情報の利用を禁止する。 | [適用対象：民間部門及び公的部門]<br>ADPPA による規律は、208 条を除く ADPPA の要件を充足する限り、GINA による規律に影響を及ぼさない (ADPPA 404 条(a)(3))。 |
| 児童オンラインプライバシー保護法(Children's Online Privacy Protection Act of 1998) (COPPA) | https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312<br><br>児童を対象としたウェブサイト若しくはオンラインサービスの運営者又は児童から個人情報を取得し又は管理していることを実際に知っている運営者は、(1)児童から取得する情報の利用及び開示方法について、ウェブサイト又はオンラインサービス上で告知し、(2)取得、利用及び/又は開示する前に、検証可能な親の同意を得て、(3)親が児童から取得した個人情報を確認し、それ以上の利用又は維持を拒否するための合理的な手段を提供し、(4)児童の参加に際し、活動への参加に合理的に必要な以上の個人情報の開示を条件としてはならず、(5)児童から取得する個人情報の機密性、安全性及び完全性を保護するための合理的な手順を確立し、維持しなければならない。 | [適用対象：民間部門]<br>ADPPA のいかなる規定も、COPPA に基づき対象事業者又はその他の者が負う可能性がある義務を緩和又は変更するものと解釈してはならない (406 条(a))。<br>したがって、ADPPA による規律は COPPA による規律に影響を及ぼさないものと考えられる。 |
| グラム・リーチ・ブライリー法（The Gramm Leach Bliley Act (GLBA) | http://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter94&edition=prelim | [適用対象：民間部門] |

| | | |
|---|---|---|
| | 銀行及び金融機関により収集される個人情報に適用される。 | |
| 公正信用報告法（The Fair Credit Reporting Act (FCRA)）、 | http://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter41/subchapter3&edition=prelim<br><br>信用情報の収集及び利用を規制する。 | [適用対象：民間部門及び公的部門] |
| 1974 年プライバシー法（The Privacy Act of 1974） | https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf<br><br>連邦機関により記録システムで保管される個人情報の収集、保管、利用及び流布に適用される公正な情報実務規程を定める。 | [適用対象：公的部門] |
| 家族教育権及びプライバシー法（The Family Educational Rights and Privacy Act (FERPA)） | http://uscode.house.gov/view.xhtml?path=/prelim@title20/chapter31/subchapter3/part4&edition=prelim<br><br>学生の個人情報を規制・保護する。 | [適用対象：民間部門及び公的部門] |
| 1994 年ドライバープライバシー法（The Driver's Privacy Protection Act of 1994 (DPPA)） | http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter123&edition=prelim<br><br>州車両管理局が収集する個人情報のプライバシー及び開示に適用される。 | [適用対象：公的部門] |
| 1984 年ケーブル通信政策法（The Cable Communications Policy Act of 1984） | http://uscode.house.gov/view.xhtml?path=/prelim@title47/chapter5/A&edition=prelim<br><br>通信サービス利用者のプライバシー保護を含む。 | [適用対象：民間部門及び公的部門] |
| ビデオプライバシー保護法（The Video Privacy Protection Act (VPPA)） | http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter121&edition=prelim<br><br>オンラインストリーミングを含むビデオその他の AV 資料のレンタル又は販売記録の開示を制限する。 | [適用対象：民間部門] |
| 公正債権回収法（The Fair Debt Collection Practices Act (FDCPA)） | https://uscode.house.gov/view.xhtml?req=(title:15%20section:1692a%20edition:prelim) | [適用対象：民間部門] |

| | | |
|---|---|---|
| | 他人のために債権回収を試みる第三債権回収者の行動を制限する。 | |

## 第4章.　米国（カリフォルニア州）

### I.　総論

#### 1.　個人情報の保護に関する法令

カリフォルニア州では、カリフォルニア消費者プライバシー法（California Consumer Protection Act。以下、「CCPA」という）[73]が制定されており、複数存在する同州の個人情報保護に関する法律の中でも、CCPA が中心的な法律となっていると言える。本報告書でも、CCPA に主として焦点を当てつつ、重要と解される箇所では CCPA 以外の個別の法令にも言及する。

CCPA は原則として民間部門を対象としており、官公庁は、営利「事業」（business）のために契約を締結するとき、CCPA を遵守しなければならない。

#### 2.　センシティブデータの取扱いに対する規制の趣旨

2018 年 6 月 28 日に成立した CCPA は、2018 年 1 月 3 日に法案 AB375[74]として提出されたが、その第 2 条には、CCPA に関するカリフォルニア州議会の意図及び目的が記載されており、これが、センシティブデータに限らない、個人情報保護一般に関する CCPA の立法目的といえる。かかる記述のうち、主に関連する箇所は以下のとおりである（AB375 第 2 条）。

> 「(i)…以下の権利を保障することで、消費者に個人情報をコントロールする効果的な手段を与え、カリフォルニア州民のプライバシーに対する権利を推し進めるのが議会の意図である。
>
> (1) いかなる個人情報が収集されているか知るカリフォルニア州民の権利
>
> (2) 個人情報が販売又は開示されているか、誰に対するものかを知るカリフォルニア州民の権利
>
> (3) 個人情報の販売を拒絶するカリフォルニア州民の権利
>
> (4) 個人情報にアクセスするカリフォルニア州民の権利
>
> (5) プライバシー権を行使しても、同等のサービス及び価格を受けるカリフォルニア州民の権利」

センシティブデータについては、CCPA の施行後に提出された Californian Privacy Rights Act （以下、「CPRA」という）の法案にその規制が含まれている。CPRA の法案を作成した Californians for Consumer Privacy という団体が公表しているホームページ[75]では、「CPRA は最もセンシティブな個人情報を対象とする強力な新しい概念を導入している。CCPA では、個人情報の販売を止める権利があるにすぎない。CPRA はさらに進んで、求める製品を提供するものでない限り、最もセンシティブな個人情報を使わないように企業に指示することができるようにする」と説明されている。このように、CPRA はセン

[73] https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5
[74] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180AB375
[75] https://www.caprivacy.org/faq/

シティブ個人情報という新たなカテゴリーを定め、消費者にその使用を制限する権限を与えることを意図して制定されているといえる[76]。

CPRA の法案は可決され法律として成立し、2023 年 1 月 1 日、CCPA を修正する形で施行され、これにより、CCPA においてセンシティブ個人情報の概念が追加された。法律の目的及び意図を定める CPRA 第 3 条の(A)(2)は、「消費者は、承認のない利用又は開示により消費者に被害を与える高いリスクをもたらすセンシティブ個人情報の利用を制限することを含め、個人情報の利用をコントロールすることができるべきであり、どのように収集され、利用され、開示されるかについて意味のある選択権を有するべきである」と定めている。

なお、CCPA の規定（Cal. Civ. Code § 1798.140(ae)）の注釈には以下の記載があり、これは、CCPA におけるセンシティブ個人情報の範囲は、GDPR を反映するように意図されていることの表れであると言える。

> 「GDPR 第 9 条における類似の文言：『…人種若しくは種族的出身、政治的意見、宗教的若しくは思想的信条又は労働組合員であること、遺伝子に関するデータ、自然人を一意に識別するための生体データ、健康に関するデータ又は自然人の性生活若しくは性的志向に関するデータの処理…。』本項この定義はより広く、通信内容、金融口座情報、ID データ等が含まれる。」

## II. センシティブデータの範囲―総論

### 1. センシティブデータの範囲一覧

CCPA は、消費者の「個人情報」（personal information）のうちの一定のものを「センシティブ個人情報」に該当するとしているところ、個人情報については、「特定の［カリフォルニア居住者］又は世帯を特定し、それと関係し、記述し、合理的に連想し、又は合理的に関連付ける」ものと定義している（Cal. Civ. Code § 1798.140(v)(1)）。なお、厳密には CCPA は、個人情報の定義箇所では「カリフォルニア居住者」との文言は用いず、「消費者」（consumer）についての情報を指すと定義しているが、その「消費者」も別途定義されており、それによれば、全カリフォルニア居住者及び世帯に適用されるよう定義している。したがって、CCPA の個人情報の主体は、いわゆる消費者に限られるわけではない。

但し、「公的に利用可能な」（publicly available）情報は、個人情報とはみなされない。Cal. Civ. Code § 1798.140(v)(2)によると、「公的に利用可能」とは、連邦、州、地方政府の記録から合法的に利用可能となった情報、本人により若しくは広く分配されたメディアから合法的に一般公衆に利用可能になったと企業が信じる合理的な基礎がある情報、若しくは本人が情報を特定の聴衆に限定しなかった場合に本人が情報を開示した相手方により利用可能とされた情報を意味する。他方、「公的に利用可能」には含まれない場合として、消費者が知らずに企業が消費者について収集した生体情報が挙げられている。

さらに、公的に利用可能な個人情報に加えて、非識別化された個人情報及び消費者情報の集合体は、CCPA により規律される個人情報の種類から除外される（Cal. Civ. Code § 1798.140(v)(3)）。

CCPA は、上記の個人情報の定義を前提として、以下のカテゴリーの個人情報が「センシティブ個人情報」に該当すると定めている（Cal. Civ. Code § 1798.140(ae)）。

- 消費者のソーシャルセキュリティー、運転免許、州身分証明書又はパスポートの番号を明らかにする個人情報
- 消費者のアカウントログイン、金融口座、デビットカード又はクレジットカード番号と、アカウントへのアクセスを可能にする必須のセキュリティコード若しくはアクセスコード、パスワ

[76] https://ccprivacy.wpenginepowered.com/wp-content/uploads/2020/04/WhyCPRA.pdf?_sm_au_=iVV4Rq6PJFFMMZFFKkM6NKsW8f6TG

ード又は証明書との組み合わせを明らかにする個人情報

- 消費者の正確な地理的位置を明らかにする個人情報
- 消費者の人種若しくは民族的出身、宗教的若しくは思想的信条又は労働組合員であることを明らかにする個人情報
- 消費者の郵便物、電子メール及びテキストメッセージの内容を明らかにする個人情報。ただし、事業者が通信の意図された受信者である場合を除く。
- 消費者の遺伝子に関するデータを明らかにする個人情報
- 消費者を一意に特定するための生体情報の処理
- 消費者の健康に関して収集及び分析された個人情報
- 消費者の性生活又は性的志向に関して収集及び分析された個人情報

なお、以下に列挙するデータのカテゴリーのデータは CCPA から適用対象から除外される（Cal. Civ. Code § 1798.145-146）。したがって、上記のカテゴリーに含まれる個人情報であっても、以下のいずれかにあたれば CCPA による規制対象外となる。

- カリフォルニア医療情報機密保持法（Health information governed by California's Confidentiality of Medical Information Act (CMIA)）又は連邦医療保険の携行性と責任に関する法律（Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)）が適用される健康情報
- 連邦公正信用報告法（Federal Fair Credit Reporting Act (FCRA)）が適用される信用情報
- 連邦グラム・リーチ・ブライリー法（Federal Gramm Leach Bliley Act (GLBA)）が適用される信用情報
- 1994 年ドライバープライバシー法（Federal Driver's Privacy Protection Act of 1994 (DPPA)）が適用されるドライバー情報
- カリフォルニア車両法典（California's Vehicle Code）の特定の規定及び合衆国法典における「交通」規定（"Transportation" provisions in the federal United States Code）が適用される車両情報, and
- Section 651 of Federal Harbors and Navigation Code 及び合衆国法典第 46 編第 4310 条（Section 4310 of Title 46 of Federal United States Code）に関する船舶情報

当局の公表している主要な資料、あるいは学者・有識者・実務家の資料（論文・記事等）においてセンシティブ個人情報の上記のカテゴリーごとに分けてその例、趣旨や範囲等についての個別に具体的に説明した内容は本調査の限りでは特に見当たらない。

2. センシティブデータを推知させる情報（推知情報）について

CCPA によると、「個人情報」の定義には、「消費者の嗜好、特徴、心理的傾向、素地、振舞い、態度、能力、適性を反映した消費者に関するプロファイルを作成するために、この項に特定された情報から導き出された推知」が含まれる（Cal. Civ. Code § 1798.140(v)(1)(K)）。

「推知する」（Infer）又は「推知」（inference）とは、事実、証拠その他情報若しくはデータの源から情報、データ、仮定又は結論を派生させることを意味する（Cal. Civ. Code § 1798.140(r)）。このことから、他の情報から導き出された推知であって、個人情報に該当し、かつ CCPA でセンシティブ個人情報に該当すると定められた種類の情報に該当するものは、「センシティブ個人情報」となると解される。

カリフォルニア司法長官事務所（OAG）は、個人情報の収集と推知に関するガイダンスを公開しており[77]、それによれば、「推知とは、企業が収集した他の情報（オンライン取引、ソーシャルネットワーク

[77] https://oag.ca.gov/system/files/opinions/pdfs/20-303.pdf

の投稿又は公的記録等）に基づく、消費者について推論された特徴（結婚している、家を有している、オンラインショッピングを利用する、投票に行くなど）である。」とされる。同ガイダンスはまた、「消費者に関するプロファイルを作成する」ため、という条件に該当しない場合には、推知が個人情報に該当しなくなるという点についても説明している。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。

Cal. Civ. Code § 1798.140(ae)の(2)(B)は、以下の情報がセンシティブ個人情報に該当すると定義している。

> 「(B) 消費者の健康に関して収集及び分析された個人情報」

もっとも、CCPA は、HIPAA のプライバシー、セキュリティ及び違反通知の規則が適用される対象事業体又は業務関係者（CCPA 上のサービス・プロバイダーに類似している。）が収集する保護された健康情報を明示的に除外していることに留意されたい（Cal. Civ. Code § 1798.145(c)(1)(A)）。健康情報に関する CCPA の規律は、HIPPA 等、CCPA でその適用が除外される連邦法の対象事業体でないすべての事業者（例えば、ほとんどの民間部門の使用者）に適用される。

なお、CCPA 自体は健康情報を定義していないが、カリフォルニア医療情報機密保持法（CMIA）は「医療情報」（Medical Information）を次の通り定義し、医療情報について対象事業者に守秘義務を課す規制を設けている。

> 「患者の病歴、メンタルヘルス申請情報、精神若しくは身体の状態又は治療に関して、ヘルスケア提供者、医療サービス計画、製薬会社又は請負業者が保有し、又はそこから得られる、電子的又は物理的形態の、一切の個人特定可能な情報。『個人特定可能』（Individually identifiable）とは、医療情報に、患者の氏名、住所、電子メールアドレス、電話番号、社会保険番号その他単独で又は他の公的に利用な可能と組み合わせて個人の身元を明らかにする情報のような、個人の特定を可能とするのに十分な個人を特定する情報の要素が含まれていることを意味する。」（Cal. Civ. Code § 56.05）。

(i)　医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する。

医療検査結果は、消費者の健康に対して収集及び分析された個人情報であり、したがって CCPA におけるセンシティブ個人情報に該当する。

(ii)　事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。事業者が市販の検査機器を利用して行った検査結果は、消費者の健康に関して収集及び分析された個人情報であり、CCPA におけるセンシティブ個人情報に該当する。

(iii)　消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。市販の検査機器を利用することによる、消費者についての検査結果は、消

費者の健康に関して収集及び分析された個人情報であり、CCPA におけるセンシティブ個人情報に該当する。

(iv)　消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する。消費者が自ら判断した健康状態は、消費者の健康に関して収集及び分析された個人情報であり、CCPA におけるセンシティブ個人情報に該当するものと思われる。

なお、（CMIA にはセンシティブデータの概念はないものの）CMIA において「医療情報」に該当するためには、データは「［…］ヘルスケア提供者、医療サービス計画、製薬会社又は請負業者が保有し、又はそこから得られる［…］」ものでなければならない。したがって、医師等の判断を介することなく消費者が自ら判断した健康状態は、CMIA の適用対象とならない。

(v)　予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無は、センシティブデータに該当する。予防接種の接種有無は、消費者の健康に関して収集及び分析された個人情報であり、CCPA におけるセンシティブ個人情報に該当する。

（CMIA にはセンシティブ健康データの概念はないものの）、予防接種の接種有無というデータは、CMIA における「医療情報」にも該当する。上記(iv)と異なり、予防接種の接種有無は、（データ主体によって自己報告された場合であっても）ヘルスケア提供者から得られる情報に該当すると解されるためである。

(2)　趣旨

健康情報をセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3)　追加的規律（該当する場合）

CMIA は、センシティブな個人データと通常の（すなわち、センシティブでない）個人データとを区別していないが、「医療情報」に適用される。CMIA は、機密な医療情報について、誰がどういう場合に公開できるかを規定し、また、医療情報の共有、売却その他不法な利用を禁じている。一般論として、CMIA により、ヘルスケア提供者、ヘルスケアサービス計画、請負会社及び製薬会社は、患者又は患者の法的代理人により署名された所定の形式の有効な書面による承認を受けることなく、患者の医療情報を開示することができない（Cal. Civ. Code § 56.10[78]）。

2.　遺伝子に関するデータ

(1)　センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、センシティブデータに該当する。

[78] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV

Cal. Civ. Code § 1798.140(ae)の(1)(F)は、以下の情報を明らかにする個人情報が「センシティブ個人情報」に該当すると定義している。

「(F) 消費者の遺伝子データ」

なお、データ漏洩時の通知義務について定めるカリフォルニアデータ侵害通知制定法（Cal. Civ. Code § 1798.82）に関し、2021 年にその対象となる「個人情報」の定義が拡大された。すなわち、対象事業者に対して、居住者の暗号化されていない個人情報のセキュリティが侵害された場合、カリフォルニア居住者に通知することが義務付けられているところ、Cal. Civ. Code § 1798.82(h)(1)(H)によると、「個人情報」は「遺伝子に関するデータ」を含むとされた。そこにいう「遺伝子に関するデータ」の定義は次の通りである。

> 「『遺伝子に関するデータ』とは、形式にかかわらず、個人の生物学的サンプルの分析から、又は同様の情報を得られる他の情報源から得られた、遺伝物質に関連する一切のデータを意味する。遺伝物質には、DNA、RNA、遺伝子、染色体、対立遺伝子、ゲノム、DNA 又は RNA の変化又は装飾、一塩基多型（SNPs）、生物学的サンプルその他資料の分析から得られた未解釈のデータ及びそれから外挿、派生又は推知した一切の情報を意味する。」（Cal. Civ. Code § 1798.82(i)(5)）。

(i) 医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する可能性が高い。すべての遺伝子に関するデータは CCPA においてセンシティブデータに該当する。CCPA は、上記(1)で該当する箇所を引用している Cal. Civ. Code § 1798.140(ae)以上に遺伝子に関するデータを定義していないが、カリフォルニアの他の法律（例：遺伝情報プライバシー法（Genetic Information Privacy Act (GIPA)[79]やカリフォルニアのデータ侵害通知制定法）が遺伝子に関するデータを定義している。データ侵害通知制定法は上述の通りである。GIPA における定義は次の通りであり、実質的にデータ侵害通知制定法と同じ定義といえる。

> 「形式にかかわらず、消費者からの生物学的サンプル（すなわち、DNA が含まれていると知られている、生物組織、血液、尿又は唾液のような、人間のあらゆる物的部分、そこからの排出物又は派生物）の分析から、又は同等の情報を得られる要素から生ずる、遺伝物質に関するデータと定義している。遺伝物質には、DNA、RNA、遺伝子、染色体、対立遺伝子、ゲノム、DNA 又は RNA の変化又は装飾、一塩基多型（SNPs）、生物学的サンプルその他資料の分析から得られた未解釈のデータ及びそれから外挿、派生又は推知した一切の情報を意味する。」

このため、カリフォルニア州法の下で遺伝子に関するデータがセンシティブであるかどうかは、誰が検査を行ったかによって決まるものではない。医師等が実施する遺伝子検査の結果は、通常、上述の遺伝子に関するデータの定義に該当すると想定されるため、カリフォルニア州法の下ではセンシティブデータに該当する可能性が高い。

(ii) 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する可能性が高い。すべての遺伝子に関するデータは、CCPA においてセンシティブデータに該当する。CCPA は遺伝子に関するデータを定義していないが、カリフォルニアの他の法律（例：GIPA）における遺伝子に関するデータの規定については上記 2(1)(i)で上述の通りである。

このため、カリフォルニア州法の下で遺伝子に関するデータがセンシティブであるかどうかは、誰が検査を行ったかによって決まるものではない。消費者が市販の遺伝子検査キットを利用して行った遺伝子

[79] https://law.justia.com/codes/california/2021/code-civ/division-1/part-2-6/chapter-2-6/section-56-18/

検査であっても、その結果は上述の遺伝子に関するデータの定義に該当すると想定されるため、カリフォルニア州法の下でセンシティブデータに該当する可能性が高い。

(iii) 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当する可能性がある。

CCPA は遺伝情報を定義しておらず、上述の他のカリフォルニア州法の定義においても、遺伝子検査キットを解することなく個人が自ら判断した遺伝子に関する情報は遺伝子に関するデータに該当しない可能性がある。他方で、連邦法では、遺伝情報には、個人の遺伝子検査や個人の家族の遺伝子検査に関する情報に加え、個人の家族における疾患や障害の発現に関する情報（すなわち、家族の病歴）が含まれる旨を定めているものが見られ、例えば、家族の病歴は、ある人が将来病気や障害、状態になるリスクが高いかどうかを判断するために用いられることが多いため、2008 年遺伝情報非差別法（GINA）の遺伝情報の定義に含まれている。CCPA の解釈においてもこの定義やその背後にある考え方を踏まえ、センシティブデータに該当するという解釈がなされる可能性がある。

(2) 趣旨

遺伝子に関する情報をセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3) 追加的規律（該当する場合）

GIPA は、消費者向けの遺伝子検査会社に対し、消費者の遺伝子に関するデータの収集、利用又は開示について、少なくとも以下の各項目について個別的かつ明示的な同意を得ることを求めている。

- 消費者に対して提供された遺伝子検査の製品又はサービスを通じて収集された遺伝子に関するデータの使用
- 消費者が求めた最初の検査が完了した後の消費者の生物学的サンプルの保管
- 遺伝子検査又はサービスの主要目的及び固有の文脈的な使用を超えた遺伝子に関するデータ又は生物学的サンプル各利用
- サービス提供者を除く第三者に対する消費者の遺伝子に関するデータ又は生物学的サンプルの各移転又は開示
- マーケティング目的

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する。

Cal. Civ. Code § 1798.140(ae)[80]の(2)(C)は、以下の情報が「センシティブ個人情報」に該当すると定義している。

「(C) 消費者の性生活又は性的志向に関して収集及び分析された個人情報」

(2) 趣旨

性生活・性的指向に関するデータをセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3) 追加的規律（該当する場合）

特に見当たらない。CCPA のもとでは、性生活及び性的志向は他のセンシティブデータと同様に扱われる（下記 IV を参照）。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する。

Cal. Civ. Code § 1798.140(ae)は、関連する箇所で以下のとおり規定する。

「『センシティブ個人情報』は、［…］（1）［］（D）消費者の人種若しくは民族的出身、宗教若しくは政治的信条又は労働組合員であることを明らかにする個人情報を意味する。」

(2) 趣旨

労働組合への加入に関する情報をセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3) 追加的規律（該当する場合）

特に見当たらない。CCPA の下では、労働組合員であることは他のセンシティブデータと同様に扱われる（下記 IV を参照）。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

[80] https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.140.&lawCode=CIV

自然人を一意に識別することを目的とする生体データは、センシティブデータに該当する。

Cal. Civ. Code § 1798.140(ae)(2)(A)は、以下の情報が「センシティブ個人情報」に該当すると定義している。

> 「(A) 消費者を一意に識別するための生体情報の処理」

「生体情報」は、Cal. Civ. Code § 1798.140(c)において以下の通り定義されている。

> 「個人のデオキシリボ核酸（DNA）に関連する情報を含む、個人の生理的、生物学的、又は行動の特徴であって、個人の身元を確立するために単独で若しくは互いに組み合わせて、又は他の識別データとともに使用される、又は使用することが意図されるもの。」

その具体例としては、顔紋、マニューシャテンプレート（指紋の紋様の特徴点の情報）、声紋などの識別子テンプレートを抽出することができる、虹彩、網膜、指紋、顔、手、掌、静脈パターン、音声録音が含まれるほか、個人を識別させる情報を含むキーストロークパターンやリズム、歩行パターンや歩行リズム、睡眠・健康・運動データも含まれる（Cal. Civ. Code § 1798.140(c)）。

(2) 趣旨

自然人を一意に識別することを目的とする生体データをセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3) 追加的規律（該当する場合）

特に見当たらない。CCPA のもとでは、消費者を一意に識別するための生体情報の処理は他のセンシティブデータと同様に扱われる（下記 IV を参照）。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータがセンシティブデータに該当するか否かは、条件による。

Cal. Civ. Code § 1798.140(ae)の(1)(B)は、以下の情報を明らかにする個人情報が「センシティブ個人情報」に該当すると定義している。

> 「(B) 口座へのアクセスを可能にする必須のセキュリティコード若しくはアクセスコード、パスワード又は証明書と組み合わせられた、消費者の口座ログイン、金融口座、デビットカード又はクレジットカード番号」（強調のため一部下線を追加している。）

したがって、口座番号やクレジットカード番号等は、口座へのアクセスが可能となる情報と組み合わされたものである場合には、センシティブデータに該当する。

金融に関する個人情報は、さまざまな他のカリフォルニア州法や連邦法に基づき保護されるが、ほとんどの組織に適用される包括的な法律ではない。

CCPA は、連邦法のグラム・リーチ・ブライリー法（及びその施行規則）、カリフォルニア金融情報プライバシー法及び連邦法の農業信用法（Farm Credit Act of 1971）が適用される個人情報の収集、処理、

売却又は開示を CCPA の適用対象から明示的に除外しており、そのような収集等については CCPA は適用されないことに留意が必要である（Cal. Civ. Code § 1798.145(e)）。

(2) 趣旨

金融口座番号、クレジットカード番号等に関する情報をセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は本調査の限りでは見当たらないが、センシティブデータ一般の取扱に対する規制の趣旨（I. 2 参照）が妥当すべき種類の情報であるためと解される。

(3) 追加的規律（該当する場合）

特に見当たらない。CCPA のもとでは特定の金融データは他のセンシティブデータと同様に扱われる（下記 IV を参照）。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

この節では、信用に関するデータは（クレジットスコアとして知られる）信用度（creditworthiness）を指すものとする。

信用に関するデータは、CCPA におけるセンシティブデータに該当しない。Cal. Civ. Code § 1798.140(ae)は信用データを含まない。他方、通常の個人データを定義する Cal. Civ. Code § 1798.140(v)(1)(D)が次のように定めており、信用に関するデータもこの定義に該当すると解されるため、通常の個人データに該当する。

> 「（D）個人の財産、購入、獲得若しくは検討した製品又は他の購入若しくは消費の履歴若しくは傾向を含む、商業情報」（Cal. Civ. Code § 1798.140(v)(1)(D)）

但し、連邦法である公正信用報告法（Fair Credit Reporting Act。以下、「FCRA」という）、カリフォルニア州法である、調査対象消費者報告機関法（Investigative Consumer Reporting Agencies Act。以下「ICRAA」という）及びカリフォルニア消費者信用報告機関法（California Consumer Credit Reporting Agencies Act）等の様々な法律が、信用情報の取得方法を、特に、雇用主等が従業員等の信用情報を取得する方法について、規制している。いずれもプライバシーや個人情報の処理に焦点を当てた法令ではないものの、例えば、FCRA と ICRAA は、本人への通知や同意に関する要件を定めるほか、求職者にはバックグラウンドチェックのコピーを受け取る権利を認めている点で、信用に関するデータの処理にも規律が及ぶ法令である。

(2) 趣旨

信用に関するデータは CCPA におけるセンシティブデータとはみなされないと考えられる。信用に関するデータの処理は上述のように連邦法及び州法の対象となっており、多くの場合で CCPA の適用外となるためである。

(3) 追加的規律（該当する場合）

特に見当たらない。但し、上述の通り、連邦及び州レベルのさまざまな法律が、信用データの入手方法について定めている。

なお、CCPA は、消費者報告機関及び情報提供者（FCRA に定義される）が収集、保持、利用、販売又は共有した個人情報をその適用から明示的に除外している。これにより、個人情報が FCRA の対象であり、同法に従って利用される限りは、CCPA の適用対象から除外される。

FCRA 及び ICRAA は、通知及び同意の要件を原則として課しているほか、候補者は、バックグランドチェックのコピーを受け取る権利が認められている。FCRA 及び ICRAA を遵守するためには、特別のフォームを使用する必要がある。通知及び同意の要件は、使用者が現従業員の違法行為又は不正行為を疑っている場合には適用されない。ICRAA では、報告が違法行為又は不正行為を疑うためのものでなければ、調査が行われるたびに本人の同意が必要とされており、この点は FCRA とは異なる。

さらに、債権回収に関してはさまざまな法律がある。連邦レベルの公正債権回収法（Fair Debt Collection Practices Act）、カリフォルニア州レベルの公正債権回収法（Fair Debt Collection Practices）（いずれも 1970 年代に成立）が、債権回収者による多くの詐欺的、不誠実、不公正、不合理な債権回収行為を禁止している。いくつかの限られた例外を除き、債権回収業者は、債権回収に関するいかなる情報も第三者に伝えてはならない（例外の一つは、信用調査機関への伝達に関するものである）。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。

(2) 趣旨

カリフォルニア州法が、政府から金銭的保護及び援助を受けている事実に関するデータをセンシティブデータに位置付けていない理由は、必ずしも明らかではない。

(3) 追加的規律（該当する場合）

該当なし。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、センシティブデータに該当しない。

(2) 趣旨

成年後見制度の保護を受けている事実に関する情報をセンシティブデータに位置付けている趣旨又は理由について取り立てて説明した資料は調査の限りでは見当たらない。アメリカでは、成年後見制度（conservatorship と呼ばれる）は、裁判所への申請及び裁判所の審理を必要とする司法手続である。そ

の結果、成年後見は裁判手続であり、審理及び記録は公開されているため、アメリカにおいて成年後見の情報は一般的に公開されており（但し成年後見の種類によっては（非自発入院等）、その例外的な性質により機密となっているものもある）、そのことから、センシティブデータに位置付けていられないとも考えられる。

(3) 追加的規律（該当する場合）

該当なし。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報は、CCPA の定義する「センシティブ個人情報」に該当しない。ただし、CCPA では、児童の個人情報の取扱いについて特別の要件が設けられていることに留意されたい（下記(3)参照）。

(2) 趣旨

CCPA には、既に未成年の児童のデータの取扱いに関する規則が含まれているためと考えられる。

(3) 追加的規律（該当する場合）

CCPA は、16 歳未満の消費者の情報を同意なく販売することを禁じている。13 歳未満の児童については、保護者の同意が必要である。13 歳から 16 歳の児童は、直接同意することができる。なお、連邦法である COPPA に基づく保護は、CCPA の要件に加えて適用される（COPPA については、第 3 章米国（連邦）を参照されたい）。

デジタル世界におけるカリフォルニアの未成年者のプライバシー権法（California's Privacy Rights for California Minors in the Digital World Act）（Calif. Bus. & Prof. Code §§ 22580-22582）（別名「消しゴム」法案）は、未成年者が、インターネットウェブサイト、オンラインサービス、オンラインアプリケーション又はモバイルアプリケーションに投稿したコンテンツ又は情報を、削除し、又は削除を請求し削除を受けることを認めている。同法は、未成年者向けのウェブサイト又はオンラインサービスの運営者が、未成年者が購入することが禁止されている特定の商品又はサービスを未成年者に販売し、又は広告することを禁じている。同法はさらに、未成年者に固有の個人情報に基づき特定の製品を販売又は広告すること、及びそれを故意に利用し、開示し、集計し、又は第三者に行わせることを禁じている。

また、カリフォルニア州知事は、最近、児童がアクセスする可能性のあるオンラインサービス、製品又は機能を提供する事業者が特定の要件（2024 年 7 月 1 日から施行）を遵守することを義務付けるカリフォルニア年齢適正デザインコード法（California Age-Appropriate Design Code Act）に署名している。

11. オンライン行動履歴（ウェブサイトの閲覧履歴等）に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴（ウェブサイトの閲覧履歴等）に関する情報は、センシティブデータに該当しない。CCPA の通常の個人情報の定義に、「ブラウジング履歴、検索履歴及びインターネットウェブサイト、アプリケーション又は広告との消費者のインタラクションに関する情報を含むがそれに限られない、インターネットその他電子ネットワークアクティビティ情報」が含まれている。

(2) 趣旨

カリフォルニア州法が、オンライン行動履歴（ウェブサイトの閲覧履歴等）に関する情報をセンシティブデータに位置付けていない理由は、必ずしも明らかではない。

(3) 追加的規律（該当する場合）

該当なし。

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

消費者の特性を推知する目的なしに収集及び処理されるセンシティブ個人情報は、CCPA のもとで、センシティブでない個人情報とほとんど同様に取り扱われる（Cal. Civ. Code § 1798.121(d)）。

消費者の個人情報を取得するために、CCPA は事業者（Cal. Civ. Code § 1798.140(d)で CCPA により定義される）に、「収集時通知」で特定の情報を消費者に提供することを求める。CCPA はそのような通知に数々の要件を課しており、例えば、収集時通知には、消費者について事業者が収集する個人情報のカテゴリー及び情報カテゴリーを利用する目的を記載しなければならない。

また、事業者が消費者の個人情報を「共有」（share）又は「販売」（sell）する場合、収集時通知は、"Do Not Sell"及び"Do Not Share"のリンクを含まなければならない。CCPA は、個人情報の「販売」を、金銭その他の対価で事業者が第三者に対して個人情報を（口頭、書面、電子的方法その他の方法で）移転することと広く定義している。通知は、消費者が事業者のプライバシー取扱い及びプライバシー権について詳細な説明を得ることができる事業者のプライバシーポリシーへのリンクが含まれていなければならない。したがって、CCPA は事業者にプライバシーポリシーを策定することを義務付け、当該プライバシーポリシーに置いて含めるべき事項を定めていているものの、「収集時通知」は、事業者のプライバシーポリシーと同一ではない要件として別途求められている。

事業者は、原則として個人情報の収集時に、CCPA に基づく、これらの収集時の通知の要件を遵守する必要があり、この要件はセンシティブ個人情報の取得にも適用される。CCPA の収集時の通知されなければならない事項は次のとおりである。

- 消費者に関して収集される個人情報のカテゴリーのリスト。個人情報の各カテゴリーは、収集される個人情報について消費者が十分に理解できるように記載しなれなければならない。
    - 特に、センシティブ個人情報に関しては、「事業者がセンシティブ個人情報を収集する場合、収集されるセンシティブ個人情報のカテゴリー及びセンシティブ個人情報のカテゴリーが収集又は利用される目的、並びに情報が販売又は共有されるか」という点を通知すべき項目として規定している。また、「事業者は、本条に適合する通知を消費者に行うことなく、センシティブ個人情報の追加的カテゴリーを収集し、センシティブ個人情報を収集した開示

された目的と適合しない追加的目的で収集されたセンシティブ個人情報を利用することはできない。」ことも特に定めている。

- 個人情報のカテゴリーが利用される目的
- 事業者が各カテゴリーの個人情報を保持しようとする期間
- 事業者が個人情報を販売する場合、消費者がオプトアウトできる"Do Not Sell My Personal Information"とのタイトルのリンク（オフラインの通知では、会社のウェブサイトのリンク又はデータ収集フォーム上のチェックボックスでの代替が許容される）
- 事業者のプライバシーポリシーへのリンク、又はオフラインの通知では、プライバシーポリシーのオンライン上の位置

さらに、原則として、センシティブ個人情報を含む個人情報を収集する事業者は、消費者の個人情報が、個人情報を収集及び処理した目的を達成するため、若しくは当該個人情報が収集された文脈と適合する別の開示された目的を達成するために合理的に必要かつ適切である範囲でのみの収集、利用、保持及び共有されるようにし、これらの目的と適合しない方法でさらに処理されないようにしなければならない（Cal. Civ. Code § 1798.100(c)）。

2. 利用

CCPA は、事業者が、消費者に収集する個人情報が何か公表し、特定のケースでデータの保存、移転及び利用をオプトアウトする権利を消費者に与えなければならない、オプトアウト制度のもとで運用されている。事業者は、EU の一般データ保護規則（GDPR）のようにデータ処理の「法的根拠」（legal basis）を確立する必要はない。

センシティブ個人情報に関して、CCPA の規定（Cal. Civ. Code § 1798.121）は、「センシティブ個人情報の利用及び開示を制限する消費者の権利」を特に定める。したがって、CCPA に基づく一般的な権利を消費者に提供することとは別に、事業者は、センシティブ個人情報を合法的に処理するために、この規定を遵守しなければならない。Cal. Civ. Code§ 1798.121 は次のように規定する。

- 消費者は、消費者に関するセンシティブ個人情報を収集する事業者に対し、いつでも、消費者のセンシティブ個人情報の利用を、商品又はサービスを要求する平均的消費者が合理的に期待するサービス及び商品を提供し、［1798.140(e)条に定義された特定の「事業目的」を］遂行するのに必要で、［オプトアウトプリファランスシグナル（opt-out preference signals）に関して採用された規則により］承認される使用に制限するよう命ずる権利を有する。この節に規定されるもの以外の目的で消費者のセンシティブ個人情報を利用又は開示する事業者は、消費者に対し、…(中略)この情報が追加的な特定の目的のために利用又はサービス提供者若しくは請負業者に開示されることがあること、及び消費者がセンシティブ個人情報の利用又は開示を制限する権利を有することを通知しなければならない。
- サービス提供者（すなわち、データの処理者であって、データの管理者ではない者）又は請負業者（すなわち、サービス提供者に類似するが、事業のためにデータを処理する必要がない者）もまた、消費者が事業者に対して消費者のセンシティブ個人情報の利用を制限し、又はやめるように命じたとの通達を事業者から受領した後、センシティブ個人情報を利用することが禁じられる。

さらに、CCPA の Cal. Civ. Code§ 1798.135 は、「個人情報の販売、共有及び利用並びにセンシティブ個人情報の利用を制限する方法」を規定する。Cal. Civ. Code§ 1798.135(a)では、上記に特定された許可された目的（例：問題となるサービス又は商品を提供し、又は特定の事業目的を遂行するのに必要である

ため）以外の目的でセンシティブ個人情報を販売又は共有する事業者は、消費者が合理的にアクセスできる形式で、次の事項を提供しなければならない。

- "Do Not Sell or Share My Personal Information"とのタイトルの事業者のインターネットホームページ（利用者が個人情報の販売又は共有をオプトアウトすることを可能にするページ）の目立つリンク
- 同様の"Limit the Use of My Sensitive personal Information"との（CCPA の他の規定に従い、消費者がセンシティブ個人情報の利用又は開示を制限することを可能にするホームページへの）リンク
- 消費者が容易に個人情報の販売若しくは共有をオプトアウトし、又は消費者のセンシティブ個人情報の利用若しくは開示を制限することを可能にする、上記 2 つのリンクの代わりとなる異なるリンク
- 事業者が、製品又はサービスの使用料金を消費者に伝えることで、上記 3 つのリンクから受領したオプトアウトのリクエストに応じる場合、消費者に金銭的インセンティブプログラム（例：「ロイヤルティ」プログラム）を提示すること。

これらのリンク及びアクションは、事業者が消費者に対し、自らの意思でオプトアウトプリファレンスシグナル（例：ブラウザのプラグインからの送信）を送ることで個人情報の販売若しくは共有からオプトアウトし又はセンシティブ個人情報の利用を制限できるようにしている場合には、不要である（Cal. Civ. Code § 1798.135(b)(1)）。

個人情報の販売、共有及び利用並びにセンシティブ個人情報の利用を制限するのに事業者が用いなければならない方法については、CCPA はさらに詳細な規定を用意している（Cal. Civ. Code § 1798.135）。

3. 第三者提供

CCPA に基づき、個人情報の移転のあり方によってさまざまな規律が適用される。

個人情報の移転が消費者の個人情報の「販売」若しくは「共有」に当たる場合、当該移転が CCPA の他の規定に基づき適用除外とならければ、事業者は、個人情報の受領者と特定の契約を締結しなければならない（Cal. Civ. Code § 1798.100(d)）。サービス提供者及び請負業者に対する移転は、CCPA の「販売」の定義から除外されるが、その場合でも、CCPA に列挙された「事業目的」のいずれかのためにサービス提供者若しくは請負業者に対して行う個人情報の移転については、当該移転が CCPA の他の規定に基づき適用除外とならければ、個人情報の受領者と契約を締結する義務が事業者に課される。

さらに、カリフォルニアプライバシー保護機関（CPPA）により将来発出される規則について定める Cal. Civ. Code § 1798.185 (a) (15) (B)は、消費者の個人情報の処理が消費者のプライバシー又はセキュリティに対する重大なリスクを呈する事業者には、定期的に次の事項を CPPA に提出することが当該規則により義務付けられる旨を規定している。

「センシティブ個人情報の処理をするかどうかを含む、個人情報の処理に関するリスク評価、並びに処理に関する消費者の権利への潜在的な利益に対し、処理により生じる消費者、事業者、他の利害関係者及び公共に対する利益を特定し、かつ重み付けすることに関するリスク評価。本条は、事業者に対して企業秘密の開示を求めるものではない。」

したがって、データの処理行為及び移転に関するリスク評価が必要であり、センシティブ個人情報に関わる場合、その評価はより厳格な精査を受けることとなり得る。

4. 管理

CCPA において、消費者の個人情報を収集する事業者は、「個人情報を無承認又は違法なアクセス、破壊、利用、変更又は開示から保護するために個人情報の性質に適切な合理的セキュリティ手続及び慣行」を実施しなければならない。しかし、同法は、この義務をこれ以上定義せず、いかなるセキュリティ手続及び慣行が「合理的」か定めていない。実務上、企業は関係する業界の慣行や、カリフォルニア州当局が発行したこのトピックに関するガイダンスを参照すべきとされている。カリフォルニア司法長官事務所は、2014 年[81]及び 2016 年[82]に報告書を発行しており、セキュリティ実務を論じ、インターネットセキュリティセンターが公開する 20 のデータセキュリティコントロール（CIS コントロール）を強調している。

5. 漏えい等

事業者又は州機関は、カリフォルニア州居住者の暗号化されていない個人情報が正当な権限を有さない者に取得され、又は合理的に取得されたと考えられる場合には、当該カリフォルニア州居住者に通知しなければならない（政府機関については Cal. Civil Code § 1798.29、事業者については Cal. Civ. Code § 1798.82 を参照）。なお、カリフォルニア州法は、通知義務を生じさせる被害について特に限定する基準は設けていない。

例外はあるものの（例えば、医療機関及び金融機関等、他の連邦規制制度が妥当する事業者）、一般に、事業者は、影響を受けたデータ主体に対し、「可能な限り最も適切な時期に、不合理な遅滞なく」データ侵害について通知しなければならず、カリフォルニア州法は、事業者が使用できる書面による通知のドラフトも提供している。

データ侵害が 500 以上のデータ主体に影響を与える場合、事業者又は期間は、カリフォルニア司法長官事務所にも通知しなければならない。

6. 請求権

CCPA に基づき、消費者は、原則として、次の一般的権利を有する。

- 事業者が収集する個人情報とその利用及び共有の方法について知る権利
- 収集された個人情報を削除する権利
- 個人情報の販売又はクロスコンテクスト行動広告のための共有をオプトアウトする権利並びに合法的に規定され承認された目的を超えたセンシティブ個人情報の利用及び開示をオプトアウトする権利
- CCPA の権利行使について差別されない権利
- 個人情報を訂正する権利
- オプトアウト又は他の権利行使に伴い報復を受けない権利

Cal. Civ. Code § 1798.121 によれば、センシティブ個人情報については、さらに、消費者は、事業者に対して、消費者が要求したサービスを提供するなどの限られた目的でのみ、消費者のセンシティブ個人情

[81] https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/2014_cybersecurity_guide.pdf
[82] https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf

報を使用するよう求める権利を有する。CCPA 規則草案[83]において、かかる権利を本人に通じする義務やウェブサイトにおいてその権利行使のためのリンクを設ける義務などが規定されている（CCPA 規則草案§ 7014 、Notice of Right to Limit and the “Limit the Use of My Sensitive Personal Information” Link） 。

請求権の行使について、CCPA は原則として、カリフォルニア司法長官事務所によってのみ執行することができたが、最新の法改正により、CPPA へかかる権利行使の権限が移管された。また、CCPA は、その範囲は限定されているものの、消費者に対し、プライバシー法の違反について企業を直接訴えることができる私的訴権を与えている。この私的訴権は Cal. Civ. Code § 1798.150 に規定されており、CCPA のデータ侵害及びセキュリティに関する義務違反に限られる。これに関しては、具体的には以下の通り定められている。

- 第 1798.81.5(d)(1)(A)で定義される暗号化若しくは編集されていない個人情報又は電子メールアドレスとパスワードの組合せ若しくはアカウントへのアクセスを許可する秘密の質問と答えが、個人情報を保護するために情報の性質に応じた合理的なセキュリティ手続及び慣行を実施し維持する義務を事業者が違反したことにより、不正アクセス漏洩、盗難又は開示の被害を受けた消費者は、次の民事訴訟を提起することができる。
    - 1 件の 1 消費者あたり 100 ドル以上 750 ドル以下の金額又は実際の金額いずれか大きいほうの損害賠償を請求すること
    - 差止め又は確認的救済
    - その他裁判所が適切とみなす救済

## V. 本人同意、プロファイリング

### 1. 本人同意

#### (1) センシティブデータ規制（上記III）との関係

CCPA 上、センシティブデータの処理は、本人の同意を必要とするものではない。

CCPA は、消費者の個人情報の収集及び処理について消費者の同意を一般的に求めるものではなく、例えば、特定の未成年者のデータを販売又は共有する場合（上記参照）、対価を得て個人情報を取得する場合（金銭的インセンティブ）といった、特定の状況でのみ必要とされるのみであって、センシティブデータを処理する際に特に同意が求められるわけではない。

#### (2) 要件一般

CCPA は、「同意」を、「狭く定義された特定の目的のために消費者に関する個人情報を処理することへの同意を示す、言明によるもの及び明確な肯定的行動によるものを含む、消費者又は消費者の法定後見人、代理人若しくは消費者の財産管理人として行為する者により、自由になされた、具体的な、情報に基づく、曖昧でない消費者の希望の表示」と定義し、反対に、「個人情報処理と他の関係しない情報が記載された一般的又は広範な利用規約その他類似の文書を承諾することは、同意を構成しない。あるコンテンツにマウスオーバーすること又はあるコンテンツをミュートし、一時停止し、又は閉じること

[83] https://cppa.ca.gov/regulations/pdf/20221102_mod_text.pdf。なお、本調査の基準日時点では草案であったが、その後この内容で CCPA 規則として成立した（https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf）。以下、CCPA 規則草案に言及する箇所について同じ。

は、同意を構成しない。」と定めている（強調のため一部下線を追加している）（Cal. Civ. Code § 1798.140(h)）。

(3) 情報提供

CCPA に基づき同意が必要な場合に有効な同意であるためには、少なくも、事業者は、消費者が何に同意するか正確に説明する必要がある。消費者の同意が有効とみなされるために事業者が十分な情報を提供したかどうかが争われる場合には、カリフォルニアの裁判所が事案ごとに分析することとなる。なお、CCPA が、特定の開示、通知、プライバシーポリシーに特定の情報を含めることを要求している点には留意が必要である（もっとも、この要件は特に同意に関するものではない）。

(4) 形式

CCPA は、同意の形式について具体的な要件を定めていないが、CCPA 規則草案は、事業者は、CCPA に基づく消費者のリクエストを提出及び消費者からの同意取得の方式を、以下の原則を組み込んで設計し、実施しなければならないと規定する（CCPA 規則草案§ 7004 、Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent）。

- 理解が容易であること。消費者が読みやすく理解しやすいことばを使用しなければならない。
- 選択の対称性。消費者の選択能力を損ない、又は妨げるため、消費者がよりプライバシーを保護する選択を行うための道筋は、プライバシーを保護しない選択を行う道筋より、長く、困難で、又は時間がかかるものであってはならない。
- 消費者を混乱させる言葉やインタラクティブ要素を避けること。二重否定を使ってはならない。トグル又はボタンは、消費者の選択を明確に表示するものでなければならない。
- 消費者の選択能力を害し、又は妨げる選択アーキテクチャを避けること。同意は自由になされた、具体的な、情報に基づく、曖昧でないものでなければならず、事業者は、消費者の選択能力を害するように方式を設計してはならない。
- 行使が容易であること。事業者は、消費者が CCPA の請求を提出するプロセスに、不必要な負担又は抵抗を付加してはならない。方式は、機能的であって、請求を提出する消費者の選択を損なわないようにするためにテストされなければならない。

したがって、同意が必要とされる場合、その同意は明確で、あいまいでないものでなければならない。例えば、事業者は、消費者が以前にオプトアウトプリファレンスシグナルを送信した後に、さらにオプトアウトプリファレンスシグナルを受けなかったとしても、そのことをもって、個人情報の販売又は共有に対するオプトインの同意であると解釈してはならない。

(5) 個別同意の必要性

CCPA 及び CPPA 規則草案は、同意は各処理行為に関して個別に取得しなければならないと明示的に規定しているわけではないが、同意の各種類の要件は、同意がそもそも必要となる理由によって異なる。したがって、実務上、異なる処理行為については別個の同意が必要となりうる。例えば、13 歳未満の児童のデータを販売又は共有することと、対価を得て個人情報を取得する場合（金銭的インセンティブプログラムへの参加）では、別個の同意が必要となる。

(6) 同意撤回

事前の同意が必要な場合においてその同意が取得された場合、消費者は、後にオプトアウトを選択できる。

例えば、13 歳未満の消費者のデータを販売又は共有する文脈において、CPPA 規則草案は、「事業者が(a)に従って個人情報の販売又は選択に対する同意を取得した場合、事業者は、保護者又は後見人に対し、子に代わって販売・共有若しくはそのための処理をオプトアウトする権利を通知しなければならない」と規定する （CPPA 規則草案§ 7070 (Consumers Less Than 13 Years Old) ）。 つまり、同意することにより、消費者が後に考えを変えてオプトアウトすること、すなわち、同意を撤回することは妨げられない。

また、Cal Civ. Code § 1798.125(b)(3)は、個人情報の収集、個人情報の販売若しくは共有又は個人情報の保持についての消費者に対する補償の支払いといった金銭的インセンティブの提供する場合について消費者の同意を求めているが、これについても同様に、CPPA 規則草案は、事業者が消費者に対して「金銭的インセンティブの通知」を提供しなければならないとし、この通知に「いつでも金銭的インセンティブをやめる権利及び消費者がこの権利を行使する方法についての記述」が含まれなければならないとしている（CPPA 規則草案§ 7016 (Notice of Financial Incentive)）。このことから、消費者が同意の後に撤回できることが明確に示されている。

(7) その他留意事項

該当なし。

2. プロファイリング

(1) プロファイリング・データ分析に対する規律

Cal. Civ. Code § 1798.140(z)は、「プロファイリング」を、「自然人に関する特定の人的側面を評価するため、特に自然人の仕事のパフォーマンス、経済的状況、健康、好み、関心、信頼度、振舞い、位置又は動きを分析又は予測するために［…］個人情報を自動的に処理する一切の形式」と定義し、プロファイリングを含む自動化された意思決定技術（automated decision making technology）等に係る規則が作成されるべきことを規定する（Cal. Civ. Code § 1798.185(a)(16)）が、CCPA にはそれ以上の具体的なプロファイリングに関する規定は設けられていない。CCPA の同規定に基づき、CPPA は、自動化された意思決定に関する規則の制定に向け検討を開始しており、2023 年 3 月 27 日まで公衆から意見を募っていた[84]。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリング・データ分析により生成されたデータは、センシティブデータに該当しうる。CCPA に定められたセンシティブ個人情報の定義（Cal. Civ. Code § 1798.140(ae)）は、その情報がプロファイリングにより生成されたものであることを理由としてある情報がセンシティブ個人情報に該当することを否定するものではないと解されるためである。

[84] https://cppa.ca.gov/regulations/pdf/invitation_for_comments_pr_02-2023.pdf

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

CCPA の法文は、プロファイリングにより生成された個人情報に異なるルールを定めていないが、CPPA は自動化された意思決定に関する規則の制定に向け検討を進めている。

## VI. センシティブデータの取扱いに係る裁判例・決定等

センシティブ個人情報に関する CCPA の規定がごく最近の 2023 年 1 月 1 日に施行されたことからして、センシティブデータをめぐる注目すべき判例は政府の決定はまだ存在しない。例えば、カリフォルニア司法長官事務所が公表する CCPA 執行事例集には、「センシティブ個人情報」を検討するものはない。しかし、「プライバシー執行措置」と題された他のカリフォルニア司法長官事務所のページには、「センシティブ」データに短くではあるが言及する執行事例がある。それらの執行事例は、「センシティブ個人情報」に関する CCPA の規定が施行されする前のものであるため、厳密には CCPA 上のセンシティブ個人情報に関する事例ではないが、健康に関する個人情報など、各事例において対象となった個人情報について、カリフォルニア司法長官事務所が、機微性が高いものととらえた例と解される。

## VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

上記で言及したデータプライバシーに関連する法律のほか、連邦法やカリフォルニア州法により規律される「センシティブデータ」概念は見当たらない。もっとも、連邦及びカリフォルニア州の差別禁止法は、CCPA のセンシティブ個人情報の定義に含まれる特定のカテゴリーのデータを規律している。この他、本調査の趣旨に基づき現地有資格者により選定された関連のある法令として、以下の法令が挙げられている。但し、個人情報を規制する州法の性質（カリフォルニア州のみでも、個人情報の処理を規制する法律は 100 以上存在する。）により、列挙されている法令以外にも、関連する法令がある可能性がある点に留意されたい。

| **法令の名称** | **URL** | 適用対象（公的部門・民間部門） |
|---|---|---|
| カリフォルニア消費者プライバシー法（California Consumer Protection Act (CCPA), California Civil Code § 1798 *et seq.*） | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5 | 民間部門（官公庁は、営利「事業」のために契約を締結するとき、CCPA を遵守しなければならない。） |
| CCPA 規則（CCPA Regulations, California Code of Regulations, title 17 § 7001 *et seq.*） | https://cppa.ca.gov/regulations/pdf/cppa_regs.pdf | 民間部門（官公庁は、営利「事業」のために契約を締結するとき、CCPA を遵守しなければならない。） |
| カリフォルニアデータ侵害通知制定法（California's data breach notification statute laws）（公的部門について California Civil Code § 1798.29 、民間部門について California Civil Code § 1798.82） | https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.29&lawCode=CIV 及び https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.&part=4.&chapter=&article= | 公的部門（§ 1798.29 は官公庁に適用される)、民間部門 (§ 1798.82 は事業者に適用される。) |

| | | |
|---|---|---|
| カリフォルニア医療情報機密保持法（California Confidentiality of Medical Information Act, California Civil Code § 56 *et seq*.） | https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=56.10.&lawCode=CIV | 民間部門（但し、ヘルスケア提供者、健康保険会社及び契約の相手方である医療情報にアクセス可能な個人又は事業者に適用される。） |
| カリフォルニアオンラインプライバシー保護法（California Online Privacy Protection Act, California Business and Professions Code § 22575 *et seq*.） | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC | 民間部門 |
| デジタル世界におけるカリフォルニアの未成年者のプライバシー権法（Privacy Rights for California Minors in the Digital World Act, California Business and Professions Code § 22580 *et seq*.） | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.1.&lawCode=BPC | 民間部門 |
| カリフォルニア Shine the Light 法（California Shine the Light Law, California Civil Code § 1798.83） | https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV | 民間部門 |
| 消費者調査報告機関法（Investigative Consumer Reporting Agencies Act (ICRAA), California Civil Code § 1786 *et seq*.） | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.6A.&part=4.&chapter=&article=1 . | 民間部門（消費者調査報告機関に適用され、記録を主に交通安全、法執行若しくは許認可目的で保持する政府機関又はライセンスのある保険代理店、保険ブローカー、勧誘人、保険会社若しくは生命保険代理店を除く。） |
| カリフォルニア消費者信用報告機関法（California Consumer Credit Reporting Agencies Act (CCRAA), California Civil Code § 1785.1 *et seq*.） | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.6.&part=4.&chapter=1.&article= | 民間部門（消費者信用報告機関に適用され、記録を主に交通安全、法執行若しくは許認可目的で保持する政府機関を除く。） |
| 公正債権回収法（Fair Debt Collection Practices, Civil Code § 1788 *et seq*）. | https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.6C.&part=4.&chapter=&article=1 . | 民間部門（債権回収者に適用される。） |
| 遺伝情報プライバシー法（Genetic Information Privacy Act (GIPA), Civil Code § 56.18 *et seq*.） | https://law.justia.com/codes/california/2021/code-civ/division-1/part-2-6/chapter-2-6/section-56-18/ | 民間部門（消費者遺伝子検査会社を監督するために適用される。） |

# 第5章.　中国

## I.　総論

### 1.　個人情報の保護に関する法令等

中国では、个人信息保护法（PRC Personal Information Protection Law。以下、「PIPL」という）が制定されており、複数存在する同国の個人情報保護に関する法律の中でも、PIPL が中心的な法律となっていると言える。本報告書でも、PIPL に主として焦点を当てつつ、重要と解される箇所では PIPL 以外の個別の法令にも言及する。

なお、PIPL を含む法令の適用範囲については、中国の実務上、「公的部門」と「民間部門」の区別が必ずしも明確ではない。具体的には、中国には国有企業が多数あり、これは営利的又は私的な機能だけでなく、準政府的又は公的な機能も担っている場合がある。このため、本報告書において、中国については、ある法律又は規則が、国有又は政府保有の企業が準政府的な機能を果たす際の個人データの処理を規制する場合、その法律又は規則は「公的部門」に適用されるものと分類した、ある法律又は規則が、国有企業が営利的な機能を果たす際の個人データの処理を規制する場合、民間企業による個人データの処理を規制する場合と同様に、その法律又は規則は「民間部門」に適用されるものと分類した。

### 2.　センシティブデータの取扱いに対する規制の趣旨

機微な個人情報を保護し、その処理を規制することを目的として、PIPL をはじめとする、VII で挙げる法令による、センシティブデータの取扱いに対する規制が行われている。

## II.　センシティブデータの範囲―総論

PIPL 第 28 条は、「機微な個人情報」（Sensitive personal information）を次の通り定義している。

> 「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある個人情報をいい、生体認証、宗教上の信念、特定の能力、医療、健康、金融口座、居場所などに関する情報及び 14 歳未満の児童の個人情報を含む。」

この通り、PIPL の「機微な個人情報」の定義は、あくまで、個人情報が「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」かどうかである。したがって、第 28 条で列挙されていない個人情報であっても、この基準を満たす限りは、「機微な個人情報」に該当する。

例えば居場所に関する情報については、個人の正確な位置情報は、個人のプライバシーに深くかかわり、犯罪等に悪用された場合に本人に深刻な損害を与える可能性があるため、「機微な個人情報」に該当するものと解される。PIPL の実施規則がまだ公布されておらず、機微な個人情報の定義が広範に定義されているため、この定義に該当する可能性のある個人情報の種類を排他的に列挙することはできないが、下記「1.センシティブデータの範囲一覧」にある通り、情報セキュリティの技術 - 個人情報保護の詳細 (GB/T 35273-2020)がいくつかの例を提供している。

### 1.　センシティブデータの範囲一覧

当局の公表しているセンシティブデータについての解説の資料として、「情報セキュリティの技術 - 個人情報保護の詳細」という文書（以下、「詳細解説」という。）が公表されており、同文書における各データ項目に関する説明は以下の表の通りである。

| （資料の名称・URL）<br>情報セキュリティの技術 - 個人情報保護の詳細 (GB/T 35273-2020)<br>http://c.gb688.cn/bzgk/gb/showGb?type=online&hcno=4568F276E0F8346EB0FBA097AA0CE05E | |
|---|---|
| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
| 個人の財産情報 | 銀行の口座番号、認証情報（パスワード）、銀行の預金情報（預金残高、返済記録など）、不動産情報、クレジットカード情報、信用情報、取引及び消費履歴、資金フローの情報及び銀行取引明細、並びに仮想通貨、仮想取引及びゲームにおける交換コードなどの仮想財産情報など。 |
| 個人の健康情報 | 病理学的情報、入院記録、医師の指示、検査結果、手術及び麻酔の記録、看護記録、薬剤投与記録、薬剤及び食物アレルギーの情報、生殖情報、病歴、診断及び治療、家族の病歴、現在までの病歴、感染歴など医療に関連して発生した記録。 |
| 生体認証情報 | 個人の遺伝子、指紋、声紋、掌紋、耳介、虹彩及び顔認証における特徴点など。 |
| 個人識別情報 | 身分証明書、軍歴証明書、パスポート、運転免許証、社員証、社会保障カード、住民票など。 |
| その他の機微な情報 | 性的指向、結婚歴、宗教上の選好、未公表の犯罪歴、通信記録及び通信内容、連絡先、友人リスト、チャットグループのリスト、居場所の追跡記録、ウェブ閲覧履歴、宿泊情報並びに正確な位置情報など。 |

学者・有識者・実務家の資料（論文・記事等）においてセンシティブ個人情報の上記のカテゴリーごとに分けてその例、趣旨や範囲等についての個別に具体的に説明した資料は特に見当たらない。

2. センシティブデータを推知させる情報（推知情報）について

この点に関する中国の規制当局から明確なガイダンスは特に見当たらない。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。

(i) 医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する。

(ii) 事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。

(iii)　消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。PIPL 第 28 条の「機微な個人情報」の定義においては、健康に関する情報を、その情報を取得した検査の実施主体で区別することはしていない。従って、検査結果が個人の健康に関する情報である限りは、センシティブデータに該当すると解される。

(iv)　消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する。 PIPL 第 28 条の「機微な個人情報」の定義においては、健康に関する情報を、その情報を取得した検査の実施主体で区別することはしていない。従って、検査結果が個人の健康に関する情報である限りは、センシティブデータに該当すると解される。

(v)　予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無は、センシティブデータに該当する。予防接種に関する情報は一般的に健康に関する情報として「機微な個人情報」に該当しすると解される。

(2)　趣旨

健康に関するデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人の安全を脅かす事態が容易に起こり得ると考えられるためである。

(3)　追加的規律（該当する場合）

PIPL の他に健康に関するデータに適用される法令として、母集団健康情報に関する管理弁法[85]が挙げられる。この法令は、国民の健康情報の管理に関する安全対策を定めたものであり、あらゆるレベルの医療・保健サービス機関による、国民の健康情報の収集、管理、利用、安全、プライバシー保護に適用される。

2.　遺伝子に関するデータ

(1)　センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、特にその種類を問うことなく、センシティブデータに該当する。個人の生体認証に関する情報は、PIPL 第 28 条の「機微な個人情報」の定義に明示的に含まれており、詳細解説は、遺伝子情報が生体認証に関する情報の範囲に含まれるとしている。

(i)　医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。遺伝子に関する情報は、詳細解説によれば生体認証に関する情報を構成し、PIPL 第 28 条の「機微な個人情報」の定義において

[85] http://www.nhc.gov.cn/guihuaxxs/gongwen12/201405/783ec8adebc6422bbebdf79db3868d0b.shtml

は、生体認証に関する情報を、その情報を取得した検査の実施主体で区別することはしていない。従って、検査結果が個人の遺伝子に関する情報である限りは、センシティブデータに該当すると解される。

(ii) 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する。遺伝子に関する情報は、詳細解説によれば生体認証に関する情報を構成し、PIPL 第 28 条の「機微な個人情報」の定義においては、生体認証に関する情報を、その情報を取得した検査の実施主体で区別することはしていない。従って、検査結果が個人の遺伝子に関する情報である限りは、センシティブデータに該当すると解される。

(iii) 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当する。遺伝子に関する情報は、詳細解説によれば生体認証に関する情報を構成し、PIPL 第 28 条の「機微な個人情報」の定義においては、生体認証に関する情報を、その情報を取得した検査の実施主体で区別することはしていない。従って、検査結果が個人の遺伝子に関する情報である限りは、センシティブデータに該当すると解される。

(2) 趣旨

遺伝子に関するデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人の安全を脅かす事態が容易に起こり得ると考えられるためである。

(3) 追加的規律（該当する場合）

PIPL の他に遺伝子に関するデータに適用される法令として、ヒト遺伝資源に関する管理規則[86]が挙げられる。この規則では、中国のヒト遺伝資源の収集、保存、利用、海外への提供に関する規則と事前承認要件等が定められている。 例えば、①外国人又は外国人支配者が中国のヒト遺伝資源を収集、保存、海外に提供することは認められない、②中国のヒト遺伝資源の販売は厳しく禁止されている、などの規律を設けている。

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的趣向に関するデータは、センシティブデータに該当する。詳細解説には、個人の性的指向に関する情報が機微な個人情報に該当すると記載されている。個人の性生活に関する情報は、機微な個人情報として明示されていないが、一般的には性的指向に関する情報の一部を形成すると考えられている

(2) 趣旨

[86] https://flk.npc.gov.cn/detail2.html?ZmY4MDgwODE2ZjNjYmIzYzAxNmY0MTQ3MmYxOTFmZDY

性生活・性的指向に関するデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人の安全を脅かす事態が容易に起こり得ると考えられるためである。

(3) 追加的規律（該当する場合）

特になし。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータがセンシティブデータに該当する可能性はあるが、この点に関して中国の規制当局による明確なガイダンスは特に見当たらない。センシティブデータへの該当性は、PIPL 上の機微な個人情報の定義のうち、「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」情報であるかという基準への該当性に基づき判断される。

(2) 趣旨

労働組合への加入に関するデータの中には、政治的意見や特定の能力に関するものもあり、そのようなデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人の安全を脅かす事態が起こりうると考えられるためである。

(3) 追加的規律（該当する場合）

特になし。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、特にその種類を問うことなく、センシティブデータに該当する。

(2) 趣旨

生体データが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人の安全を脅かす事態が容易に起こり得ると考えられるためである。

(3) 追加的規律（該当する場合）

PIPL の他、自然人を一意に識別することを目的とする生体データには次の法令が適用される。

- 顔認証技術による個人情報の処理を伴う民事事件の処理における法律の適用に関する複数の問題についての最高人民法院の解釈[87]

  この文書の内容は、法律、規制又は当事者の合意に違反して、顔認識技術を使用して顔情報を収集、保存、使用、処理、移転、提供又は公開することに関わる民事事件に適用される。

- インターネット情報サービスにおけるディープシンセシス(深層合成)に関する管理弁法[88]

  本文書は、中国国内でインターネット情報サービスを提供するために深層合成技術を利用する場合に適用される規則を定めたものであり、一般的な義務、データ及び技術の仕様、サービス提供者の法的義務などが含まれる。生体認証に関する情報について、顔や人の声などのバイオメトリクス情報を編集する深層合成サービスに従事する事業者に対し、本人の同意を得ること、及び深層合成技術で使用される基礎モデル、テンプレート、又はその他のツールのセキュリティ評価を実施することを求めている。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータは、センシティブデータに該当する。銀行の口座番号、認証情報（パスワード）、銀行の預金情報（預金残高、返済記録など）、不動産情報、クレジットカード情報、信用情報、取引及び消費履歴、資金フローの情報及び銀行取引明細、並びに仮想通貨、仮想取引及びゲームにおける交換コードなどの仮想財産情報などのデータがセンシティブデータに該当する。

(2) 趣旨

金融・財産に関するデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人若しくは個人の財産の安全を脅かす事態が容易に起こり得ると考えられるためである。そのような事態を生じさせうる場合の具体例としては、弁済期限を溶かした事実に関する情報が漏えいした場合などが考えられる。

(3) 追加的規律（該当する場合）

PIPL の他、金融・財産に関するデータには次の法令が適用される。

- バンクカードの決済代行会社に関する管理弁法[89]

  金融情報のセキュリティを強化するために、銀行カード決済機関に適用される規則を定める。事業者に適用される主な義務には、①ネットワークセキュリティ法の遵守、②銀行カードによる清算についてのサービスから取得した ID 情報、口座情報、取引情報その他の関連する機密情報の機密保持などがある。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

[87] https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3Yjk2OTcxYzAxN2I5YmJiYjgyOTEzZWE%3D
[88] http://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm
[89] http://www.gov.cn/gongbao/content/2016/content_5109339.htm

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータのうち、クレジットの記録、信用情報、取引及び消費の記録、資金フローの記録、銀行取引明細などがセンシティブデータに該当する。詳細解説は、これらの種類の情報を機微な個人情報として列挙している。その他の信用情報が機微な個人情報に該当するかどうかは不明であるが、その情報が「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」限り、そのデータはセンシティブデータに該当するに該当する。

(2) 趣旨

信用に関するデータが漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する事態又は個人若しくは個人の財産の安全を脅かす事態が容易に起こり得ると考えられるためである。

(3) 追加的規律（該当する場合）

PIPL の他、信用に関するデータには次の法令が適用される。

- 信用調査業に関する管理弁法[90]
- 信用調査業に関する行政規則[91]
- 個人の信用情報の基礎的データベースの運用に関する暫定弁法[92]

  これらの文書は、個人の信用に関する情報を処理するにあたり適用される規律を定めており、信用情報に関するセキュリティ要件などが規定されている。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報がセンシティブデータに該当する可能性はあるが、この点に関して中国の規制当局による明確なガイダンスは特に見当たらない。センシティブデータへの該当性は、PIPL 上の機微な個人情報の定義のうち、「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」情報であるかという基準への該当性に基づき判断される。

(2) 趣旨

政府等の金銭的保護を受けている事実に関するデータは、漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある場合には、該当する可能性があると考えられる。

[90] http://www.gov.cn/gongbao/content/2021/content_5654782.htm
[91] http://www.gov.cn/zhengce/2013-01/29/content_2602614.htm
[92] http://www.pbccrc.org.cn/zxzx/zhengcfg/202208/76c37535beb94d128e1d981f813adcb3.shtml

(3) 追加的規律（該当する場合）

特になし。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報がセンシティブデータに該当する可能性はあるが、この点に関して中国の規制当局による明確なガイダンスは特に見当たらない。。センシティブデータへの該当性は、PIPL 上の機微な個人情報の定義のうち、「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」情報であるかという基準への該当性に基づき判断される。

(2) 趣旨

成年後見制度の保護を受けている事実に関するデータは、漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性があるとき、該当する可能性があると考えられる。

(3) 追加的規律（該当する場合）

特になし。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

14 歳未満の児童のデータはセンシティブデータに該当する。PIPL 第 28 条において、14 歳未満の児童の個人情報がの「機微な個人情報」に含まれることを明記している。

(2) 趣旨

14 歳未満の児童の保護のため。

(3) 追加的規律（該当する場合）

PIPL 第 31 条は、児童に関する情報について、次の通り規定している。

> 「14 歳未満の児童の個人情報を処理する場合、個人情報取扱者（個人情報処理活動の過程で、処理目的及び方法を独自に決定する組織又は個人）は当該児童の両親又はその他の保護者の同意を得なければならない。

14 歳未満の児童の個人情報を処理する個人情報取扱者は、当該処理に特化した規則を策定するものとする。」

これにより、具体的には、14 歳未満の児童の個人上を処理する場合には、それに対応したプライバシーポリシーの作成が必要となる。

また、PIPL 第 72 条は次の通り規定している。

「インターネットを通じ未成年者の個人情報を処理する個人情報取扱者は、適法性、正当性及び必要性の原則を遵守しなければならない。個人情報取扱者が 14 歳未満の児童の個人情報を処理する場合、法令に別段の定めがある場合を除き、当該児童の両親又はその他の保護者の同意を得なければならない。

個人情報取扱者は、未成年者又はその他の保護者から個人情報の訂正又は削除を求められた場合には、法令に別段の定めがある場合を除き、速やかに当該個人情報の訂正又は削除の措置を講じなければならない。」

PIPL の他に児童に関するデータに適用される法令として、児童の個人情報のネットワークの保護に関する規則[93]が挙げられる。

11. オンライン行動履歴に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報がセンシティブデータに該当する可能性はあるが、この点に関して中国の規制当局による明確なガイダンスは特に見当たらない。センシティブデータへの該当性は、PIPL 上の機微な個人情報の定義のうち、「漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性がある」情報であるかという基準への該当性に基づき判断される。詳細解説では、ウェブ閲覧履歴が「機微な個人情報」に該当する具体例として挙げられており、このことから、オンライン行動履歴に関するデータが該当する可能性が高いと解される。

(2) 趣旨

オンライン行動履歴に関するデータは、漏えいした場合又は違法に利用された場合、自然人たる個人の尊厳を害する可能性又は個人若しくは個人の財産の安全を脅かす可能性があると考えられるためである。

(3) 追加的規律（該当する場合）

特になし。

[93] http://www.gov.cn/zhengce/2019-10/08/content_5728947.htm

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

PIPL は、個人情報の処理に適用される。「処理」（Processing）とは、個人情報の取得、保存、利用、追加処理、移転、提供、公開、削除を含む広範な定義である（第 4 条）。機微な個人情報の処理に関する加重要件は、第 28 条から第 32 条及び第 55 条で規定される。

具体的には、以下の加重要件が機微な個人情報の処理に適用される。

- 個人情報取扱者は、十分な必要性及び特定された目的があり、厳格な保護措置が講じられている場合に限り、機微な個人情報を処理できる（第 28 条）。
- 機微な個人情報の処理には、別途本人の同意を必要とする（第 29 条）。
- 機微な個人情報を処理する場合、個人情報取扱者は、他の法令が秘密とすることを必要とする若しくは通知を不要とする場合又は通知により政府の法的な責任の遂行が妨げられる場合を除き、機微な個人情報の処理の必要性並びに本人の権利及び利益に及ぶ影響について、本人に通知しなければならない（第 30 条）。
- 法律又は行政規則が機微な個人情報の処理に行政上の許可を必要とする場合又はその他の制限を課している場合は、それらが優先されるものとする（第 32 条）。
- 個人情報取扱者は、機微な個人情報を処理する場合、まず個人情報保護に与える影響を評価し、処理内容を記録しなければならない（第 55 条）。

### 2. 利用

上記 1 の通り、個人情報の「処理」には利用が含まれる。機微な個人情報の利用に適用される規律は、上記 1 の通りである。

### 3. 第三者提供

上記 1 に記載の規律に加え、機微な個人情報を含む個人情報の移転には、PIPL 第 21 条から第 23 条及び第 55 条も適用される。

それらの具体的な内容は以下の通りである。

- 個人情報取扱者が個人情報の処理を第三者に委託する場合、個人情報取扱者は、委託された処理目的及び方法、処理の期限、個人情報の種類、保護措置、各当事者の権利及び義務等について受託者と合意し、受託者による個人情報の処理について監督するものとする（第 21 条）。
- 個人情報取扱者の同意がない場合、受託者は、個人情報の処理をさらに第三者に委託することはできないものとする（第 21 条）。
- 個人情報取扱者は、合併、分割、解散、破産宣告などにより個人情報を移転する必要がある場合、移転先の名前及び連絡先を本人に通知し、受領者は引き続き個人情報取扱者の義務を履行するものとする（第 22 条）。
- 個人情報取扱者が、自信が処理した個人情報を他の個人情報取扱者に提供する場合、情報を提供する個人情報取扱者は、受領者の名前及び連絡先、処理目的及び方法、個人情報の種類を本人に通知し、別途本人の同意を得なければならない（第 23 条）。

- 個人情報取扱者は、個人情報の処理を第三者に委託する場合又は他の個人情報取扱者に個人情報を提供する場合には、まず個人情報保護に与える影響を評価し、処理内容を記録しなければならない（第 55 条）。

個人情報の越境移転においては、PIPL 第 38 条から第 43 条及び第 55 条並びにデータ輸出の安全評価措置の規定も適用される。

具体的には、次の規定が適用される。

- 業務上又はその他の理由により真に必要とされる場合、以下の条件のいずれかを満たせば、国外の受領者に個人情報を提供できる（第 38 条）。
  (1) 個人情報取扱者が、国家サイバースペース機関が主催するセキュリティ評価に合格していること。
  (2) 個人情報取扱者が、国家サイバースペース機関の規則に従い、専門機関による個人情報保護認証を受けていること。
  (3) 個人情報取扱者が、国外の受領者との間で、国家サイバースペース機関制定の標準契約に準拠した契約を締結し、その契約において両当事者の権利及び義務が規定されていること。
  (4) 法律、行政法規又は国家サイバースペース機関が求めるその他の条件を満たすこと
- 個人情報取扱者は、国外の受領者による個人情報の処理が PIPL に定める個人情報保護基準に適合するよう、必要な措置を講じなければならない（第 38 条）。
- 個人情報取扱者は、国外の受領者に個人情報を提供する場合、当該受領者の名前及び連絡先、処理目的及び方法、個人情報の種類並びに当該受領者に対し PIPL 上の権利を行使する方法及び手続きなどを本人に通知し、別途本人の同意を得なければならない（第 39 条）。
- 個人情報取扱者は、国外の受領者に個人情報を提供する場合、まず個人情報保護に与える影響を評価し、処理内容を記録しなければならない（第 55 条）。

機微な個人情報については、データ輸出の安全性評価弁法第 4 条に基づき、安全性評価が必要となる基準が低く設定されており、通常の個人情報に比べて、安全性評価が必要な場合が拡大されている。具体的には、次の通り規定されている。

- 前暦年の 1 月 1 日以降累計で 10 万人以上の個人情報を国外に提供する場合又は累計で 1 万人以上の機微な個人情報を国外に提供する場合、国家サイバースペース機関に安全評価を申請しなければならない。

4. 管理

PIPL は「管理」について特に言及していないが、「処理」の定義が広い（取得、保存、利用、追加処理、移転、提供、公開及び削除）ことから、PIPL 第 28 条から第 32 条及び第 55 条規定の、機微な個人情報の処理に関する要件は、管理にも適用されるものと考えられる。

具体的には以下の義務が課されるものと解される。

- 個人情報取扱者は、十分な必要性及び特定の目的があり、厳格な保護措置が講じられている場合に限り、機微な個人情報を処理できる（第 28 条）。
- 機微な個人情報の処理には、別途本人の同意を必要とする（第 29 条）。

- 機微な個人情報を処理する場合、個人情報取扱者は、PIPL が本人に通知する必要がないことを定めた場合を除き、機微な個人情報の処理の必要性並びに本人の権利及び利益に及ぶ影響について、本人に通知しなければならない（第 30 条）。
- 法律又は行政規則が機微な個人情報の処理に行政上の許可を必要とする場合又はその他の制限を課している場合は、それらが優先されるものとする（第 32 条）。
- 個人情報取扱者は、機微な個人情報を処理する場合、まず個人情報保護に与える影響を評価し、処理内容を記録しなければならない（第 55 条）。

5. 漏えい等

PIPL 第 57 条は、個人情報の漏えい、毀損又は滅失の可能性がある場合に関して規定するが、機微な個人情報が含まれる場合とそうでない場合との区別はしていない。
具体的には、次の規定が適用される。

- 個人情報取扱者は、速やかに改善措置を講じ、個人情報保護業務を行う規制当局及び本人に通知しなければならない。通知には、以下の内容を含めるものとする。

(1) 漏えい、不正な改変若しくは滅失が発生した、又は発生するおそれのある個人情報の種類並びにそれらの原因及びそれらにより生じうる被害

(2) 個人情報取扱者が講じた改善措置及び本人が被害を軽減するために講じられる措置

(3) 個人情報取扱者の連絡先

- 個人情報取扱者が情報の漏えい、不正な改変又は滅失による被害を防止できる有効な措置を講じている場合、個人情報取扱者による本人に対する通知は要しないものとする。

6. 請求権

PIPL 第 15 条及び第 44 条から第 50 条は、データ主体の権利を規定するが、これらの条項では、機微な個人情報が含まれる場合とそうでない場合との区別はしていない。

具体的には、次の規定が適用される。

- 本人は、本人の同意に基づく個人情報の処理について、その同意を撤回する権利を有する（第 15 条）。
- 本人は、自己の個人情報の処理について知らされる権利及び決定する権利並びに他者による自己の個人情報の処理を制限又は拒否する権利を有する（第 44 条）。
- 本人は、個人情報取扱者が保有する自己の個人情報を閲覧及び謄写する権利を有する。ただし、法令に基づき秘密が保持される必要がある場合又はその提供が政府の活動を阻害する可能性がある場合は、この限りでない（第 45 条）。
- 個人情報取扱者は、本人から自己の個人情報の閲覧又は謄写を求められたときは、適時これらを行わなければならない。個人情報取扱者は、本人により指定された個人情報取扱者への個人情報の提供が求められた場合、その求めが国家サイバースペース機関の課す条件を満たしているときは、これを提供できるようにしなければならない（第 45 条）。
- 本人が自己の個人情報が不正確又は不完全であることを発見した場合、本人は個人情報取扱者に対してその訂正又は補完を請求する権利を有するものとする。個人情報の訂正又は補完を求められた場合、個人情報取扱者は、個人情報を確認し、適時、訂正又は補完をしなければならない（第 46 条）。

- 次に掲げる場合、個人情報取扱者は自ら個人情報を消去しなければならない。個人情報取扱者が自ら消去しない場合、本人は、個人情報取扱者に対し、消去を求める権利を有する（第 47 条）。
  (1) 処理目的が達成された場合若しくは達成されなくなった場合又は処理目的の達成に当該個人情報が必要でなくなった場合
  (2) 個人情報取扱者が製品又はサービスの提供を中止した場合又は保存期間が満了した場合
  (3) 本人が同意を撤回した場合
  (4) 個人情報取扱者が法令若しくは行政法規に違反した場合又は契約に違反して個人情報を処理した場合
  (5) その他法令に定める場合
- 本人は、個人情報取扱者に対し、個人情報の処理について説明を求める権利を有するものとする（第 48 条）。
- 個人情報取扱者が本人による権利行使の求めを拒否する場合、当該本人は法律に従い人民法院に訴訟を提起できるものとする（第 50 条）。

上記に加え、機微な個人情報について、データ主体は、PIPL 第 30 条に基づき、処理の必要性並びに個人の権利及び利益に与える影響について知らされる権利も有する。

## V. 本人同意、プロファイリング

### 1. 本人同意

#### (1) センシティブデータ規制（上記III）との関係

PIPL は、機微な個人情報の処理に関する加重要件として、機微な個人情報の処理には、別途本人の同意を必要としている（第 29 条）。

#### (2) 要件一般

PIPL において、機微な個人情報の処理についての同意に関する要件一般についての定めは特に見当たらない。

#### (3) 情報提供

個人情報を処理する場合、機微な個人情報であるか否かを問わず、PIPL 第 17 条に基づき以下の情報の提供が必要となる。

- 個人情報取扱者の名前及び連絡先
- 処理目的及び手段
- 処理する個人情報の種類
- 個人情報の保存期間
- データ主体が権利を行使する方法及び手順

さらに、機微な個人情報を処理する場合、PIPL 第 30 条に基づき、以下の情報の提供も必要となる。

- 処理の必要性
- 処理が本人の権利及び利益に与える影響

(4) 形式

法令上は明確な規定はないが、実務上は個人情報取扱者が、同意を取得していることの証明責任を負う。

(5) 個別同意の必要性

法令上、個人情報の処理行為や目的毎に同意を得ることを求める明確な規定はない。機微な個人情報の処理に際しては、別途本人の同意が必要である。実務上、「機微な個人情報」処理ついての複数の処理行為や目的を対象とした同意を取得するケースが見られており、その適法性を否定する当局の判断は特に見当たらない。

(6) 同意撤回

処理の法的根拠が同意である場合は撤回できる。

(7) その他留意事項

14 歳未満の児童の個人情報を処理する場合は、親又はその他法定代理人の同意を得る必要がある。

2. プロファイリング

(1) プロファイリング・データ分析に対する規律

PIPL 第 24 条及び第 55 条は、プロファイリング・データ分析に関して、次の通り定める。

- 個人情報を自動化された意思決定（個人の行動、習慣、興味若しくは趣味又は個人の経済状況、健康若しくは信用状況などについて、コンピュータープログラムによる自動的な分析及び評価を経てなされる意思決定）のために利用する個人情報取扱者は、意思決定の透明性及び結果の公正さを確保し、本人に対し取引価格など当該取引の条件に関する不当な差別的取り扱いを行ってはならない（第 24 条）。
- 本人の権利及び利益に重大な影響を与える意思決定において自動化された意思決定が用いられる場合、本人は、個人情報取扱者に対し説明を求める権利及び自動化された意思決定のみを手段としてなされる個人情報取扱者の意思決定を拒否する権利を有するものとする（第 24 条）。
- 個人情報取扱者は、個人情報を自動化された意思決定に利用する場合、まず個人情報保護に与える影響を評価し、処理内容を記録しなければならない（第 55 条）。

インターネットのポップアップウィンドウによるプッシュ通知サービスに関する管理弁法第 5 条は、未成年者に対するポップアップウィンドウによるプッシュ通知に関連して、プロファイリングについて次の通り定める。

- インターネットポップアップウィンドウによるプッシュ通知サービスを提供する場合、アルゴリズムを利用して未成年者をプロファイリングしたり、未成年者の身体的又は精神的健康に影響を与える可能性のあるプッシュ通知をしてはならない。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリング・データ分析により生成されたデータは、センシティブデータに該当しうる。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

プロファイリングやその他のデータ分析によって生成された個人情報が、機微な個人情報の定義を満たす場合、上記 IV の機微な個人情報の取扱いに係る規律と同様のものが適用される。

## VI. センシティブデータの取扱いに係る裁判例・決定等

機微な個人情報の不正な処理に関する事例や公になった処分はあったが、社会的に問題になったとは考えられないため、ここでは割愛する。

## VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

上記で言及したデータプライバシーに関連する法律のほか、本調査の趣旨に基づき現地有資格者により選定された関連のある法令として、以下の法令が挙げられている。

| 法令の名称 | URL | 公的部門と民間部門のいずれを対象とするか |
|---|---|---|
| 个人信息保护法<br>（個人情報保護法） | https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3YjY0NzJhMzAxN2I2NTZjYzIwNDAwNDQ%3D | 両部門 |
| 网络安全法<br>（サイバーセキュリティ法） | https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4Mjc2ZjA5M2Q%3D | 両部門 |
| 民法典<br>（民法） | http://regional.chinadaily.com.cn/pdf/CivilCodeofthePeople'sRepublicofChina.pdf | 両部門 |
| 刑法修正案（九）<br>（刑法修正案（九））| https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY2OTBiYjA0YWI%3D | 両部門 |

| | | |
|---|---|---|
| 刑法修正案（七）<br><br>（刑法修正案（九））| https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY2OGI0NjA0OTc%3D | 公的部門 |
| 电子商务法<br><br>（電子商取引法） | https://flk.npc.gov.cn/detail2.html?MmM5MDlmZGQ2NzhiZjE3OTAxNjc4YmY4YWYwNTBiODE%3D | 民間部門 |
| 最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释<br><br>（人民の個人情報侵害の刑事事件の処理における法律の適用に関する複数の問題についての最高人民法院及び最高人民検察院の解釈） | https://flk.npc.gov.cn/detail2.html?NDAyODgxZTQ1ZmZiYmU0MTAxNWZmYmZjMTExYTAzNTA%3D | 両部門 |
| 最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定<br><br>（顔認証技術による個人情報の処理を伴う民事事件の処理における法律の適用に関する複数の問題についての最高人民法院の解釈） | https://flk.npc.gov.cn/detail2.html?ZmY4MDgxODE3Yjk2OTcxYzAxN2I5YmJiYjgyOTEzZWE%3D | 民間部門 |
| 电信和互联网用户个人信息保护规定<br><br>（電気通信事業者及びインターネット利用者の個人情報保護に関する規則） | http://www.gov.cn/zhengce/2022-08/23/content_5722717.htm | 民間部門 |
| 儿童个人信息网络保护规定<br><br>（児童の個人情報のネットワーク保護に関する規則） | http://www.gov.cn/zhengce/2019-10/08/content_5728947.htm | 民間部門 |
| 汽车数据安全管理若干规定（试行）<br><br>（車両データのセキュリティ管理に関する複数の規制（試行）） | http://www.gov.cn/zhengce/zhengceku/2021-09/12/content_5640023.htm | 民間部門 |
| 数据出境安全评估办法<br><br>（データ輸出時の安全評価弁法） | http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm | 民間部門 |

| | | |
|---|---|---|
| 互联网信息服务算法推荐管理规定<br><br>（インターネット情報サービスにおけるアルゴリズムによる推薦に関する管理弁法） | http://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm | 民間部門 |
| 互联网用户账号信息管理规定<br><br>（インターネット利用者のアカウント情報に関する管理弁法） | http://www.gov.cn/zhengce/zhengceku/2022-06/28/content_5698179.htm | 民間部門 |
| 互联网信息服务深度合成管理规定<br><br>（インターネット情報サービスにおけるディープシンセシス（深層合成）に関する管理弁法） | http://www.gov.cn/zhengce/zhengceku/2022-12/12/content_5731431.htm | 民間部門 |
| 人类遗传资源管理条例<br><br>（ヒト遺伝資源に関する管理規則） | https://www.most.gov.cn/xxgk/xinxifenlei/fdzdgknr/fgzc/flfg/201906/t20190612_147044.html | 民間部門 |
| 人口健康信息管理办法（试行）<br><br>（母集団健康情報に関する管理弁法（施行）） | http://www.nhc.gov.cn/guihuaxxs/gongwen12/201405/783ec8adebc6422bbebdf79db3868d0b.shtml | 公的部門 |
| 网络交易监督管理办法<br><br>（オンライン取引の監督及び管理に関する弁法） | http://www.gov.cn/zhengce/zhengceku/2021-03/16/content_5593226.htm | 民間部門 |
| 银行卡清算机构管理办法<br><br>（バンクカード（銀行が発行するクレジットカード） の決済代行会社に関する管理弁法） | http://www.gov.cn/gongbao/content/2016/content_5109339.htm | 民間部門 |
| 网络预约出租汽车经营服务管理暂行办法<br><br>（オンライン配車オペレーションサービス管理に関する暫定弁法） | http://www.gov.cn/zhengce/2022-08/23/content_5722697.htm | 民間部門 |
| 征信业管理条例<br><br>（信用調査業に関する管理規則） | http://www.gov.cn/zhengce/2013-01/29/content_2602614.htm | 民間部門 |

# 第6章. インド

## I. 総論

### 1. 個人情報の保護に関する法令等

個人情報の保護に関する法令として、2000 年情報技術法（Information Technology Act）（以下「IT 法」という。）[94]、及び同法に基づき制定された 2011 年情報技術規則（合理的なセキュリティ慣行及び手順並びにセンシティブデータ（sensitive personal data or information. 以下「SPDI」という。）に関する規則）（Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011）（以下「SPDI 規則」という。）[95]が存在する。本調査においては、IT 法及び SPDI 規則を主に対象として回答を行っている。なお、これらの法令は公的部門、民間部門のいずれも対象としている。

### 2. センシティブデータの取扱いに対する規制の趣旨

SPDI 規則の趣旨は、センシティブデータを保護するために、合理的なセキュリティ慣行及び手順を規定する点にある。SPDI 規則の根拠となる規定である IT 法 43-A 条において、自己が所有・管理し、又は運営するコンピュータリソースにおいて、SPDI を処理・取引し、又は取り扱う法人等（IT 法上、組合等も含む概念として body corporate という語が用いられており、その訳語として「法人等」としている。以下、本章において同じ）は、合理的なセキュリティ慣行及び手順の実施又は維持を怠り、それにより不当な損害又は不当な利得を与えた場合は、影響を受けた者に補償として損害を賠償する責任を負う旨が規定されている。

## II. センシティブデータの範囲—総論

### 1. センシティブデータの範囲一覧

IT 法 43A 条と SPDI 規則は、以下に関する個人情報を SPDI として指定する。

(i) パスワード

(ii) 銀行口座、クレジットカード、デビットカードその他支払手段等の金融情報

(iii) 身体的、生理学的又は精神的健康状態

(iv) 性的指向

(v) 医療記録及び病歴

(vi) 生体認証に関する情報

(vii) サービス提供のために法人等に提供された上記各号の情報

(viii) 合法的な契約等に基づき処理、保存又は加工するために法人等が受領した上記各号の情報

[94] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
[95] https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf

なお、(vii)及び(viii)はデータの内容としては上記(i)から(v)と同様のものを指し、それらが外部からのサービス提供の一環として授受されたとしても SPDI に該当することを規定したものであると解される。

ただし、公開されている情報、又は自由にアクセス可能な情報、若しくは IT 法その他施行された法律に基づきもたらされる情報は、SPDI にはあたらない。

なお、「個人情報」（personal information）は、自然人に関する情報であって、直接又は間接に、法人等に利用可能又はその可能性がある他の情報と組み合わせて、個人を特定することができる一切の情報を意味する。

当局の公表している主要な資料、あるいは学者・有識者・実務家の資料（論文・記事等）においてセンシティブデータに関してその例、趣旨や範囲等について個別に具体的に説明したものは特に見当たらない。上記の SPDI のうち、一部のデータ項目については SPDI 規則上に次のような規定が存在する。

（資料の名称・URL）
SPDI 規則は、一部の SPDI の特定のカテゴリーの範囲と意味について、ガイダンスを提供している。

| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
|---|---|
| 生体認証（Biometrics） | SPDI 規則は、「生体認証」を、指紋、網膜及び光彩、声紋、顔面パターン、指の長さ並びに DNA 等の人の身体の特徴を認証目的のために測定及び分析する技術を意味するものとして定義する。 |
| パスワード | SPDI 規則は、「パスワード」を、入場又は情報へのアクセスを得るために使用する、秘密の言葉、フレーズ、コード、パスフレーズ、シークレットキー又は暗号化若しくは復号化の鍵を意味するものとして定義する。 |

2. センシティブデータを推知させる情報（推知情報）について

推知情報は、SPDI 規則における SPDI に当たらない。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。身体的、生理学的及び精神的な健康状態並びに医療記録及び病歴に関する個人情報は、SPDI に該当するためである。

(i) 医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する。医療記録及び病歴は SPDI に該当するためである。

(ii) 事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

医師等の判断を介していない検査結果は、それが、事業者にとって利用可能又はその可能性がある他の情報との組み合わせにより自然人を特定することができる、身体的、生理学的又は精神的健康状態に関連する情報（サーマルカメラによる体温検査等）を含む限りにおいては、センシティブデータに該当する。

(iii) 消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

医師等の判断を介していない検査結果は、センシティブデータに該当しないと考えられる。SPDI 規則は、SPDI を取り扱う法人という文脈でのみ適用されるところ、個人たる消費者が市販の検査機器を利用して行った検査結果は、健康状態に関連する情報が法人によって処理されるわけではないから、SPDI に基づく義務は適用されない。しかしながら、かかる検査結果が法人に提供された場合には、上記(ii)と同様にセンシティブデータに該当する。

(iv) 消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当しない。設問 III.1(1)(iii)への回答を参照。しかしながら、かかる健康状態の情報は、身体的、生理学的又は精神的健康状態についての情報に該当すると解されるため、かかる情報が法人に提供された場合にはセンシティブデータに該当する。

(v) 予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無は、センシティブデータに該当しない。その内容が身体的、生理学的又は精神的健康状態についての状態についての情報にも該当しないと解されているためである。

(2) 趣旨

SPDI 規則からは、SPDI の各カテゴリに関する明確な立法目的は明らかではない。一定の情報を SPDI として総合的に分類した趣旨については、上記 I. 2 を参照されたい。

(3) 追加的規律（該当する場合）

国家デジタルヘルスミッションを立案する責任を負っている保険家族福祉省（Ministry of Health and Family Welfare）は、個人又はデータ主体の健康に関するデジタルデータのプライバシー保護のため、健康データ管理ポリシー（Health Data Management Policy）（以下「HDM ポリシー」という。）[96]を公表している。HDM ポリシーは国家デジタルヘルスエコシステム（インド政府が立ち上げた、安全で相互運用可能なデジタルヘルス・インフラを構築するためのイニシアチブ（National Digital Health Mission）の一部。異なる医療提供者や利害関係者間でのシームレスな医療情報の交換を可能にするデジタルシステム、レジストリ、リポジトリのネットワークとして構想されている）を通じた、法令順守のためのガイダンスとして機能し、対象者が従うべきデータプライバシー保護の最低基準を定めている。このガイダンスの対象者には以下のようなものが含まれる。

(a) HDM ポリシーに基づき ID を発行されたすべての法人及び個人

(b) 医師や医療従事者（アーユルヴェーダ、ヨーガ、自然療法、ユナニ、シッダ、ホメオパシーなど、公認のインド医学体系を実践する者を含む）、看護師、検査技師、その他の医療従事者を含むが、これらに限定されない医療従事者

(c) 保健家族福祉省、国家衛生局、関連専門機関、規制当局の管理機関

(d) 健康情報提供者

(e) 取引に関連して電子形式で個人データを収集、保存、送信する医療施設

(f) 中央政府、州政府、保険会社、慈善団体等

[96] https://abdm.gov.in:8081/uploads/health_management_policy_bac9429a79.pdf

(g) 医薬品製造業者、医療機器製造業者、及び関連サプライチェーンに関与する事業体

(h) 研究機関、健康データ分析のためにデータを利用する研究者を含む研究者個人、統計学者、アナリスト、公衆衛生機関などの研究機関

(i) 国家デジタルヘルスエコシステムの一環として個人データを収集又は処理するすべての個人及び事業体等

HDM ポリシーは、データ主体（個人）の個人情報を取得するための同意の枠組みを規定し、個人情報が収集及び処理される方法についてデータ主体がコントロール及び意思決定に関する権限を保持することを強調している。

また、HDM ポリシーは、データ主体に対して個人データの収集及び処理についてプライバシー通知を行うこと並びにその方法について定めている。それによれば、特に 18 歳以下の者を子供とし、子供の個人データを扱うデータ受託者（データ管理者に類似している。）は、保護者の同意を得たうえで、「子供の利益を最優先」してデータを取り扱わなければならない。データ受託者は、アカウンタビリティ、透明性、プライバシーバイデザイン、選択・同意を基礎とした共有、目的制限、データの質並びに合理的なセキュリティ慣行及び手順等の取扱原則を守らなければならない。

2. 遺伝子に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

SPDI 規則上、遺伝子に関するデータは SPDI として明確に分類されているわけではないことから、直ちにセンシティブデータに該当するとは言えない。もっとも、遺伝子に関するデータは身体的若しくは生理学的情報又は医療記録及び病歴に該当し得るため、かかる場合にはセンシティブデータに該当するといえる。

(i)　医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。医師による検査結果であれば、身体的若しくは生理学的情報又は医療記録及び病歴に該当すると解されるためである。

(ii)　消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

医師等の判断を介していない検査結果は、センシティブデータに該当しないと考えられる。SPDI 規則は、SPDI を取り扱う法人という文脈でのみ適用されるところ、個人たる消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、検査結果が法人によって処理されるわけではないから、SPDI に基づく義務は適用されない。しかしながら、かかる検査結果が法人に提供された場合には、その内容が身体的若しくは生理学的情報又は医療記録及び病歴に該当する場合には、当該法人に SPDI が適用される。

(iii)　消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当しないと考えられる。設問 III. 2(1)(ii) 参照。しかしながら、かかる検査結果が法人に提供された場合には、その内容が身体的若しくは生理学的情報又は医療記録及び病歴に該当する場合には、当該法人に SPDI が適用される。

(2) 趣旨

SPDI 規則からは、SPDI の各カテゴリに関する明確な立法目的は明らかではない。一定の情報を SPDI として総合的に分類した趣旨については、設問 I. 2 への回答を参照されたい。

(3) 追加的規律（該当する場合）

遺伝子に関するデータの取扱いに適用される特別な規律はない。ただし、2017 年人間参加生医学健康研究のための国家倫理ガイドライン（National Ethical Guidelines for Biomedical and Health Research involving Human Participants 2017）が、研究への参加者、生物資料及びデータを含む、インドで実施される健康のための生医学、社会及び行動科学研究に対し適用される。同ガイドラインは、生物資料の検査とそれにより生成されたデータを規律する。とりわけ、一般的な遺伝子診断検査について、機関毎のポリシーにより同意が必要か否かを定めるべき旨を規定している一方で、研究については、インフォームドコンセントを必要としている。

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的趣向に関するデータは、センシティブデータに該当する。性的指向に関する個人情報は、SPDI に該当するためである。

(2) 趣旨

SPDI 規則からは、SPDI の各カテゴリに関する明確な立法目的は明らかではない。一定の情報を SPDI として総合的に分類した趣旨については、I. 2 への回答を参照されたい。

(3) 追加的規律（該当する場合）

他に適用される規律はない。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当しない。労働組合への加入に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

労働組合への加入に関するデータをセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

該当なし。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、センシティブデータに該当する。例えば、指紋、目の網膜や虹彩、声のパターン、顔のパターン、手の計測値、DNA といったデータが、SPDI とみなされる生体データに含まれると解される。

(2) 趣旨

SPDI 規則からは、SPDI の各カテゴリに関する明確な立法目的は明らかではない。一定の情報を SPDI として総合的に分類した趣旨については、I. 2 への回答を参照されたい。

(3) 追加的規律（該当する場合）

2019 年 Aadhaar 法その他の改正法案により改正された、（財政等の補助、利益及びサービスの提供を対象とする）2016 年 Aadhaar 法（以下「Aadhaar 法」という。）[97]は、個人の同一性を認証するための生体データの処理について、一定の要件及び制限を規定する。具体的には、同法に基づき生体データを登録することで得られる Adhaar 番号という個人識別番号の処理に関し、個人に関する情報の安全管理措置を政府機関に義務付け、関連する一定の生体データの第三者への提供を制限するほか、同法に基づき収集された生体データが IT 法の SPDI に該当し、IT 法の SPDI に関する規律が適用されることなどを明記している。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータのうち、銀行口座、クレジットカード、デビットカードその他支払手段の詳細などの一定の金融に関するデータは、センシティブデータに該当すると考えられる。銀行口座、クレジットカード、デビットカードその他支払手段等の金融情報に関する個人情報は、SPDI に該当するためである。その他支払い手段の詳細として具体的にどういったものがあるかについては明らかにされていないが、UPI（インドにおける銀行口座間決済のためのシステム）や仮装通貨の支払い情報などが含まれる可能性がある。

(2) 趣旨

SPDI 規則からは、SPDI の各カテゴリに関する明確な立法目的は明らかではない。一定の情報を SPDI として総合的に分類した趣旨については、I. 2 への回答を参照されたい。

[97] https://uidai.gov.in/images/Aadhaar_Act_2016_as_amended.pdf

(3) 追加的規律（該当する場合）

インドには、銀行及び金融情報に関するデータを規律する特有の法律がいくつか存在する。例えば、Master Direction - Know Your Customer (KYC) Direction, 2016（2021 年 5 月 10 日更新）[98]に基づき、銀行は、銀行と顧客の間の契約関係から生じた顧客情報に関して秘密を保持することが求められる。口座開設のために顧客から収集された情報は、秘密情報として取り扱う必要がある。

さらに、Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions 2022[99]が、すべての指定銀行及び非銀行金融会社に適用される。これによると、カード発行会社又は非銀行金融会社は、情報を使用する目的と情報が共有される組織に関して具体的な同意を得ることなく、口座開設又はカード発行時に取得した顧客に関する情報を、他人又は他の組織に開示してはならないこととされている。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータは、センシティブデータに該当しない。信用に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

信用に関するデータをセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

信用に関するデータは SPDI には該当しないが、2005 年信用情報機関法[100]及びその規則（CIC 法）は、信用情報機関を規制しており、信用情報の正確性や安全性、プライバシーに関する原則を定めるほか、信用情報の共有のための要件を規定する。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。政府等の金銭的保護を受けている事実に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

[98] https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=11566
[99] https://rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12300
[100] https://legislative.gov.in/sites/default/files/A2005-30.pdf

政府等の金銭的保護を受けている事実に関する情報をセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

該当なし。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、センシティブデータに該当しない。成年後見制度の保護を受けている事実に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

成年後見制度の保護を受けている事実に関する情報をセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

該当なし。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報は、センシティブデータに該当しない。児童に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

児童に関する情報をセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

該当なし。

11. オンライン行動履歴に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報は、センシティブデータに該当しない。オンライン行動履歴に関する個人情報は、SPDI に該当しないためである。

(2) 趣旨

オンライン行動履歴に関する情報をセンシティブデータとしないことについての立法趣旨は、本調査の限りでは特に見当たらなかった。

(3) 追加的規律（該当する場合）

該当なし。

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

SPDI の収集に先立ち、文書又は電子通信手段を通じて、利用の目的についての書面による同意が SPDI の提供者（本人）から取得される必要がある（SPDI 規則第 5 条第 1 項）。さらに、SPDI を収集する者は、SPDI の提供者（本人）が SPDI の収集、収集の目的、意図された受領者並びに当該 SPDI の収集及び保持を行う機関の名称及び住所を通知するため、その状況に応じた合理的な措置をとらなければならない（SPDI 規則第 5 条第 3 項）。

SPDI を収集する者は、その機能又は活動と関連する合法的な目的であって、SPDI の収集が目的の達成のために必要とみなされない限り、SPDI を収集してはならない（SPDI 規則第 5 条第 2 項）。

### 2. 利用

当初収集された理由と異なる理由のために SPDI を利用することは許されない（SPDI 規則第 5 条第 5 項）。

### 3. 第三者提供

SPDI 規則に基づき移転元が実施するデータ保護と同程度のデータ保護を保証する者（インド国内又は国外の法人かを問わない。）に対しては、次のいずれかの場合であれば、SPDI を移転しうる（SPDI 規則第 7 条）。

- 移転元と情報提供者（本人）の間の合法的な契約を履行するために必要である場合
- 情報提供者（本人）がデータ移転に同意した場合

4. 管理

SPDI に関して、IT 法第 43-A 条は、「合理的なセキュリティ慣行及び手順」（reasonable security practices and procedures）の遵守を法人等に義務付けている。法人等は、合理的なセキュリティ慣行及び手順を実施し、保護しようとしている情報資産に応じた管理的、技術的、組織的及び物理的なセキュリティコントロール措置を含む、包括的かつ実証的な情報セキュリティプログラム及びポリシーを有している場合、合理的なセキュリティ慣行及び手順を実施したとみなされる。
情報セキュリティマネジメントシステム要件に関する国際規格 IS/ISO/IEC 27001 は、SPDI 規則が指定した、SPDI を取り扱うにあたって実施し得る標準（以下「指定標準」という。）の一つである（SPDI 規則第 8 条第 2 項）。データ保護のための指定標準以外の内容の自主基準を採用する場合には、その自主基準についてについてインド政府による承認及び通知を受ける必要がある（SPDI 規則第 8 条第 3 項）。法人等が実施する指定標準又は自主基準は、中央政府が承認した独立監査機関により認証されるか、監査される必要があり、監査は、少なくとも一年に一回又は社内手順及びコンピュータリソースに重要なアップグレードがあったときに、監査機関により実施される必要がある（SPDI 規則第 8 条第 4 項）。

5. 漏えい等

SPDI 保護のための合理的なセキュリティ慣行及び手順の実施及び維持を怠り、第三者に不当な損害又は不当な利得を与えた法人は、影響を受けた第三者に対し、補償として損害賠償をする必要がある（IT 法第 43-A 条）。補償の額に上限はなく、個別の事案ごとに裁定機関により決定される。

センシティブデータについての漏えい等が発生した場合の当局又は本人への報告義務は特に規定されていないが、サイバーセキュリティとインシデント報告の側面を扱うために IT 法に基づいて任命された統括機関であるインドコンピュータ緊急対応チーム（"CERT-In"）の規則に定められたサイバーセキュリティ事案に該当する漏えいとなる場合には、同規則に従い、法人等の対象事業者は、そのようなインシデントを知ってから 6 時間以内に当局に報告することが必要となる。

6. 請求権

SPDI を収集し、加工し、又は取り扱う法人は、当該 SPDI の提供者（本人）に対して、SPDI を確認又は修正する権利を与え、かつ、不正確又は不十分と判明した場合に、当該データが可能な限り訂正又は修正されるようにしなければならない。法人はまた、情報提供者（本人）に対し、提供した情報に関し、書面により、いつでも同意を撤回できる選択権を与えなければならない。

V. 本人同意、プロファイリング

1. 本人同意

(1) センシティブデータ規制（上記III）との関係

SPDI 規則上、法人等は、SPDI の収集に先立ち、文書又は電子通信手段を通じて、利用の目的に関する書面による同意を SPDI の提供者（本人）から取得する必要があるとされている（SPDI 規則第 5 条第 1 項）。

(2) 要件一般

SPDI 規則上、同意そのものに関する要件としての一般的な定めは特段存在しない。なお、下記(4)及び(7)でも述べる通り、黙示的な手法を通じて取得された同意は、適切な同意とはいえない（SPDI 規則第 5 条第 1 項）。

(3) 情報提供

SPDI を収集する法人等は、情報提供者（本人）が SPDI の収集、収集の目的、想定される提供先並びに当該 SPDI の収集及び保持を行う機関の名称及び住所を把握できるようにするためにその状況で合理的な措置をとらなければならない（SPDI 規則第 5 条第 3 項）。

(4) 形式

SPDI 規則に基づく同意は、文書、FAX その他電子的通信手段（E メール等）を通じて、SPDI の提供者から書面により取得しなければならない。SPDI 規則において、黙示的同意又は推定された同意は、有効ではない（SPDI 規則第 5 条第 1 項）。

(5) 個別同意の必要性

SPDI 規則は、利用目的に関して同意を取得することを法人等に求めているが（SPDI 規則第 5 条第 1 項）、各利用目的が明確に言及されている限り、同意をまとめて取得することを特に制限していないため、そのようなまとめての同意の取得も可能と解されている。利用目的に変更がある場合には、新たに同意を取得しなければならないと解される（SPDI 規則第 5 条第 1 項）。

(6) 同意撤回

データ主体は、同意を撤回することができ、撤回の際、データ主体はその旨を書面で伝える必要がある（SPDI 規則第 5 条第 7 項）。同意が撤回される場合、法人等は、関係する SPDI が要求される商品又はサービスを提供しない選択権を有する（SPDI 規則第 5 条第 7 項）。

(7) その他留意事項

インド政府が発表したプレスノート[101]は、SPDI 規則第 5 条第 1 項の同意は電磁的方法による取得も認められるとしていることから、クリックラップ又はクリックスルーを通じて事前の書面による同意を得ることも可能であると解される。但し、予めチェックされたチェックボックスのような、黙示的な手法を通じて取得された同意は、適切な同意とはいえない（SPDI 規則第 5 条第 1 項）。

2. プロファイリング

(1) プロファイリング・データ分析に対する規律

[101] https://www.meity.gov.in/writereaddata/files/PressNote_25811.pdf

プロファイリング・データ分析に対する規律は特に見当たらない。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリング・データ分析により SPDI が生成される場合、当該生成された SPDI には IT 法及び SPDI 規則が適用される。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

SPDI において、プロファイリングにより SPDI を生成することと SPDI を取得することは区別されていない。したがって、いずれの場合でも同様の SPDI 規則の要件が適用される。プロファイリングによって SPDI が生成される場合であっても、V. 1.本人同意の項目で言及のある通知や同意の要件に従わなければならない。

## VI. センシティブデータの取扱いに係る裁判例・決定等

SPDI に関する請求に関し判決が下された事案のうち、本調査の趣旨を踏まえ現地カウンセルにより選定された事例と判決について、以下概略を示す。もっとも、そうした判決並びに判決に関する主張及び議論のすべてが一般的に公開されているわけではなく、概略にとどまる点には留意されたい。

- *IDBI Bank v. Sudhir S. Dhupia*[102]では、上訴人である銀行（IDBI）が、保持する顧客の銀行口座に関して合理的なセキュリティ慣行及び手順の維持を怠ったために、IT 法第 43-A 条に違反していると判断された。銀行は、頑強な認証プロトコルを備えたセキュアなインターネットバンキングシステムを提供することができておらず、詐欺的な取引の発生につながった。この判決では、コンピュータリソースを有し SPDI を取り扱う会社は、合理的なセキュリティ慣行及び手順を維持する特定の義務が課されていることが示された。
- *Amit Patwardhan v. Rud India Chains Private Limited*[103]では、使用者が元従業員に対して、会社の営業秘密を漏洩したとして訴えを提起した。元従業員は、バロダ銀行に給与用口座を持ち、元従業員の銀行取引明細書が使用者の訴状に添付されていた。使用者である会社は、いかに銀行取引明細書にアクセスしたのか説明することができず、銀行支店長も、会社によるアクセスへの自身の関与を否定した。裁判官は、とりわけ、元従業員の銀行取引明細書は SPDI に該当すると判示した。本件銀行取引明細書は、使用者により疑わしい手段でアクセスされ、使用者は元従業員の銀行情報にアクセスする権利を有しないとされた。バロダ銀行も当事者となった、元従業員が提起した後続の訴え[104]では、「データ侵害が発生したことは明らかであり」「銀行はこれがどのように起きたかを自ら調査することが全くなかった。」「これは、顧客のセンシティブデータのプライバシーに関する銀行の無関心を示すものとして余りある。」旨判示された。バロダ銀行は、IT 法第 43-A 条の規定に違反したとして、元従業員に INR5,000 を補償することが命じられた。

[102] 2019 SCC OnLine TDSAT 226.
[103] Complaint No. 1 of 2013.
[104] Complaint No. 15 of 2013 dated 28 June 2013.

VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

該当なし。念のため付言すると、2022 年 11 月 18 日、インド電子情報技術省は、パブリックコンサルテーションのためにデジタルパーソナルデータ保護法案（Digital Personal Data Protection Bill 2022）[105]（以下「2022 年法案」という。）の草案を公開した。現地専門家による本調査への回答時点では、2022 年法案のパブリックコメント期間は、2023 年 1 月 2 日に終了するとされており、国会には提出されていないが、現状、7 月に開始が予定される会期中に提出されると言われている。将来的に 2022 年法案が成立し、施行された場合には、この限度において個人情報に関する既存の法制度が変更され、同法令に基づく規律が適用されることになる。現状の法案では通常の個人情報とセンシティブデータを区別していないため、法案に修正がなければ、センシティブデータについての追加的な義務は規定されないことになる。

[105] https://www.meity.gov.in/writereaddata/files/The Digital Personal Data Potection Bill%2C 2022_0.pdf

# 第7章.　ブラジル

## I.　総論

### 1.　個人情報の保護に関する法令等

個人情報の保護に関する包括的な法令として、Lei Geral de Proteção de Dados（法律#13,709/18—一般データ保護法（以下「LGPD」という）[106]が存在する。これらの法令は公的部門、民間部門のいずれも対象としている。

LGPD は 2020 年 9 月施行のブラジルにおける最初の包括的データ保護法である。LGPD 第 3 条によると、同法は域外適用があり、また、産業、処理方法、本店所在国又はデータ所在国にかかわらず、自然人又は法人により行われる処理行為に適用される。ただし、次のいずれかの場合に限られる。

- 個人データ処理がブラジルで行われる場合
- 個人データ処理が、ブラジルにおける商品及びサービスの提供若しくはブラジルに所在するデータ主体からの個人データの処理のために行われる場合
- 処理される個人データがブラジルで収集された場合。なお、データ収集時点においてデータ主体がブラジルにいた場合、個人データはブラジルで収集されたものとみなされる。

### 2.　センシティブデータの取扱いに対する規制の趣旨

センシティブデータの取扱いに対する規制の趣旨については、必ずしも明らかではない。個人データ全般の取扱いについては、LGPD の前身となる法案 4060/2012 は、前文において、同法案が、ブラジル連邦共和国憲法に従い、個人データの処理及び個人権の保護に法的及び制度的秩序を提供することを目的としているとしている。さらに、同法案は、新たな技術的現実の中で、自由な取引及び通信を妨げることなく、特に個人の人格及びプライバシーに保護を与えることで関係を規律する法規範を確立することが必要であると説明している。

LGPD によると、その主たる目的は、自由及びプライバシーの基本的権利並びに自然人の人格の自由な発展を保護することである（第 1 条）。

また、後掲の「ガイドライン: 小規模処理事業者のための情報セキュリティ」において、センシティブデータがかかわるセキュリティインシデントは、データ主体に損害を与えたり、データ主体を差別的な状況にさらすおそれがより高い旨が触れられており、このこともセンシティブデータの取り扱いを規制する趣旨を構成すると解される。

## II.　センシティブデータの範囲—総論

LGPD が、以下で詳述するように、「個人データ」及び「センシティブ個人データ」を定義し、それに関するルールを定めている。

LGPD は、「個人データ」（personal data）と「センシティブ個人データ」（sensitive personal data）を区別して、それぞれ以下の通り定義している。

- 「個人データ」（第 5 条第 I 号）：識別された、又は識別され得る自然人に関するデータ
- 「センシティブ個人データ」（第 5 条第 II 号）：人種若しくは民族的起源、宗教的信念、政治的

[106] http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

意見、労働組合員であること又は宗教的、哲学的若しくは政治的組織の一員であることに関する個人データ、健康又は性生活に関するデータ及び自然人に関連付けられた遺伝子データ又は生体データ

センシティブ個人データの定義に関し、LGPD に基づきセンシティブとみなされるデータのリストが、例示なのか、それとも網羅的なリストであるかという点が、学者及び実務家の間で現在議論されている[107]。

仮に例示的であるとする理解が通説となれば、どのような情報がセンシティブ個人データとなるかは、判例法、当局である Autoridade Nacional de Proteção de Dados（以下、「ANPD」という。）及び学者の議論等によって今後決定されることとなる。反対に網羅的であるとする立場に基づく場合、高リスクととらえられている個人データの処理について、センシティブ個人データとしての扱いが不要となり、保管方法並びにセキュリティ及び秘密保持手段の調整に影響を及ぼる可能性がある。

1. センシティブデータの範囲一覧

以下の表において、センシティブ個人データとして LGPD 上定義されているデータ項目、あるいは本調査において対象となっている推知情報等の具体的なデータ項目のうちの一部について、資料における説明を該当する資料の名称・URL と共に記載している。

（資料の名称・URL）

1. *Guia Orientativo: Tratamento de dados pelo poder público*（ガイドライン：行政機関による個人データの処理）[108]：ANPD により公開されたこのガイドラインでは、以下のデータ項目に関して、次のような事例が説明されている。

| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
|---|---|
| 健康データ | （ANPD がガイドラインで提供する具体例）タバコ管理政策において取り扱う個人データ<br>公衆衛生部門が、タバコ管理並びに肺がん防止及び治療に関する公共政策を計画し実行するために、公立病院で治療を受けた喫煙者の個人データを処理しており、この政策においては、個人データは公衆衛生部門それ自体が処理し、喫煙をやめようとしている人のためのガイダンス及び補助プログラムを担当する当局と共有されるとする。この場合、当該データにはセンシティブ個人データを含むため、処理は LGPD 第 11 条第 II 号 b（法令に定められた公共政策を行政機関が実施するのに必要なデータの共同処理）に基づき行われる必要がある。処理の目的は、LGPD に従い、法令により規定された公共政策の実施に限られる。<br><br>（ANPD がガイドラインで提供する例）ワクチン接種に関する公共政策において取り扱う個人データ<br>ワクチン接種に関する公共政策を設計し、実施し、かつモニタリングするために、自治体の公衆衛生部門が、感染症の感染確認事例に関するデータを収集する。データは、公共政策に関する研究を実施するという特定の目的のために、研究機関と共有される。この場合、その研究機関に |

[107] なお、調査基準日以後の 2023 年 3 月 7 日にブラジルの最上級審である Superior Court of Justice の判決（case AREsp 2.130.619）において、Francisco Falcão 裁判官が、LGPD におけるセンシティブ個人データに列挙されている種類のデータは限定列挙であると言及した。ただ、簡潔な言及に過ぎなかったこともあり、この判決の後も研究者や実務家の間でも議論は続いている。

[108] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_tratamento_de_dados_pessoais_pelo_poder_publico__defeso_eleitoral.pdf

| | |
|---|---|
| | よる当該データの処理は、目的原則のもと、収集の本来の目的と適合するものと考えられるが、健康に関するセンシティブ個人データにかかわるため、研究機関は、常に LGPD 第 13 条及び第 4 章を遵守し、データの共有及び開示の際には慎重にならなければならない。この意味で、可能な限り、この情報の共有にはデータの仮名化又は匿名化が含まれることが望ましいとされている。 |

（資料の名称・URL）
2. *Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados (LGPD) por agentes de tratamento no contexto eleitoral*（ガイドライン：電子的文脈における処理行為者による一般データ保護法（LGPD）の適用）[109]：ANPD により公開されたこのガイドラインでは、以下のデータ項目に関して、次のような事例が説明されている。

| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
|---|---|
| 推知されたデータ | センシティブ個人データは、推知処理又は相互参照されるデータベースによっても明らかになり得る。したがって、データ主体の個性に関するセンシティブな側面が開示され、又は間接的に識別され、権利利益が侵害又は制限される可能性があり、人種若しくは民族的起源、宗教的信念、政治的意見、労働組合員であること又は宗教的、哲学的若しくは政治的組織の一員であることに関する情報、健康又は性生活に関するデータ及び遺伝子データ又は生体データを開示する場合、センシティブ個人データについての LGPD の規定が適用される。<br>これは、名前、住所及び消費プロフィール（例：購入又はブラウジング履歴）のような、他のセンシティブではない情報に基づき、宗教的信念、人種的出身又は政治的意見を識別する場合にあてはまる。同様に、選挙活動に従事する寄付者及びボランティアのデータベースについても、データ主体の登録情報及び連絡先が含まれているにすぎない場合であっても、情報収集を担当した党又は候補者と結びつけることによって、政治的意見を明らかにし、センシティブ個人データとみなされる可能性がある。 |
| 政治的意見に関するデータ | （ANPD がガイドラインで提供する例）政党が提供するアプリケーションにより収集される個人データ<br>政党は、協力者及び有権者一般に無料アプリケーションを提供し、そのアプリケーションが、利用者の同意を得て、基本的な身元確認データ、顔認証情報及び地理的位置情報等を収集する。この場合、収集されたデータは、識別され、又は識別され得る自然人に関する情報を表しており、したがって、個人データ処理の全体は LGPD の規定に従って実施されなければならず、ANPD 及び選挙裁判所の調査の対象となる。さらに、収集された顔認証情報は、データベースに組み込まれて利用者を識別するのに使用されるものであり、センシティブ個人データに該当するものであることから、処理は LGPD 第 11 条に定められた法的根拠を遵守してより慎重に行われなければならないこととなる。利用される文脈にもよるものの、アプリケーションにより収集されたすべての情報は、センシティブ個人データを推知する目的で処理される場合、センシティブ個人データとみなされる可能性がある。 |

（資料の名称・URL）

[109] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf

| 3. *Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte*（ガイドライン: 小規模処理事業者のための情報セキュリティ）[110]：このガイドラインも ANPD の公表によるものである。 | |
|---|---|
| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
| センシティブ個人データ一般 | センシティブ個人データに関わるセキュリティ事故は、データ主体に関連する損害または損害のリスクを生じさせる可能性が高いため、センシティブ個人データには、より具体的な処理の法的根拠（LGPD 第 11 条に規定）の要件など、LGPD においてより厳しい要件がある。<br><br>さらに、センシティブ個人データは LGPD の下で特別な保護が与えられていることを踏まえ、センシティブ個人データを保存する小規模な処理業者に対し、データ主体の特定を困難にする、仮名化技術（暗号化など）の対策のを導入を提案する。<br><br>また、例えば会社のウェブサイトなど、公共のネットワーク上で不必要に公開されているセンシティブ個人データやその他の個人データを削除することが重要である。会社の業務にセンシティブ個人データの処理が含まれる場合（例えば医療サービスの場合）、顧客の情報アクセスについて、制御されたアクセスチャネルを設けることを推奨する。 |

| （資料の名称・URL）<br>4. *Estudo Preliminar - Hipóteses Legais aplicáveis ao tratamento de dados pessoais de crianças e adolescentes*（予備的調査――児童及び青年の個人データ処理に適用される法的前提）[111]：ANPD により公開されたこのガイドラインでは、児童及び青年のデータ[112]項目に関して、次のような説明がなされている。 | |
|---|---|
| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
| 児童及び青年のデータ | LGPD は、児童及び青年の個人データの処理について特定の章を置いている。LGPD の主要部である第 14 条は、国内及び国際的な法的枠組みに見られるように、これらのデータ主体のデータの処理は、関連立法の規定に基づき、児童及び青年の最善の利益のために実施されなければならないとしている。そして、第 14 条第 1 項は、「児童の個人データの処理は、親又は法定代理人の少なくとも 1 人の具体的かつ顕著な同意に基づき実施されなければならない。」と規定する。同条第 3 項は、児童の情報の収集は、親又は法定代理人に連絡する必要がある場合、又は児童の保護のため必要がある場合に、第 1 項に基づく同意なくして実施することができると規定する。これらの条項の解釈は、学説、実務及び世論においても議論があり、LGPD 上の事由のうちいずれにより児童及び青年の個人データの処理が認められるかという点は明確にされていないため、個人データを処理する者にとって法的に不安定な状況であると考えられている。<br><br>例えば、近時に ANPD に宛てられた質問の中には、この点について行政機関により異なる立場が示された例が見受けられる。児童の個人データを処理するには同意が唯一の適切な法的前提であるとする主張がある一方で、研究機関による研究の実施等、LGPD 第 7 条及び第 11 条に規定された他の法的前提により、行政機関どうし又は行政機関と公立大学の間で個人データを共有することができるという主張も存在する。さらに |

[110] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf
[111] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf
[112] 後述の通り、児童に関するデータについては、LGPD 上のセンシティブデータの定義には該当しないものの、LGPD 上特定の章が設けられたうえで特別の規律に服することから、本項目においても取り上げている。

| | |
|---|---|
| | は、児童及び青年からのデータは、センシティブデータとして扱われるよう解釈すべきであるから、その処理は LGPD 第 11 条に規定された法的前提を根拠としてのみ行われ得るとする見解もある。 |

2. センシティブデータを推知させる情報（推知情報）について

LGPD 第 12 条第 2 項によると、特定の個人の行動プロフィールを形成するために利用されるデータは、個人が識別される場合には、個人データとみなされ得るが、センシティブ個人データを推知させることについて特別の条項は規定されていない。

しかしながら、ANPD による提言についていえば、II.1 で言及したガイドライン（電子的文脈における処理行為者による一般データ保護法（LGPD）の適用）の項目で記述したとおり、データが利用される文脈によっては、個人データが他のセンシティブデータを推知するために処理される場合、その個人データはセンシティブ個人データとみなされる可能性がある。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。

(i) 医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当すると考えられる。

LGPD における健康に関するデータの定義は広く、ANPD はこの点に関する具体的な規則を公表していないものの、個人を識別し、又は識別し得る健康に関連するデータはセンシティブ個人データとなる健康に関するデータに該当すると考えられる。医師等により実施された検査結果は、他のデータと組み合わせることで個人の識別が可能となるのであれば、センシティブ個人データとみなされ得る。

(ii) 事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当すると考えられる。上記 III.1.(1) (i)と同様に、他のデータと組み合わせることで個人の識別が可能となる健康に関するデータと考えられるためである。

(iii) 消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当すると考えられる。上記 III.1.(1) (i)と同様に、他のデータと組み合わせることで個人の識別が可能となる健康に関するデータと考えられるためである。

(iv) 消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する。

上記 III.1.(1) (i)と同様に、他のデータと組み合わせることで個人の識別が可能となる健康に関するデータと考えられるためである。

(v)　予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無は、センシティブデータに該当する。

上記 III.1.(1) (i)と同様に、他のデータと組み合わせることで個人の識別が可能となる健康に関するデータと考えられるためである。

(2)　趣旨

法案#4060/2012（LGPD の前身である法案）の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPD が自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する目的を有する点を踏まえると、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮し、健康情報が差別的な行動を招き、その他の方法で害を与える可能性があるものとして、当該情報の誤った使用が個人に対して高いリスクを有すると認識していたと考えられる。

(3)　追加的規律（該当する場合）

健康保険との関係で、LGPD 第 11 条第 5 項は、民間医療保険のサービス提供者が、保険の加入並びに受取人（Beneficiaries）の承認及び除外の判断において、保険の危険選択を目的として健康データを処理することを禁じている。

国民健康庁（ANS）は、リスクの計算が保険契約に内在するものであって、被保険者が支払う対価の額に影響する要素となり得ることから、規準#27/2015 において、民間医療保険のサービス提供者によるリスク軽減のための法的仕組みの存在を認識しつつも、リスクが高いと考えられる保険契約者を除外することや、そうした人との契約の締結を避けることにつながり得るような危険選択を禁じている。

2.　遺伝子に関するデータ

(1)　センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、センシティブデータに該当する。

何が「遺伝子データ」に該当し得るかを規定した LGPD の条項又は ANPD の規則は存在しない。

(i)　医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。

LGPD における遺伝子に関するデータの定義は広く、ANPD はこの点に関する具体的な規則を公表していないものの、個人を識別し、又は識別し得る、医師等が実施した遺伝子検査に関するデータはセンシティブ個人データとなる遺伝子データに該当すると考えられる。医師等により実施された遺伝子検査の結果は、他のデータと組み合わせることで個人の識別が可能となるのであれば、センシティブ個人データとみなされ得る。

(ii) 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当すると考えられる。上記 III.2.(1) (i)と同様にして、他のデータと組み合わせることで個人の識別が可能となる遺伝子に関するデータと考えられるためである。

(iii) 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当すると考えられる。上記 III.2.(1) (i)と同様にして、他のデータと組み合わせることで個人の識別が可能となる遺伝子に関するデータと考えられるためである。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPD が自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する目的を有する点を踏まえると、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮し、遺伝子に関する情報が差別的な行動を招き、その他の方法で害を与える可能性があるものとして、当該データの誤った使用が個人に対して高いリスクを有すると認識していたと考えられる。

(3) 追加的規律（該当する場合）

該当なし。

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPD が自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する目的を有する点を踏まえると、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮し、性生活・性的指向に関する情報が差別的な行動を招き、その他の方法で害を与える可能性があるものとして、性生活（に関するデータ）の誤った使用が個人に対して高いリスクを有すると認識していたと考えられる。なお、「性的指向」（sexual orientation）という用語は LGPD の法文において明確に規定されていないものの、「性生活」（sex life）（ただし性生活という語も LGPD に定義はされていない）にこれが含まれることが示唆されるとする解釈が学説及び実務上みられる。

(3) 追加的規律（該当する場合）

該当なし。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する。

(2) 趣旨

法案#4060/201 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

もっとも、LGPD が自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する目的を有する点を踏まえると、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮し、労働組合への加入に関する情報が差別的な行動を招き、その他の方法で害を与える可能性があるものとして、当該データの誤った使用が個人に対して高いリスクを有すると認識していたと考えられる。

(3) 追加的規律（該当する場合）

該当なし。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、センシティブデータに該当する。

生体データは、LGPD に基づくセンシティブ個人データの定義に含まれている。なお、LGPD 上は「自然人を一意に識別することを目的とする」という点については特に言及していない。この事項に関する ANPD による公式のガイダンスは存在しないものの、識別され、又は識別される可能性のある個人に関する限りで、生体データはセンシティブ個人データに該当するから、少なくとも個人を一意に識別する目的で処理が実施される場合はセンシティブ個人データにあたると考えられる。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。もっとも、LGPD が自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する目的を有する点を踏まえると、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮し、生体データは差別的な行動を招き、その他の方法で害を与える可能性があるため、生体データの誤った使用が個人に対して高いリスクを有すると認識していたと考えられる。

(3) 追加的規律（該当する場合）

該当なし。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータは、センシティブデータに該当しないと解される。仮に LGPD がセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、金融・財産に関するデータは典型的にはそのような議論の対象になっていないように見受けられる。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPD における自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護するという立法目的を踏まえると、立法者としては、LGPD 上のセンシティブ個人データに与えられる高レベルの保護を考慮し、金融データについては個人データに与えられる保護で十分であると認識していたと考えられる。

(3) 追加的規律（該当する場合）

(i) 銀行秘密法

2001 年 1 月補足法#105（以下「銀行秘密法」という。）第 1 条に基づき、金融機関その他ブラジル中央銀行に営業が許可された法人（販売会社等）は、能動的か受動的かを問わず、提供した業務及びサービスの機密性を保持しなければならない。これは、金融機関その他ブラジル中央銀行に営業が許可された法人（販売会社等）は、現金、長期預金、貯蓄口座、通貨支払又は小切手支払、投資、掛け買い注文、信用業務、資金移転、口座残高その他中央銀行が許可する同種の取引に関する情報の秘密性を保持しなければならないことを意味している。

(ii) クラウドサービスの提供に関する中央銀行規則

銀行及び金融サービス提供者によるクラウドサービスの利用には、当該サービスが基幹事業に関連するとみなされる限り、中央銀行決議#4,893/2021 及び通達#85/2021 などのルールが適用される。これらの規則は、サイバーセキュリティポリシーを確立及び維持する義務並びにデータ処理、データストレージ及びクラウドコンピューティングの重要なサービスについて契約を締結するための要件を定めている。

これらの規則は、金融機関がクラウドサービスについて契約を締結するに際しての義務及び中央銀行が遵守すべき運用上の手順を定めている。また、同規則は各契約に含まれる必要のある条項も定めている。

これにより、ブラジルの金融機関は、コーポレートガバナンス及びマネジメントプラクティスを文書化して採用するとともに、(i)金融機関への処理されたデータへのアクセスの提供、(ii)データの機密性、完全性、利用可能性及び回復性の保証、(iii)論理的又は物理的管理を通じた、金融機関の顧客に関するデータの識別及び分離の各事項について、クラウドサービス提供者の能力を検証する義務を負う。

ブラジルの金融機関は、ソリューションを保持してから 10 日以内に、中央銀行にクラウド契約を通知し、クラウド提供者及び関連サービスに関する情報を提供しなければならない。クラウド契約の変更も、10 日以内に中央銀行に報告しなければならない。こうした通知には、(i)外部委託会社の名称、(ii)契約した関連サービスの仕様及び(iii)サービスの提供、データの保存、処理及び管理される国及び地域が含まれなければならない。しかし、サービスが提供される国について、中央銀行と各銀行管理当局との間に協力合意がない場合、ブラジルの金融機関は、契約締結前 60 日までに、中央銀行から事前の書面による許可を得る必要がある。サービスが提供される国に関する契約の変更についても、変更の 60 日前までに中央銀行に報告しなければならない。したがって、規制上の通知は、契約ごとに行われることになる。

また、当該契約では、サービスの提供、及びデータが処理される国や地域が指定されなければならない。ブラジルの金融機関は、サービスが提供される国又は地域の法規制枠組みが、当該法人及び中央銀行によるデータ及び情報へのアクセスを制約又は阻害しないようにしなければならない。当該契約には、顧客のデータ保護のためのセキュリティ措置、データ分離措置、アクセスコントロール等の要件を規定しなければならない。また、ブラジル中央銀行による契約、保存データ、データのバックアップ及び関連するアクセスキーへのアクセスが認められることが明確に規定されなければならない。

クラウドサービス提供者との契約に含まれるべき具体的な契約文言を義務付けられていないものの、規則に基づく原則が契約に盛り込むべきとされている。これらの規則の根本的な理由は、ブラジルにおける金融サービスのセキュリティ、継続性及び完全性を保護し、中央銀行がこれらの活動を検査できるようにすることであり、そのため、中央銀行は、関連するサービス提供者に対し、関連サービス提供者が処理又は保存するデータ及び情報の機密性、完全性、利用可能性及び回復性を保証するためのセキュリティ措置を採用し、かつ、中央銀行にデータへのアクセスを与えることを求めている。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータは、センシティブデータに該当しない。仮に LGPD がセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、信用に関するデータは典型的にはそのような議論の対象になっていないように見受けられる。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。LGPD における自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護するという立法目的を踏まえると、立法者としては、LGPD 上のセンシティブ個人データに与えられる高レベルの保護を考慮し、信用データについては LGPD に基づき個人データに与えられる保護で十分であると認識していたと考えられる。

(3) 追加的規律（該当する場合）

優良支払人登録法（Good Payer's Registry Law）（補足法 166/19）は、履行情報を備えたデータベースに消費者を自動で登録することを規定し、肯定的な信用記録に対する金融機関のアクセスを認めている。

肯定的な信用記録は、消費者の「履歴」として機能する。すなわち、データベースにより利用可能となった金融に関する履歴を通じて、事業者は「優良支払人」（Good Payer）を区別することができ、そのような消費者に対しては低い金利で信用を供与するといったことが可能となる。

各消費者の信用履歴として許容される具体的な記載事項としては、関係の性質（信用、商業、継続的サービス等）、信用供与又は支払義務の引受けの日付、供与された信用又は引き受けた支払義務の額、過去に支払期日が到来した額、既に支払った額、支払日がある。

情報は明確、客観的、かつ容易に理解できるという要件を満たす必要がある。また、クレジットリスク分析に関係しないデータ及び社会、民族、健康、性的指向並びに政治的、宗教的及び哲学的信念に関する情報へのアノテーション（関連付け）は禁止されている。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。仮にLGPDがセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、政府等の金銭的保護を受けている事実に関する情報は典型的にはそのような議論の対象になっていないように見受けられる。

(2) 趣旨

法案#4060/2012の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPDにおける自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護するという立法目的を踏まえると、立法者としては、LGPD上のセンシティブ個人データに与えられる高レベルの保護を考慮し、政府等の金銭的保護を受けている事実に関するデータについてはLGPDに基づき個人データに与えられる保護で十分であると認識していたと考えられる。

(3) 追加的規律（該当する場合）

該当なし。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、センシティブデータに該当しない。仮にLGPDがセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、成年後見制度の保護を受けている事実に関する情報は典型的にはそのような議論の対象になっていないように見受けられる。

(2) 趣旨

LGPD における自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護するという立法目的を踏まえると、立法者としては、LGPD 上のセンシティブ個人データに与えられる高レベルの保護を考慮し、成年後見制度の保護を受けている事実に関するデータについては LGPD に基づき個人データに与えられる保護で十分であると認識していたと考えられる。

(3) 追加的規律（該当する場合）

該当なし。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報は、センシティブデータに該当しない。仮に LGPD がセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、児童に関する情報は典型的にはそのような議論の対象になっていないように見受けられる。

(2) 趣旨

法案#4060/2012 の前文は、センシティブ個人データの定義の具体的な立法目的を示していない。

LGPD は、自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護するという立法目的を有するところ、児童に関するデータをセンシティブなものとして明確に分類していないものの、他の形式により児童及び青年に関するデータに高い保護を与えている。したがって、立法者は、児童及び青年のデータは、児童及び青年はより被害を受けやすいことから、個人に対するより高いリスクをもたらすと認識しているものと考えられる。

これは青少年が、学習及び成長過程にあり、諸問題への成人と同様な対処が困難であるという発達途上の地位にあることから、法により保護されなければならないという立法事実からも正当化される。

(3) 追加的規律（該当する場合）

LGPD は、未成年者の個人データに関して特別な要件を設けている。ブラジル児童青年法（法律 #8,069/90—ECA）によると、児童とは 12 歳までの者をいい、青年とは 13 歳から 18 歳までの者をいい、これが LGPD の適用においても参酌されている。両者は、未成年者として扱われる。

LGPD は、児童の個人データの処理のために親権者の具体的な同意を必要とし（LGPD 第 14 条第 1 項）、さらに、データ管理者がその時利用できる技術を考慮し、同意が実際に親又は法的後見人によりなされたことを確認するために合理的に努めなければならないと義務付けられている（同条第 5 項）。

LGPD は、未成年者のデータの処理について、未成年者の最善の利益のために実施されなければならず（同条柱書）、データ管理者は、データ主体の権利の行使のために、収集されるデータの種類、当該データの利用に関する情報を公表することが求められている（同条第 2 項）。LGPD 上、データ管理者は、活動に厳密に必要なデータを超えて、個人データを提供することをゲーム又はインターネットアプリケーションに児童が参加するための条件とすることは許されない（同条第 4 項）。

また、LGPD では、児童及び青年のデータの処理について、データ管理者が利用者の性質、利用者の理解力や知的能力を考慮し、簡明、明確かつアクセス可能な方法で、処理行為に関する情報を提供することを義務付けている（同条第 6 項）。データ管理者は、親及び法的代理人に情報を提供するだけでなく、児童に児童が理解できる形で情報を提供するために、適切な場合に音声画像等のツールを使用することが推奨されている（同項）。

さらに、ANPD は、児童及び青年の個人データの処理に関する法的根拠について、初期調査結果を公表した[113]。同調査は、児童の個人データの処理の法的根拠に関する議論を奨励し、ANPD による将来の意思決定の資料となることが意図されている。

上記調査で、ANPD は、児童及び青年の個人データの処理に関して、LGPD の条項として次の 3 つの解釈の可能性を示している。

- 児童の個人データの処理については、LGPD 第 14 条第 1 項に従い、親又は法的後見人の同意のみを法的根拠としうること。
- センシティブ個人データと同等であることに照らして、児童及び青年の個人データの処理には、LGPD 第 11 条に定めるセンシティブ個人データ処理の法的根拠がある場合に限り処理が認められるとすること。
- 最善の利益の原則（principle of best interest）が遵守されることを条件として、児童及び青年のデータの処理には LGPD 第 7 条に定める個人データ処理の法的根拠及び LGPD 第 11 条に定めるセンシティブデータ処理の法的根拠がある場合に限り処理が認められるとすること。

この調査で示された分析は ANPD の最終的な見解を示すものではないが、少なくとも ANPD が予定している正式な規則の公表まで、ガイダンスとして参照されうる。

## 11. オンライン行動履歴に関する情報

### (1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報は、センシティブデータに該当しない。仮に LGPD がセンシティブ個人データの定義に記載している具体的な個人データの種類はセンシティブ個人データの例示であるという見解に立てば、該当すると解釈する余地があるが、かかる立場に基づいてセンシティブ個人データに該当するとの議論が見られたのは性別、性的志向、障害に関する情報、肖像や音声といった情報であり、少なくとも本調査の限りでは、オンライン行動履歴に関する情報は典型的にはそのような議論の対象になっていないように見受けられる。

### (2) 趣旨

LGPD は、自由及びプライバシーの基本的権利並びに自然人の自由な人格的発展を保護する立法目的を有するところ、立法者としては、センシティブ個人データに与えられる高レベルの保護を考慮すると、

[113] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/estudo-preliminar-tratamento-de-dados-crianca-e-adolescente.pdf

オンライン行動履歴に関するデータを保護するのにはLGPDに基づき個人データに与えられる保護で十分であると認識していたと考えられる。

(3) 追加的規律（該当する場合）

上述のとおり、LGPDは第5条第I号において個人データの開かれた概念を採用しており、識別された、又は識別され得る自然人に関する情報を含む。

したがって、名前、RG（ID）又はCPF（納税者番号）の登録番号及び住所のような基本的身元確認情報に加えて、消費習慣、見た目又は他の人格の側面等の、個人に関連する他のデータも個人データとみなされる。

II. 2の回答のとおり、LGPD第12条第2項によると、特定の個人の行動プロフィールを形成するために利用されるデータは、個人が識別される場合には、個人データとみなされ得る。さらに、「ガイドライン：電子的文脈における処理行為者による一般データ保護法（LGPD）の適用」上において、ANPDは、使用される文脈にもよるものの、他のセンシティブな情報を推知する目的でデータを処理した場合、一切のかかる個人データはセンシティブ個人データとみなされる可能性がある（例：ブラウジング履歴）としている。

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

LGPDは、「処理」（processing）を、収集、受信、分類、利用、アクセス、複製、送信、配布、加工、保管、保存及び移転等を含む、個人データにかかわる一切の行動と定義している（LGPD第5条第X号）。

LGPD上、センシティブ個人データの処理には、処理のためのより具体的な法的根拠など、通常の個人データに比して厳格な要件が課されている。これは特に、センシティブ個人データがかかわるセキュリティインシデントは、データ主体に損害を与えたり、データ主体を差別的な状況にさらすおそれがより高いからである（ガイドライン: 小規模処理事業者のための情報セキュリティ）。

LGPDに基づき、各処理行為は、法に定められた法的根拠に従って行われなければならない。ブラジルの個人情報保護に関する法律はGDPR（EU）に影響を受けており、LGPDに基づく処理行為に関する法的根拠はGDPRのそれと類似しているが、同一ではない。また、GDPRと異なる点として、LGPDは、センシティブでない個人データの処理とセンシティブデータの処理について、法的根拠を分けて規定している点が挙げられる。。

LGPDに基づきセンシティブではないデータを処理するための法的根拠は、次の通りである（LGPD第7条）。

(i) データ主体による、自由で、情報を与えられた、明確な同意

(ii) データ管理者による法令上の義務の遵守

(iii) 行政機関について、法令、契約その他類似の文書に定められた公共政策を実施するための必要なデータの処理及び共有

(iv) 研究機関について、可能な限りデータの匿名化が保証されている場合における、研究調査の実施

(v) データ主体が当事者である契約の履行又はデータ主体が当事者である契約に関連した準備手続に必要で、データ主体が要求した場合

(vi) 訴訟、行政手続又は仲裁での権利の正式な行使

(vii) データ主体又は第三者の生命又は身体的完全性を守るため

(viii) 医療専門家又は医療サービスにより施される処置において健康を守るため

(ix) データ管理者又は第三者の正当な利益のために必要な場合。ただし、個人データの保護を必要とするデータ主体の基本的権利及び自由が正当な利益に優越する場合を除く。

(x) 信用を保護するため

LGPD に基づきセンシティブ個人データを処理するための法的根拠は、次の通りである（LGPD 第 11 条）。

I データ主体による、自由で、情報を与えられた、明確な同意。当該同意は、具体的かつ強調されたものでなければならず、特定の目的を指すものでなければならない。

II データ主体の同意がない場合については、次のために必要な場合。

(a) データ管理者が法令上の義務を遵守するため

(b) 行政機関が法令、契約その他類似の文書に定められた公共政策を実施するために必要なデータの処理及び共有を行うため

(c) 研究機関について、可能な限りデータの匿名化が保証されている場合に、研究調査を行うため

(d) 契約、訴訟、行政手続又は仲裁等での権利の正式な行使のため

(e) データ主体又は第三者の生命又は身体的完全性を守るため

(f) 医療専門家又は医療サービスにより施される処置において健康を守るため

(g) 電子的システムの本人確認又は認証手続において、詐欺を防止し、データ主体のセキュリティを保証するため。ただし、LGPD 第 9 条に定められたデータ主体権が保護される場合に限り、データ主体の基本的権利及びが優先され、個人データの保護が必要とされる場合を除く

他の法人への個人データの移転も処理に含まれ、一つの企業グループ内での共有であっても処理の法的根拠を特定することが必要であるところ、通常の個人データの移転については、組織は一般的に正当な利益（LGPD 第 7 条第 IX 号）によることができる一方、センシティブ個人データの移転については、適切な処理の法的根拠を見出すことがより困難となる。通常、契約に基づくものを含む権利の正式な行使（LGPD 第 11 条第 II 号 d）がその根拠となる場合が多いと考えられる。

2. 利用

LGPD 上の「処理」の定義に基づき、センシティブデータに関する「処理」のルールが適用されるため、取得と同様のルールが適用される。定義については、IV. 2.を参照。

3. 第三者提供

LGPD によると、通常の個人データ、センシティブデータいずれについても、第三者提供に関する同様の規律が適用される。

4. 管理

センシティブ個人データは、より高い水準の保護を受ける。

LGPD は、特にセンシティブ個人データの場合、可能な限り、データの匿名化、又は少なくとも仮名化を強く推奨しており（第 11 条第 II 号 c）、匿名化されたデータは（完全に匿名化された限りで）個人データとしての保護の対象から外れる（第 12 条）。なお、匿名化それ自体は法的根拠を必要としないと考えられる。

また、ANPD は、データ管理者に対し、商業及び産業の秘密を害しない範囲で、データ処理業務に関する、センシティブ個人データを含む個人データの保護に関するデータ保護影響評価（DPIA）の実施を求める権限を有する（LGPD 第 38 条）。LGPD に基づく DPIA は、データ管理者が作成しなければならない文書であり、市民の自由及び基本的権利にリスクを及ぼす可能性のある、個人データにかかわる処理行為、並びに対策、保護手段及びリスク緩和メカニズムの記述を含まなければならない（同条）。どのような処理がハイリスクとみなされるのかといった点を明示するリストは現時点では公表されていない。

5. 漏えい等

LGPD 上、データ管理者は、データ主体に重大なリスク若しくは損害を引き起こし、又は引き起こす可能性があるセキュリティインシデントが発生した場合、合理的な期間内に ANPD 及びデータ主体に通知する必要がある（LGPD 第 48 条）。

ANPD によると、重大なリスク又は損害を引き起こす可能性があるインシデントとは、特に大規模なデータ、センシティブデータ並びに児童及び青年又は老人のような脆弱なグループからのデータにかかわる場合、データ主体に対して物的又は精神的な損害を与え、データ主体を差別又はなりすましの危険がある状況にさらす可能性があるものをいう（本ガイダンス）。

LGPD は、インシデントの通知を ANPD に対してだけでなく、データ主体に対しても行うことを求めている（LGPD 第 48 条）。通知は、データ主体に対して重大なリスク又は損害（すなわち、金融詐欺及びなりすましを含む資産的損害を与える可能性があるかどうか、影響を受けるデータ主体の数、インシデントの結果データにアクセスできた第三者の意思、影響を受けるデータ主体が脆弱な当事者とみなされるかどうかという要素が考えられる。）を引き起こす可能性があるセキュリティインシデントについて行われなければならない（同条及び本ガイダンス）。LGPD は、データ管理者に、インシデントが疑いの段階であっても、データ管理者は当局及びデータ主体に通知すべきとしている（ANPD のウェブサイトにおける説明[114]）。

通知について法律上具体的な期限は定められていないが、ANPD は、予備的ではあるものの推奨事項として、インシデントを認識してから 2 営業日以内に通知することを推奨している（本ガイダンス）。

6. 請求権

通常の個人データとセンシティブな個人データには、同じデータ主体の権利が適用される（LGPD 第 18 条）。

[114] https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/incidentes-de-seguranca-com-dados-pessoais

## V. 本人同意、プロファイリング

### 1. 本人同意

#### (1) センシティブデータ規制（上記III）との関係

上記 III の通り、LGPD では、個人データの各処理行為は、法に定められた法的根拠に従って行われなければならないとされており、センシティブ個人データについては、処理のための法的根拠について通常の個人データに比して厳格な要件が課されているところ、本人の同意は、LGPD が定めるセンシティブ個人データを処理するための法的根拠にあげられている（LGPD 第 11 条）。

#### (2) 要件一般

データ主体の同意に基づきセンシティブ個人データを収集する場合、下記(3)〜(6)に加え、LGPD 第 11 条第 I 号で推奨されるように、具体的かつ強調した方法で同意を取得することが必要であるとされる。強調されたフォームに関しては、収集されるセンシティブ個人データの種類及び処理行為者により利用その他の処理がされる具体的な目的を示すために、センシティブ個人データの処理のための権限付与が本文と分離されて表示されていることなどが推奨される（ANPD の公表する *Guia Orientativo: Cookies e proteção de dados pessoais*（クッキー及びデータ保護に関するガイドライン）[115]）。

データ主体が明らかに公開したデータについては、データ主体の権利の保護及び LGPD に規定された原則の遵守を条件として、同意に関する要件は免除される（第 7 条第 4 項）。同意の要件が免除される場合であっても、処理行為者が LGPD に基づく他の義務、特に一般原則の遵守及びデータ主体の権利の尊重は依然求められる（第 7 第 6 項）。

#### (3) 情報提供

LGPD は、データ主体に次の通知事項を定めている。

(i) 同意拒否の可否及び同意拒否の帰結に関する情報（LGPD 第 18 条第 VIII 号）

(ii) データ処理活動の目的（LGPD 第 9 条第 I 号）

(iii) 個人データの第三者との共有に関する情報（同条第 V 号）

(iv) データ処理活動を行うデータ処理行為者の情報（同条第 VI 号）

(v) データ管理者の身元確認情報及び連絡先情報（同条第 III 号及び第 IV 号）

(vi) LGPD 第 18 条に基づき与えられる権利への明示的な言及を含む、本人の権利（同条第 VII 号）

(vii) データ処理活動の形式及び期間（同条第 II 号）

#### (4) 形式

LGPD は、書面その他データ主体の意思を証明できる手段により、データ主体の同意を得る必要がある旨定める（第 8 条）。

[115] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf

同意が同意以外を表明する文脈の書面においてなされる場合、同意の文言は他の事項から明確に区別されなければならない。センシティブ個人データについていえば、同意は特に具体的かつ強調された形でなされなければならない（第 8 条第 1 項）。

さらに同意は、特定の目的のために個人データを処理することに対して、データ主体が自由で（すなわち、同意するか拒否するかについて、データ主体に実質的な選択権がなければならない）、情報を与えられた、明確な表明としての同意でなければならない。個人データ処理についての一般的又は黙示的な承認は無効とされる（第 8 条第 4 項）。

(5) 個別同意の必要性

各処理目的について、個別に同意を得ることが必要である。複数の異なる処理目的のために一括で同意を取得することを許容する法的根拠はなく（第 8 条第 4 項）、処理の新たな目的がある場合、新たな同意を得なければならない（第 8 条第 6 項）。

(6) 同意撤回

LGPD 上、本人は同意を撤回することができ、その撤回は容易かつ無償であるべきと規定されている（第 8 条第 5 項、第 18 条第 IX 号）。

同意が撤回された場合、同意に基づく処理は停止しなければならず、関連する個人データは速やかに消去しなければならない（法律上の保管義務が適用される場合を除く。LGPD 第 15 条第 III 号、第 16 条及び第 18 条第 VI 号））。データ処理行為者は、個人データを提供した者に対し、当該個人データを消去するように速やかに通知しなければならない。ただし、通知が不可能であり、又は負担が不釣り合いに大きい場合はこの限りではない（LGPD 第 18 条第 6 項）。

(7) その他留意事項

LGPD は、LGPD を遵守して同意を本人から取得したことの証明はデータ管理者がすべきと規定している（LGPD 第 8 条第 2 項）。したがって、少なくとも潜在的な請求に対して防御するために、同意管理システムを導入することが一般的に推奨される。

同意の言語について、LGPD で明示的に規定された要件はないものの、ANPD 及び裁判所により、情報が提供されていない、又は自由に行われたものではないとみなされるおそれがあるため、ポルトガル語で同意を取得することを強く推奨される。この点については、将来的に規制される可能性がある。

2. プロファイリング

(1) プロファイリング・データ分析に対する規律

III. 11 の回答のとおり、LGPD 第 12 条第 2 項によると、特定の個人の行動プロフィールを形成するために利用されるデータは、個人が識別される場合には、個人データとみなされ得る。

さらに、データ主体は、個人、職業、消費、信用のプロフィール又は人格の諸側面を確定することを目的とした決定など、個人データの自動的な処理又は分析のみを基礎とした個人の利益に影響を与える決定について、再調査を求める権利を有する（LGPD 第 20 条）。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

LGPD 上、プロファイリング・データ分析により生成されたデータに関するセンシティブ個人データの該当性についての特別の定めは無い。プロファイリングその他のデータ分析により生成されたデータが、LGPD の定義によるセンシティブ個人データに該当する場合には、センシティブ個人データに該当する。プロファイリングその他のデータ分析が一般的な個人データに帰着する場合、当該データはセンシティブであるとはみなされない。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

プロファイリングによりセンシティブ個人データを生成する場合にはセンシティブ個人データを処理するルールが適用される。生成されたデータは、現在、*Guia Orientativo: Aplicação da Lei Geral de Proteção de Dados (LGPD) por agentes de tratamento no contexto eleitoral*（データ処理エージェントによる電子的方法の文脈における処理への LGPD の適用に関するガイドライン[116]）の推奨事項によると、ANPD によりセンシティブ個人データとみなされているからである。

## VI. センシティブデータの取扱いに係る裁判例・決定等

データ保護をブラジルの法的枠組みに包括的に導入したのは、比較的最近であることから、執行事例や判例法理は、ブラジルにおいてまだ発達途上といえる。もっとも、本調査の趣旨に鑑み言及に値すると考えられる事例として、以下の通り、不適切な顔認識行為につき、ViaQuatro が 100,000 レアルの罰金が科された例がある。

> 2021 年 5 月 10 日、サンパウロ高等裁判所は、ViaQuatro 社に対し、顔認識技術を不適切に使用したとして、100,000 レアルの罰金を科す決定を下した[117]。IDEC（ブラジルの消費者保護機関）によると、とりわけ、ViaQuatro は利用者の同意なく地下鉄駅で顔認識データを収集したため、罰金を科され、反応を捉える目的で広告の前にいる人の存在を認識し、感情、性別及び年齢層を識別するカメラの実装及び使用を継続することを禁止された。裁判所の決定は、単なる顔認識や顔検出は生体データとみなされる可能性があるが、ViaQuatro 社のそれらのデータ処理が LGPD 第 11 条に規定されている法的根拠に基づいていなかったとした。また、同決定は、データ処理の目的は、合法的、具体的、明示的かつ情報主体に通知されたものでなければならず（LGPD 第 6 条第 I 号）、今回のケースでは、顔認識はマーケティング目的で使用され、データ主体はそのような使用について通知されていなかったと述べている。さらに同決定は、収集された画像の中には子供や青少年の画像も含まれていることに触れており、それらの画像は未成年者の最善の利益のために処理されるべきであったこととなる（LGPD 第 14 条）。さらに、IDEC は、地下鉄駅にはそのような技術が使用されている表示がなかったため、これらの行為に透明性が欠如していたことも強調している。

## VII. その他 （上記の他、センシティブデータの取扱いに適用される規律）

センシティブデータへの明示的な言及はないものの、法律 No. 9.029/95 は、仕事へのアクセスについて差別的又は制限的な行為をすること及びそれを維持することを禁じる（使用者が従業員に対して差別的行為を行うこと、及び LGPD においてセンシティブ個人データに該当し得る特定の種類の個人データを求めることを禁ずる。したがって、例えば、使用者が女性の従業員に対して妊娠検査又は妊娠証明を求めることを禁ずる（第 2 条第 I 号））。LGPD は、特に使用者による従業員のデータの処理を特に規制

[116] https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_lgpd_final.pdf
[117] Case No. 1090663-42.2018.8.26.0100

する規定を有していないが、労働関係に対しても適用される。LGPD は、例えば、差別禁止原則を定め（第 6 条第 IX 号）、処理行為は、不正、濫用的な、又は差別的な目的で行ってはならないと規定する。労働関係におけるデータ保護は、ANPD その他機関により、さらに規律され得る。

なお、ジェンダーアイデンティティについて、2019 年にブラジル最高裁（STF）が、「ジェンダーアイデンティティ差別」が人種差別の概念に適合するという判例法を確立した。STF の解釈では、「ジェンダーアイデンティティ差別」（gender identity）は人種差別と同様に考えらえるとしている。LGPD において、「人種」は、上記で引用したとおり、センシティブ個人データとみなされる。学者の間でも「ジェンダーアイデンティティ」がセンシティブ個人データの概念に含まれるか否かという議論が行われているがあり、通説となる立場は存在しない。

このほか、個人データの保護に特化した法令ではないものの、個人データに関する規定が含まれている法令としては以下の通りである。

| 法令の名称 | URL | 公的部門又は民間部門 |
|---|---|---|
| *Constituição Federal de 1988*（1988 年ブラジル連邦共和国憲法） | ポルトガル語：<br>https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm<br><br>英訳：<br>https://www.stf.jus.br/repositorio/cms/portalStfInternacional/portalStfSobreCorte_en_us/anexo/Constitution_2013.pdf | 公的部門及び民間部門 |
| *Código Civil*（ブラジル民法典—法律#10,406/02） | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/Leis/2002/L10406.htm | 民間部門 |
| *Código de Defesa do Consumidor* (CDC)（ブラジル消費者保護法（CDC）—法律#8,078/90） | ポルトガル語：<br>https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm -<br><br>英訳：<br>http://www.procon.rj.gov.br/procon/assets/arquivos/arquivos/CDC_Novembro_2014_Ingles.pdf | 公的部門及び民間部門 |
| *Marco Civil da Internet*（インターネット法的枠組み—法律#12,965/14） | ポルトガル語：<br>https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm<br><br>英訳：<br>https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180 | 公的部門及び民間部門 |
| *Código Penal*（刑法典—法律#12,737/12 により改正） | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm | 公的部門及び民間部門 |
| *Lei de Interceptação Telefônica*（通信傍受法—連邦法#9,296/96） | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm<br><br>*翻訳はない。 | 公的部門及び民間部門 |

| | | |
|---|---|---|
| *Lei do Sigilo Bancário - Lei Complementar # 105/01*（銀行秘密法—補足法 No. 105/01） | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/LEIS/LCP/Lcp105.htm<br><br>*翻訳はない。 | 公的部門及び民間部門 |
| *Lei de Acesso à Informação*（ブラジル情報アクセス法—連邦法#12,527/11) | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm<br><br>*翻訳はない。 | 公的部門 |
| *Lei do Cadastro Positivo*（優良支払人登録法（Good Payer's Registry Law）—連邦法#12,414/11。補足法 No. 166/2019 により改正） | ポルトガル語：<br>http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm<br><br>*翻訳はない。 | 公的部門及び民間部門 |
| *Recomendações para Comunicação de Incidente de Segurança da ANPD*（セキュリティインシデント通報に関する ANPD 推奨） | ポルトガル語：<br>https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis<br><br>*翻訳はない。 | 公的部門及び民間部門 |

# 第8章.　オーストラリア

## I.　総論

### 1.　個人情報の保護に関する法令等

個人情報の保護に関する包括的な法令として、1988 年プライバシー法（Privacy Act 1988）（以下「プライバシー法」という）[118]、同法に 含まれるオーストラリア・プライバシー原則（Australian Privacy Principles）（以下「プライバシー原則」という）[119]が存在する。これらの法令は公的部門、民間部門のいずれも対象としている。

### 2.　センシティブデータの取扱いに対する規制の趣旨

センシティブ情報（sensitive information）は、プライバシー原則のもと、より高度なレベルのプライバシー保護が与えられている。これは、センシティブ情報の不適切な取り扱いが、個人又はその関係者に特に不利な結果をもたらす可能性があることを認識したものである（例えば、人種、民族的出身、組合員などに基づく差別や不当な扱いが行われる場合がある）。また、センシティブ情報の不適切な取り扱いは、屈辱や困惑を引き起こしたり、個人の尊厳を損なったりする可能性が高い。

## II.　センシティブデータの範囲―総論

### 1.　センシティブデータの範囲一覧

プライバシー法の第 6 条は、「センシティブ情報」を次のように定義する。

「(a) 個人に関する情報又は意見のうち、

(i) 人種的又は民族的出身

(ii) 政治的意見

(iii) 政治的団体の会員であること

(iv) 宗教的信条又は所属

(v) 哲学的信条

(vi) 職業団体又は同業者団体の会員であること

(vii) 労働組合の組合員であること

(viii) 性的指向又は生活

(ix) 犯罪歴

に関するものであって、個人情報でもあるもの、又は

(b) 個人に関する健康情報

[118] https://www.legislation.gov.au/Details/C2022C00361
[119] https://www.oaic.gov.au/__data/assets/pdf_file/0006/2004/the-australian-privacy-principles.pdf

(c) 個人に関する遺伝情報で、健康情報でないもの

(d) 自動的な生体認証又は生体識別の目的で利用される生体情報

(e) 生体認証テンプレート」

当局の公表している主要な資料においてセンシティブ情報の上記のカテゴリーごとに分けてその例、趣旨や範囲等についての個別に具体的に説明したものとして、オーストラリア情報委員会（Office of the Australian Information Commissioner）の公表している Australian Privacy Principle Guidelines（以下、「APP ガイドライン」という）[120]があり、同文書における各データ項目に関する説明は以下の表の通りである。

| データ項目 | 資料上の解説（具体例／趣旨／範囲等） |
|---|---|
| 健康情報 | B.77　健康情報とは以下のものを指す：<br>• 個人情報である情報又は意見であって、以下に関するもの<br>　o 個人の健康状態又は障害（その時期を問わない）<br>　o 将来の保健サービスの提供に関し表明された個人の希望<br>　o 個人に提供された、又は提供される予定の医療サービス<br>• 健康サービスを提供するため、又は提供する際に収集されたその他の個人情報<br>• 個人による身体の一部、臓器、又は身体物質の提供（その予定を含む）に関連して収集された、個人に関するその他の個人情報<br>• 個人又は個人の健康又は遺伝上の親族を予測する、又は予測しうる形式の、個人に関する遺伝情報（健康情報でない他のタイプの遺伝情報は、B.138-B.141 項で議論する「センシティブ情報」に該当する）<br>B.78　健康情報の例には以下が含まれる<br>• 個人の身体的又は精神的健康に関する情報<br>• 個人の症状又は診断、及び施された治療に関するメモ<br>• 専門医の報告書及び検査結果<br>• 予約及び請求の詳細<br>• 処方箋及びその他の医薬品の購入<br>• 歯科治療記録<br>• フィットネスクラブが保有する個人に関する記録<br>• 個人の職業への適正に関する情報（それが個人の健康に関する情報を明らかにする場合）<br>• 医療サービスを提供するために収集される個人の医療用の識別子<br>• 健康サービスを提供する目的で収集された、その他の個人情報（個人の生年月日、性別、人種、セクシュアリティ、宗教に関する情報など） |
| 政治的意見<br>哲学的信条 | B.143　政治的意見や哲学的信条といった用語は、プライバシー法では定義されていない。これらは通常の意味であり、広く解釈されるべ |

[120] https://www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf

| | |
|---|---|
| | きである。ただし、個人のすべての価値観、信念、意見が政治的意見や哲学的信条とみなされるわけではない。 |
| 遺伝情報 | 下記は、遺伝上の親族の生命、健康又は安全に対する重大な脅威を防止するために、健康情報を利用できることに関し、以下の通り解説している。<br>D. 26 プライバシー法では、遺伝情報は定義されていない。個人の健康又は遺伝上の親族を予測する、又は予測しうる形式の個人に関する遺伝情報は「健康情報」の定義の対象ともなる。遺伝上の親族の生命、健康又は安全に対する重大な脅威を防止するために必要な使用又は開示が許容された健康情報の利用場面に該当することは、それがセンシティブ情報でも健康情報 でも同じである。<br>D. 27 組織が個人への健康サービス提供の過程で、あらゆる情報源から入手した個人に関する遺伝情報も、遺伝上の親族の生命、健康又は安全に対する重大な脅威を防止するために利用できる。例えば、遺伝情報には、親子関係検査の結果や、臨床的に明らかな病態を確認する情報、又は個人が病態を発症する可能性を予測する可能性のある他の情報源からの情報が含まれる。<br>D. 28 遺伝上の親族とは、プライバシー法第 6 条(1)において、兄弟姉妹、親、子孫を含むがこれに限定されない、血縁関係にある個人を意味すると定義されている。 |

学者・有識者・実務家の資料（論文・記事等）としては、Consultation Paper[121]内において、政府はセンシティブ情報の変更の可能性について、いくつかの検討事項を概説している。この文書は、現在行われているプライバシー法の見直しにあたり、位置情報、財務情報及びより広い生体情報が、新たにセンシティブ情報の定義に含まれるよう検討されるべき旨を指摘している。また、Australian Law Reform Commission（ALRC）は、2007 年に Privacy in a brave new world: ALRC proposals for privacy and technology という文書内において、下記の通り述べており、プライバシー法において生体情報をセンシティブ情報に含めるべきとされた経緯の理解に役立つ。

「生体情報には、写真、指紋、音声記録、顔認識、虹彩・網膜スキャン、指の形状、音声認識、動的署名検証、耳の形状、体臭測定、キーストローク認証、歩行認識等が含まれる。このような情報は、一般的に個人の身体的特徴に関連するため、センシティブ情報とみなされるべきである。また、生体認証情報は、文化的背景を開示したり、他の形態のなりすましを支援する情報を提供する可能性もある。生体情報にはセンシティブ情報と同レベルの保護を与えつつ、その保護が特定の状況（生体情報が本人確認のために収集される場合など）でのみ適用されるとすべきである。」

2. センシティブデータを推知させる情報（推知情報）について

推知情報がセンシティブデータに該当するかについては、場合による。

センシティブ情報の定義された事項のいずれかを合理的に明確に示唆する情報である場合、センシティブ情報となる可能性がある。例えば、多くの名字は特定の人種又は民族的起源を持つが、その名字が純粋に個人の人種又は民族的起源を明確に示すものではないため、それだけではセンシティブ情報にならない可能性がある（APP ガイドライン B.142）。

[121] https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf

上記の例では、政治的な性質の書籍を購入することは、その個人がその政治的主張と一致することが文脈上合理的に明らかでない場合、センシティブ情報に該当しない可能性がある。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。

プライバシー法の第 6FA 条は、「健康情報」（health information）を次のように定義している。

「(a) 以下に関する個人情報でもある情報又は意見。

(i) 個人の病気、障害又は傷害を含む健康状態（いつの時点のものでも）

(ii) 将来の医療サービスの提供に関しその対象となる個人が表明した希望

(iii) 個人に対して提供された、又は提供される予定の医療サービス

(b) 個人に対する保健医療サービスを提供するため、又は提供するために収集されたその他の個人情報

(c) 個人の身体の一部、臓器又は身体物質の個人による提供又は提供の意図に関連して収集されたその他の個人情報

(d) 個人又は個人の遺伝上の親族の健康を予測する、又は予測し得る形式の、個人に関する遺伝情報」

(i)　医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する。プライバシー法第 6 FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）に該当するためである。

(ii)　事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。プライバシー法第 6 FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）に該当するためである。

(iii)　消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。プライバシー法第 6 FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）に該当するためである。

(iv)　消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態は、センシティブデータに該当する。プライバシー法第 6 FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）に該当するためである。

(v)　予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無は、センシティブデータに該当する。プライバシー法第 6 FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）に該当するためである。

(2)　趣旨

OAIC は、健康情報を、開示された場合、個人に深刻な損害を与え、及び差別を受ける可能性がある最もセンシティブな情報の一つであるとみなしている。健康情報は個人が自由に共有できるものではなく、企業がどのように健康情報を収集、利用、及び開示するかについて、個人は積極的に同意しなければならないからである（OAIC による健康及び医療研究（Health and medical research）についてのガイダンス[122]）。

(3)　追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

2.　遺伝子に関するデータ

(1)　センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、センシティブデータに該当する。まず、プライバシー法第 6FA 条の定義する健康情報のうち、(d)（個人又は個人の遺伝上の親族の健康を予測する、又は予測し得る形式の、個人に関する遺伝情報）として、「センシティブ情報」に該当しうる。「遺伝情報」はプライバシー法では明確に定義されていないが、APP ガイドラインでは、遺伝情報には親子鑑定の結果や、臨床的に明らかな状態を確認する情報、及び個人がある状態になる可能性を予測できる他のソースからの情報が含まれ（APP ガイドライン D.27）、したがって（センシティブ情報の一つである）健康情報に該当する可能性があると示唆されている。

仮に「健康情報」に該当しないとしても、個人に関する遺伝情報で、健康情報でないものとして「センシティブ情報」に該当する（プライバシー法第 6 条(c)）。

(i)　医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。医師等が行った遺伝子検査の検査結果は、プライバシー法第 6FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）又は(d)（個人又は個人の遺伝上の親族の健康を予測する、又は予測し得る形式の、個人に関する遺伝情報）に該当する可能性が高い。仮に「健康情報」に該当しないとしても、個人に関する遺伝情報で、健康情報でないものとして「センシティブ情報」に該当する（プライバシー法第 6 条(c)）。

[122] https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/health-and-and-medical-research

(ii)　消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する。消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果も、プライバシー法第 6FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）又は(d)（個人又は個人の遺伝上の親族の健康を予測する、又は予測し得る形式の、個人に関する遺伝情報）に該当する可能性が高い。仮に「健康情報」に該当しないとしても、個人に関する遺伝情報で、健康情報でないものとして「センシティブ情報」に該当する（プライバシー法第 6 条(c)）。

(iii)　消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、センシティブデータに該当する。消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報も、プライバシー法第 6FA 条の定義する健康情報のうち、(a)(i)（個人の病気、障害又は傷害を含む健康状態）又は(d)（個人又は個人の遺伝上の親族の健康を予測する、又は予測し得る形式の、個人に関する遺伝情報）又は個人に関する遺伝情報で、健康情報でないものとして、「センシティブ情報」に該当する（プライバシー法第 6 条(c)）。

(2)　趣旨

オーストラリア政府は、遺伝情報は独特の影響力を持ち、プライバシーと差別に対する特別な脅威をもたらすものであり、専用のより高度なレベルの法的保護が必要であるとみなしている。遺伝情報は、個人の民族性に関する更なる情報を暴露する可能性があり、これもまたセンシティブな情報であるため、同様の保護が与えられるべきであるからである（OAIC「Privacy Act Review – Discussion Paper (Submission by the OAIC) 2021」[123]11.62 項、ALRC「Essentially Yours: The Protection of Human Genetic Information in Australia (ALRC Report 96; Privacy Legislation Amendment Bill 2006 Explanatory Memorandum)」[124]）。

(3)　追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

3.　性生活・性的指向に関するデータ

(1)　センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する（プライバシー法第 6 条(a)(viii)）。

[123] https://www.oaic.gov.au/__data/assets/pdf_file/0023/11894/OAIC-submission-to-Privacy-Act~scussion-Paper-December-2021.PDF
[124] https://www.alrc.gov.au/publication/essentially-yours-the-protection-of-human-genetic-information-in-australia-alrc-report-96/

(2) 趣旨

オーストラリア政府は、個人の性生活及び性的指向に関するデータが開示されることにより、差別又は不当な扱いを受ける可能性があるとしている。これらの情報の誤った取り扱いは、屈辱や羞恥心を引き起こし、及び個人の尊厳を損なう可能性があるためである。また、OAIC は、これらの情報をどのように提供し、開示するかは、個人の積極的な選択に基づくべきものとしている（APP ガイドライン B.144、ALRC「For Your Information: Australian Privacy Law and Practice (ALRC Report 108)」[125]）。

(3) 追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する。労働組合員としての地位は全てセンシティブデータに該当する（プライバシー法第 6 条(a)(vii)）。

(2) 趣旨

労働組合への加入に関するデータが不正に開示された場合、特に雇用の場において差別及び不当な扱いを受ける可能性がある。したがって、OAIC は、偶発的な情報開示を保護するために、さらなる法的保護を実施する必要があるとしている（APP ガイドライン B.144、ALRC「For Your Information: Australian Privacy Law and Practice (ALRC Report 108)」）。

(3) 追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、自動的な生体識別又は生体認証を目的として特別に収集される場合にはセンシティブデータに該当する。

[125] https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/

OAIC が示した、生体データのうちセンシティブ情報に該当する対象の具体例は、個人の顔、指紋、虹彩、手のひら、署名又は声の電子コピーである（OAIC による生体認証情報スキャニング（Biometric scanning）についてのガイダンス[126]）。オーストラリア政府は、生体情報とみなされるものの範囲が広いため、追加的な保護は、自動的な生体識別又は生体認証を目的として特別に収集される生体情報のみに適用されると述べている（APP ガイドライン B.141）。

(2) 趣旨

政府は、生体情報は他のセンシティブ情報と同様の属性を持つため、当該情報により高度なレベルの保護を与えることが望ましいと考え、生体情報をセンシティブ情報に含めた（オーストラリア議会下院「Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum」[127]、ALRC「For Your Information: Australian Privacy Law and Practice (ALRC Report 108)」）。生体情報をセンシティブ情報に含めない場合、顔認識技術等の生体技術が本人の認識や同意なしに個人を特定するために利用される可能性があること、及び生体情報から本人の健康、人種・民族的出身、宗教的信条に関する更なるセンシティブ情報が明らかになることが懸念されたため、生体情報をセンシティブ情報に含めることとした。

(3) 追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータは、センシティブデータに該当しない。

(2) 趣旨

オーストラリア政府の見解では、金融情報は、現在センシティブ情報の定義に含まれている他の情報とは異なり、個人の身体的属性又は個人的信条に関連しないため、センシティブ情報の定義に含めるべきではない、とされている。OAIC は、オーストラリアのデジタル経済において、金融情報は日常的に個人によって共有されているとも言及している。多くの状況において、個人は金融情報を提供するか否かを現実的には自由に選択できないと解される。なぜなら、金融情報はサービスを提供するために必要である可能性があり、又は金融情報の収集、利用、開示若しくは記録を要求する複数の規制や制度に基づき要求されるからである。このような事情から、金融情報の取り扱いに追加の同意要件を課しても、大半の状況において、プライバシー保護としては限られた影響しか与えない可能性がある。追加の同意要件が適用されていない現状において、多くの団体が金融・財産に関する情報を収集することが法律によって義務付けられているところ、日常的に共有されている情報の取り扱いに摩擦を生じさせたり、この

[126] https://www.oaic.gov.au/privacy/your-privacy-rights/surveillance-and-monitoring/biometric-scanning
[127] https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf

情報の取り扱いに同意できる集団に誤った期待を生み出す可能性がある。（OAIC「Privacy Act Review – Discussion Paper (Submission by the OAIC) 2021」2.33 項から 2.35 項）

(3) 追加的規律（該当する場合）

個人情報の収集・利用・開示に関する標準規律（プライバシー法）以外の追加規律はない。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータは、センシティブデータに該当しない。

(2) 趣旨

OAIC の見解によると、金融情報と同様、信用情報は個人の身体的属性又は個人的信条に関連するものではなく、容易に共有できることが要求されるため、センシティブ情報とはみなされないとされている（OAIC「Privacy Act Review – Discussion Paper (Submission by the OAIC) 2021」2.34 項）。

(3) 追加的規律（該当する場合）

個人情報の収集・利用・開示に関する標準的な規律（プライバシー法）以外の追加的な規律はない。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。

(2) 趣旨

OAIC の見解によると、金融情報及び信用情報と同様、本情報は個人の身体的属性又は個人的信条に関連するものではなく、容易に共有できることが要求されるため、センシティブ情報とはみなされないとされている（OAIC「Privacy Act Review – Discussion Paper (Submission by the OAIC) 2021」2.34 項）。

(3) 追加的規律（該当する場合）

個人情報の収集・利用・開示に関する標準的な規律（プライバシー法）以外の追加的な規律はない。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

この節では、「成年後見制度の保護を受けている」という状態は、その人がもはや健全な精神状態でなくなり、法律上及び金銭上の決定を行うために指名された委任状が必要とされる場合を指すものとる。

このような状況では、本人の健康状態が明らかに示唆されるため、成年後見制度の保護を受けている事実に関するデータはセンシティブな情報となる可能性が非常に高い。

(2) 趣旨

健康情報に関する 1.(2)の回答を参照されたい。

(3) 追加的規律（該当する場合）

IV.に記載されている規律以外に適用されるものはない。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報は、大人に関する情報と同じように扱われ、当該情報が機微（sensitive）とみなされる事項に関するものであれば該当することとなる。児童に関する情報であることをもってセンシティブデータとして取り扱われるわけではない。

(2) 趣旨

OAIC は、児童を含むすべての個人がプライバシー法の下で保護されるべきであり、児童について収集された情報のうちセンシティブ情報は、同様に高度な保護のもと取り扱われることを表明している（OAIC による児童及び青少年（Children and young people）についてのガイダンス[128]）。OAIC は、その理由を明らかにしていない。

[128] https://www.oaic.gov.au/privacy/your-privacy-rights/more-privacy-rights/children-and-young-people#:~:text=The%20Privacy%20Act%201988%20protects,must%20have%20capacity%20to%20consent

(3) 追加的規律（該当する場合）

児童がセンシティブ情報の提供に同意できるかどうかという観点では、現在、18 歳未満の個人の個人情報を取り扱う組織又は機関は、本人に同意能力があるかどうかを個別に判断しなければならない（APP ガイドライン B.59）。原則として、18 歳未満の個人は、提案された内容を理解する成熟度があれば、同意する能力があるとされている（APP ガイドライン B.60）。成熟していない場合は、親又は保護者が本人に代わって同意することが適切とされる場合がある（APP ガイドライン B.60）。

組織又は機関が個人の能力をケースバイケースで評価することが現実的でない場合、組織又は機関は、不明な場合を除き、原則として、15 歳以上の個人には能力があると見なすことができる（APP ガイドライン B.61）。

なお、現在プライバシーレビューが実施されており、それに伴い児童に関する情報についての立場の検討が進められている（オーストラリア司法省（Attorney-General's Department）「Privacy Act Review Report 2022」[129]、同「Privacy Act Review Discussion Paper October 2021」[130]）。

そこでは、プライバシー法を改正し、16 歳未満の児童の場合、親又は保護者による同意を必要とすることが検討されてきた。オーストラリア司法省のディスカッション・ペーパーは、実際に可能である場合には、事業者が個別に能力を評価することを許すべきかどうかについて、追加のフィードバックを求め、また、親又は保護者の同意を得なければならない場面についても、次のような案を示して意見を求めた。

- オプション 1 - 16 歳未満の児童の個人情報を収集、利用、開示する前に、親又は保護者の同意を必要とする。
- オプション 2 - 16 歳未満の児童について、センシティブ情報の収集前、又は個人情報の二次利用や開示を行うために利用可能なメカニズムなど、現在プライバシー法が同意を要求している場面において親又は保護者の同意を必要とする。

オプション 1 が採用された場合、個人情報の内容や処理目的にかかわらず、子どもの個人情報を扱う前に保護者の同意が必要となる。Privacy Act Review Report 2022 は、教育や医療など、子どもの生活における多くの合法的かつ日常的な活動は、かかる同意の取得のために中断するようなことなく遂行される必要があり、このオプションの導入は困難であると指摘している。この点につき、OAIC は、すべての状況において同意は必要でも適切でもないという見解を提出した（Privacy Act Review - Discussion Paper, Submission by the Office of the Australian Information Commissioner, Part 13）。16 歳未満の児童の個人情報の取り扱いに関するすべての状況において、親又は保護者の同意を必要とすることは、事業者に不必要なコンプライアンス負担を生じさせ、よりリスクの高い状況における同意の価値を損なう可能性があることが配慮されているといえる。

また、ディスカッション・ペーパーでは、事業者が個人別に同意を行う能力を評価することを認めるべきかどうかについての意見も求めている。そのほか、アクセス、訂正、消去の要求を含め、子供が両親から独立してプライバシーに関する要求が可能となる時期も、想定される（同意）能力年齢によって決定される。

寄せられた意見を踏まえ、Privacy Act Review Report 2022 は、児童及び青少年と同意能力に関する既存の OAIC のガイダンス（具体的には APP ガイドライン B55 から B61 を指す）に引き続き依拠することが推奨されるとしている。これに従えば、18 歳未満の個人に同意能力があるかどうかは、事業体がケー

[129] https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report
[130] https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/user_uploads/privacy-act-review-discussion-paper.pdf

スバイケースで判断でき、また、子どもの個人情報を取り扱う場合に必ず親又は保護者の同意を必要とするというわけではないこととなる。

11. オンライン行動履歴に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報がセンシティブデータに該当するか否かは、その情報が個人のセンシティブ情報を明らかに推測させるかどうかによる。例えば、オンライン活動から、個人が労働組合のメンバーであること、又は政治的所属や性的指向を有していることが分かる場合、当該情報はセンシティブな情報に該当する（APP ガイドライン B.141）。

(2) 趣旨

オンライン行動のモニタリングから生成される情報のすべてが、個人のセンシティブ情報、又は個人情報を示唆するとは限らない。このため、明らかになったすべての情報に対して、より高度な保護が与えられるべきであるとはいえない。

(3) 追加的規律（該当する場合）

個人情報の収集・利用・開示に関する標準規律(プライバシー法)以外の追加規律はない。

IV. センシティブデータの取扱いに適用される規律

1. 取得

プライバシー原則第 3.3 条は、本人がその情報の収集に同意しており、かつ、以下のいずれかに該当する場合を除き、事業者は個人に関するセンシティブ情報を収集してはならないとしている。

(i) 事業者が政府／公的機関の場合 - 当該情報が、当該事業者の一つ以上の機能又は活動に合理的に必要である、又は直接的に関連している場合

(ii) 事業者が組織（民間企業）の場合 - 当該情報が、当該事業者の一つ以上の機能又は活動に合理的に必要なものである場合

事業者は、センシティブ情報を収集する際に本人に通知された特定の目的のためにのみ収集しなければならない（プライバシー原則第 5.1 条）。

但し、プライバシー原則第 3.4 条に基づき、以下の例外規定のいずれかが適用される場合、事業者は同意なしにセンシティブ情報を収集できる。

(a) 情報の収集が、オーストラリアの法律又は裁判所の命令又はその下で要求若しくは許可される場合

(b) プライバシー原則による情報収集に関連して、一般的に許容されている状況*が存在する場合。

(c) 事業者が組織であり、当該事業者による情報の収集に関連して、許容されている健康に関する状況**が存在する場合

(d) 事業者が執行機関であり、かつ、以下に該当すると当該機関が合理的に判断する場合

(i) 当該機関が移民局の場合、情報の収集は、当該機関が行う又は当該団体に代わって行う一つ以上の執行関連活動のために合理的に必要である、又は直接的に関連している場合

(ii) その他 - 情報の収集は、当該機関の 1 つ以上の機能又は活動のために合理的に必要である、又は直接的に関連している場合

(e) 事業者が非営利団体であり、かつ以下のいずれもに該当する場合。

(i) 情報が団体の活動に関するものである場合

(ii) 当該組織のメンバー又は当該組織の活動に関連して当該組織と定期的に接触している個人のみに関連する情報である場合

* プライバシー法の第 16A 条には、「一般的に許容されている状況」が規定されている。一般的に許容されている状況とは、以下の 7 つの状況のことであるり、ここにおける個人情報の規律がセンシティブ情報にも適用される。

| 項番号 | 対象となる取扱主体 | 対象となる事項 | 条件 |
|---|---|---|---|
| 1 | プライバシー原則における事業者（APP entity） | (a)個人情報<br><br>又は<br><br>(b)政府関連の識別子 | (a)収集、利用又は開示について、個人の同意を得ることが不合理又は実行不可能であり、かつ、<br><br>(b)個人の生命、健康若しくは安全、又は公衆衛生若しくは安全に対する重大な脅威を軽減又は防止するために収集、利用又は開示が合理的に必要であると考えられる場合。 |
| 2 | プライバシー原則における事業者 | (a)個人情報<br><br>又は<br><br>(b)政府関連の識別子 | (a)事業者が、その機能又は活動に関連する違法行為、又は深刻な性質の違法行為が行われた、行われている、又は行われる可能性があると疑うに足る理由を有しており、かつ、<br><br>(b)事業者がその問題に関連して適切な行動をとるために、収集、利用、又は開示が合理的に必要であると考えられる場合。. |
| 3 | プライバシー原則における事業者 | 個人情報 | (a)行方不明者として報告された人の居場所を特定するために収集、利用又は開示が合理的に必要であると考えられる場合であって、かつ、<br><br>(b)その収集、利用又は開示が「一般的に許容されている状況」に関するコミッショナーの規則を遵守している場合。 |

| | | | |
|---|---|---|---|
| 4 | プライバシー原則における事業者 | 個人情報 | 法的又は衡平法上の請求の成立、行使又は弁護のために、収集、利用又は開示が合理的に必要である場合。 |
| 5 | プライバシー原則における事業者 | 個人情報 | 収集、利用又は開示が、機密の代替的紛争解決手続のために合理的に必要である場合。 |
| 6 | 政府機関 | 個人情報 | 収集、利用又は開示が、外交又は領事業務のために合理的に必要である場合。 |
| 7 | 軍隊 | 個人情報 | オーストラリア及び外部領土の外で発生する以下のいずれかの事態のために、収集、利用又は開示が合理的に必要であると考えられる場合。<br><br>(a)戦争又は戦争的活動。<br><br>(b)平和維持又は平和の執行。<br><br>(c)民間援助、人道支援若しくは医療又は民間緊急事態若しくは災害救助。 |

**許容されている健康に関する状況とは、プライバシー法第 16B 条に基づき以下の通り定義される。

収集 ― 医療サービスの提供

(1) 組織による個人に関する健康情報の収集に関して、以下の場合に許容されている健康に関する状況が存在する

(a) その情報が、個人への医療サービスの提供に必要であり、かつ

(b) 以下のいずれかである

(i) その収集が、オーストラリアの法律（プライバシー法を除く）により、又はその法律に基づいて要求され又は認められている場合

(ii) 権原を有する保健又は医療に関する団体であってその組織を拘束する職業上の守秘義務を扱うものが定めた規則に従って情報を収集する場合

(1A) 組織による個人（第三者）に関する健康情報の収集に関して、以下の場合、許容されている健康に関する状況が存在する

(a) 患者に医療サービスを提供するために、個人（患者）の家族歴、社会歴又は病歴を収集する必要がある場合

(b) 第三者に関する健康情報が、組織が患者に医療サービスを提供するために必要な家族歴、社会歴、病歴の一部である場合

(c) その健康情報が、患者、又は患者が身体的もしくは法律的に情報を提供することができない場合には、その患者の責任者から、その組織が収集するものである場合

収集 — 研究等

(2) 組織による個人に関する健康情報の収集に関して、以下の場合に、許容されている健康に関する状況が存在する

(a) 以下の目的のために収集が必要である場合であり

(i) 公衆衛生又は公共の安全に関連する研究

(ii) 公衆衛生又は公衆安全に関連する統計の作成又は分析

(iii) 医療サービスの管理、資金提供、又は監視

(b) 当該目的が、匿名化された個人に関する情報を収集することによって果たすことができず

(c) 組織が、その収集について個人の同意を得ることが実行不可能であり

(d) 以下のいずれかに該当する場合

(i) その収集が、オーストラリアの法律（プライバシー法を除く）により、又はその法律に基づいて要求される場合

(ii) 権原を有する保健又は医療に関する団体であってその組織を拘束する職業上の守秘義務を扱うものが定めた規則に従って情報を収集する場合

(iii) 情報が、本項の目的のために第 95A 条に基づいて承認されたガイドラインに従って収集される場合

使用又は開示 — 研究等

(3) 組織による個人に関する健康情報を使用又は開示に関して、以下の場合に許容されている健康に関する状況が存在する

(a) 利用又は開示が、公衆衛生又は公共の安全に関連する研究又は統計の作成もしくは分析のために必要であり

(b) 組織が、その利用又は開示について個人の同意を得ることが実行不可能であり

(c) その利用又は開示が、本項の目的のために第 95A 条に基づいて承認されたガイドラインに従って行われ

(d) 開示の場合については、組織は、情報の受領者が当該情報又は当該情報に由来する個人情報を開示しないと合理的に信じていること。

使用又は開示 — 遺伝子情報

(4) 組織による個人に関する遺伝情報の使用又は開示に関して、 以下の場合に許容されている健康に関する状況が存在する

(a) 当該組織が、当該個人に対する医療サービスの提供の過程で当該情報を入手した場合であり

(b) 当該個人の遺伝上の親族である他の個人の生命、健康又は安全に対する重大 な脅威を軽減又は予防するために、その使用又は開示が必要であると組織が合理的に信じ

(c) 第 95AA 条に基づき承認されたガイドラインに従って使用又は開示が行われ

(d) 開示の場合については、情報の受領者が当該個人の遺伝上の親族であること

開示 ― 個人についての責任者[131]

(5) 組織による個人に関する健康情報の開示に関して、以下の場合に許容されている健康に関する状況が存在する

(a) 組織が当該個人に対して医療サービスを提供する場合で

(b) 情報の受領者がその当該個人についての責任者であり

(c) 当該個人が以下のいずれかに該当し

(i) 開示に同意することが身体的又は法的に不可能である

(ii) 身体的に開示への同意を伝えることができない

(d) 組織のために医療サービスを提供する他の個人（介護者）が、以下のいずれかであると納得しており

(i) 開示が、当該個人の適切なケア又は治療を提供するために必要である

(ii) その開示が心情的な理由からなされる

(e) 開示が以下の要望にも反しておらず

(i) 本人が同意を与えたり伝えたりできなくなる前に本人が表明した要望であって、

(ii) 介護者が知っている、又は介護者が知っていると合理的に予想される要望

(f) 開示が、(d)に記載された目的のために合理的かつ必要な範囲に限定されている場合

2. 利用

[131] 「責任者」の具体的な範囲については、Privacy 法の第 6AA 条（親、18 歳以上の子、配偶者や一定の親族などが責任者に該当する旨が規定されている）。

事業者は、原則として、個人情報（センシティブ情報を含む）を、それが収集された目的のためにのみ利用できる（プライバシー原則第 6.1 条）。

例外として、プライバシー原則第 6.2(a)条に基づき、事業者は、収集の主要な目的に直接的に関連する二次的な目的のためにセンシティブ情報を利用できる。直接的に関連する二次的な目的とは、たとえそのセンシティブ情報が一次時的な目的（収集時等に通知される等の適法に通知された特定の目的）を達成するという観点からは厳密には必要でない場合に想定される、一次的な目的と密接に関連する目的のことである（APP ガイドライン 6.26）。この直接的な関係の要件は、センシティブ情報の利用が、屈辱、困惑、尊厳の喪失など、個人又はその関係者に重大な影響を及ぼす可能性があることを意識したものである（APP ガイドライン 6.26）。OAIC が提供する、二次的な目的が収集の一次的な目的に直接関連している場合の例として、以下が挙げられている（APP ガイドライン 6.27）。

> 「ある医療サービス提供者が、治療を提供する目的で個人の健康情報を収集した後、倫理的及び治療上の理由から、その個人を治療できないと判断する。その後、その医療サービス提供者は、他の医療クリニックに、個人の治療の必要性及びその治療を提供できないことを通知する。この他のクリニックへの開示は、情報が収集された目的に直接的に関連し、及び個人の合理的な期待の範囲内といえよう。」

3. 第三者提供

センシティブ情報の第三者への提供に関する規律は、上記 2.利用にあたって適用される規律と同様である。事業者は、二次的な目的の例外が適用されない限り、収集された目的のためにのみセンシティブ情報を開示できる（前述のとおりである）。したがって、本人がセンシティブ情報の収集に同意した時点で、その目的及び第三者への移転について本人に説明しておく必要がある。

4. 管理

プライバシー原則第 11 条が、事業者に課される個人データを管理に関する要件を定め、APP ガイドラインは個人情報（センシティブ情報を含む）の管理に関する加重的な規制を概説している。

プライバシー原則第 11 条は、事業者に対し、保有する個人情報の安全性を確保するための積極的な措置を講じること、及び個人情報を保有することが許されるかどうかを積極的に検討することを求めている。個人情報を保有する事業者は、不正利用、妨害、損失及び無許可のアクセス、修正又は開示から情報を保護するために合理的な措置を講じなければならない（プライバシー原則第 11.1 条）。

個人情報のセキュリティを確保するために企業が取るべき「合理的な手順」（reasonable steps）は、状況によって異なる。最も関係するのは、センシティブ情報に関しては、保有する個人情報の量及び機微性によって（合理的な手順は）異なるということである。一般的に、保有する個人情報の量及び又は機微性が増すにつれて、それを保護するために講じられるべき合理的な手順は増加する（APP ガイドライン 11.7）。

事業者は、プライバシー原則に基づき個人情報を利用又は開示することが可能な目的のために、個人情報がもはや必要とされなくなった時点で、保有する個人情報を破棄又は匿名化するために合理的な措置を講じなければならない（APP ガイドライン 11.22）。この要件は、個人情報が英連邦の記録（Commonwealth record）に含まれている場合、又は事業者が法律若しくは裁判所／裁判所の命令により個人情報を保持することを要求されている場合には適用されない（プライバシー原則第 11.2 条）。

個人情報を破棄又は匿名化するために組織が取るべき「合理的な手順」は、個人情報の量及び機微性に応じて増加する。個人情報の量が増える場合、又は情報が「センシティブ情報」若しくはその他のセンシティブな性質の個人情報である場合、より厳格な手順が必要とされうる（APP ガイドライン 11.33）。

5. 漏えい等

データ侵害が発生した場合、企業は NDB スキーム（Notifiable Data Breach Scheme（通知対象データ侵害スキーム））と呼ばれる、プライバシー法に基づく、データ漏洩が個人情報に関わる個人に重大な損害をもたらす可能性が高い場合、影響を受ける個人と OAIC に通知することを義務付ける枠組みに準拠しなくてはならないことがある。プライバシー法では、NDB スキームの対象となるデータ侵害を「適格データ侵害」（eligible data breach）という用語で表現する。

「適格データ侵害」とは、個人情報への不正アクセス、開示又は漏えいがあり、その個人情報が関係する個人の何人かに重大な損害をもたらす可能性があると合理的に判断される場合をいう（プライバシー法第 3C 章第 1 節）。この「重大な損害」はプライバシー法では定義されていないが、データ漏えいの文脈では、深刻な身体的、心理的、感情的、金銭的又は名声への損害が含まれ、センシティブ情報が漏えいした場合、重大な損害が生じる可能性が高くなる。センシティブ情報が漏えいしたという事実だけで、重大な損害とみなされ、事業者は影響を受ける個人及び OAIC に通知しなければならなくなる可能性がある（Data breach preparation and response: A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth), OAIC, 2019）。さらに、漏えいが事業者の過失によって発生した場合、OAIC は事業者に対して損害賠償義務を課せる（プライバシー法 13 条）。

適格データ侵害の通知の要件には、いくつかの例外がある。

- 同じ適格データ侵害を経験したプライバシー原則における他事業者が、既に NDB スキームの要件を満たしている場合（同一の漏えい等に対して、他の事業者が通知等を行った場合等）（プライバシー法第 26WM 条）。

- データ侵害が重大な損害につながる可能性がないようにするための改善措置が組織によって取られた場合（データプライバシー法第 26WF 条）。

- 法執行機関による（通知の要件の）遵守が、その執行に関連する活動を害する可能性がある場合（プライバシー法第 26MN 条）。

- 通知が英連邦の機密保持条項と矛盾する場合（すなわち、英連邦の法律 （Commonwealth law） が情報の利用又は開示を禁止又は規制している場合）（プライバシー法 26WP 条）。

- OAIC が例外を認める場合（OAIC が例外を認めるためには、プライバシー原則における事業者が例外を申請する必要がある）（プライバシー法第 26 条 WQ 条）。

- My Health Records Act 2012 に基づく違反に関して通知義務が適用される場合（My Health Records Act 2012 (Cth) 第 75 条））。

なお、適格データ侵害が発生していないため通知が義務付けられていない場合でも、組織によっては、広報やリスク軽減の理由から、影響を受けたデータ侵害について自主的に公表する場合がある。

6. 請求権

プライバシー法に基づく権利/請求権は、センシティブ情報についても個人情報と同様である。プライバシー法は、個人が、個人情報の取り扱いをよりコントロールできるようにするためのものである。プライバシー法により、個人には以下の権利/請求権が認められている。

- 個人を特定しない、又は特定の状況下で仮名（pseudonym）を利用する選択（Privacy 法第 2.1 条）。
- 個人情報（健康情報を含む）へのアクセスの要求（プライバシー原則第 12 条）。
- 不要なダイレクトマーケティングの受信停止（プライバシー原則第 7.6 条及び第 7.7 条）。
- 個人情報に誤りがある場合の訂正要求（プライバシー原則第 13.1 条）。
- プライバシー法が適用される組織又は機関が個人情報の取り扱いを誤ったと当該個人が考えている場合、その組織又は機関についての苦情申立（プライバシー法第 36 条第 1 項）。OAIC はこの苦情を調査し、その事業者に対して訴訟手続をとる可能性がある（同法第 40 条、第 55A 条第 1 項第 b 号）。

V. 本人同意、プロファイリング

1. 本人同意

(1) センシティブデータ規制（上記III）との関係

IV. 1 で上述の通り、事業者は、センシティブ情報を収集するにあたっては、原則として本人がその情報の収集に同意している必要があるとされている（プライバシー原則第 3.3 条）。事業者が本人の同意なしにセンシティブ情報を収集できる場合は、プライバシー原則第 3.4 条に定められる例外規定のいずれかが適用される場合のみに限られる。

(2) 要件一般

同意における重要な要素として、以下の４つの点が挙げられる（APP ガイドライン B.38）。

- 同意を与える前に十分な情報を得ていること。
- 自発的な同意であること。
- 同意が最新かつ具体的であること。
- 本人が自分の同意を理解し、伝える能力を有していること。

(3) 情報提供

本人から同意を取得する際には、プライバシー原則第 5 条（収集通知の要件）に定める情報を本人に提供する必要がある。これは、事業者が個人の個人情報を収集する場合、個人情報を収集する前又は収集

した時点で、一定の事項を本人に通知し、又は本人がその事項を認識できるようにするための合理的な措置を講じることを義務化するものである（プライバシー原則第 5.1 条）。提供しなければならない情報は以下の通り（プライバシー原則第 5.2 条）。

- 事業者の概要及び連絡先の詳細。
- 収集の事実及び状況：事業者が個人以外の者から個人情報を収集する場合、又は事業体が個人情報を収集したことを個人が認識する可能性がない場合、事業体が情報を収集する又は収集した事実及び収集の状況。
- 個人情報の収集がオーストラリアの法律又は裁判所の命令により、又はその命令に基づいて要求又は許可されている場合 - 情報の収集が要求又は許可されているという事実（オーストラリアの法律名又は裁判所の命令の詳細を含む）。
- 事業者が個人情報を収集する目的。
- （もしあれば）事業者が個人情報の全部又は一部を収集しない場合に個人に及ぶ主な影響。
- 当該プライバシー原則における事業者が収集する個人情報を通常開示する他の団体、組織又は個人、又はその種類。
- 事業者のプライバシーポリシーに、個人に以下の情報が含まれていること。
    - 事業者が保有する本人に関する個人情報にアクセスし、当該情報の訂正を求める方法。
    - オーストラリアの個人情報保護法の違反について苦情を申し立てる方法、及び事業者がそのような苦情に対処する方法。
- 事業者が国外の受領者に個人情報を開示する可能性があるかどうか、及び開示する可能性がある場合、実務上これを特定できるのであれば、当該受取人の所在する国。

(4) 形式

プライバシー法第 6 条第 1 項が、「同意とは、明示的な同意又は黙示的な同意を意味する」と定めている。

明示的な同意とは、口頭又は書面により明示的に与えられるものであり、これには、手書きの署名、口頭での発言、又は同意を示すための電子媒体又は音声署名の利用が含まれる（APP ガイドライン B.39）。

黙示的な同意とは、個人及び事業者の行動から、状況に応じて同意が合理的に推認できる場合に生じる（APP ガイドライン B.40）。一般的には、個人情報を特定の方法で取り扱う提案に異議を唱えなかったという理由だけで、その個人が同意を与えたとみなしてはならず、事業者は、個人情報の収集、利用又は開示の提案について個人に通知したというだけでは、同意を推認できない（APP ガイドライン B.42）。事業者が、個人の沈黙を同意と見なすことは困難であると考えられる（APP ガイドライン B.42）。個人の意図が曖昧である場合、及び個人の意図に合理的な疑いがある場合は、黙示的な合意があったとはいえない（APP ガイドライン B.42）。

OAIC は、プライバシーの重要性に鑑み、センシティブ情報の取得にあたっては明示的な同意を取得すべきとしている（APP ガイドライン B.44）。

(5) 個別同意の必要性

複数の異なる処理目的をひとまとめにして同意を取得することは可能であり、APP ガイドラインでは bundling consent（まとめられた同意）とされている（APP ガイドライン B.48）。プライバシー原則の下では、事業者は、個人が情報を提供する際に、何に同意しているのかを明確にする必要がある（プライバシー原則第 5.1 条）。目的は明確に定義される必要がある。Bundling consent の場合、どの収集、利用及び開示に同意するかを選択する機会が個人に与え られない可能性があるため、同意の任意性を損なう可能性がある。事業者は、1 つ又は複数の提示された目的に対する同意を拒否する機会を個人に提供し、 個人が提案された各目的について十分に知らされ、個人が提案された 1 つ又は複数の目的 に同意しなかった場合の結果について通知されるよう、努めるべきとされる（ APP ガイドライン B.49）。事業者は、例えば、明確ではない将来の利用に対する同意や、「すべての正当な利用又は開示」に対する同意など、目的に対して必要以上に広範な同意を求めるべきではない（APP ガイドライン B.53）。事業者は、同意を求める際に、それが関連する目的を説明しなければならない（APP ガイドライン B.53）。必要とされる明確性のレベルは、個人情報の機微性によって異なる（APP ガイドライン B.53）。

(6) 同意撤回

個人は、いつでも同意を撤回できる。同意撤回のプロセスには、個人が容易に利用可能なものであるべきとされる（APP ガイドライン B.54）。個人が同意を撤回すると、事業者は、その個人の個人情報の今後の利用又は開示について、もはや過去の同意に依拠できなくなる（APP ガイドライン B.54）。事業者は、個人が同意を撤回した場合、サービスにアクセスできなくなるなど、潜在的な影響があることを個人に認識させるべきとされる（APP ガイドライン B.54）。

(7) その他留意事項

上記回答以外の留意事項はない。

2. プロファイリング

(1) プロファイリング・データ分析に適用される規律

オーストラリアには、GDPR の第 4 条 4 項と同様のルールはない。プロファイリングその他の自動化された意思決定に特段関連するプライバシー規制はなく、プライバシー法の一般的な規律が適用されることになる。最も注目すべきは、プライバシー原則第 6 条が、センシティブ情報を二次的な目的のために利用又は開示できる範囲を制限していることである。例えば、二次的な目的が主要な目的と直接関係がない場合、個人の同意が必要となる。これにより、個人の同意なしに個人情報に基づく自動的な意思決定又はプロファイリングの実施が制限されしうる。

なお、オーストラリアにおける個人情報の定義には、個人に関する意見が含まれることには留意が必要である。収集した情報のプロファイリングの結果がその性質上機微な個人に関する意見である場合（「センシティブ情報」の一つである場合）、本報告書で概説したセンシティブ情報に関わる標準的な規則が適用される。

例えば、事業者が個人に関する健康情報を有しており、その情報のプロファイリングの結果、その個人が癌である可能性が高いことが示された場合、そのデータは個人の健康に関する意見としてセンシティブ情報となり、センシティブ情報として扱われなければならないと解される。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

上記の例で述べたように、プロファイリングによって生成されたデータは、センシティブな個人データに該当する可能性がある。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

前述の通り、センシティブデータの処理（生成）については、同様の（センシティブデータにかかる）ルールが適用される。

## VI. センシティブデータの取扱いに係る裁判例・決定等

1. Clearview AI 社についてコミッショナーが調査を開始した事案（[2021] AICmr 54（2021 年 10 月 14 日））[132]

Clearview AI 社は、個人情報の収集について個人への同意又は通知なしにセンシティブ情報を収集し、その情報を顔認識検索ツールを通じて公開した。同社は、オーストラリア人からの顔画像及び生体情報の収集の中止、及び過去に収集した全ての情報の破棄をコミッショナーから命じられた。

2. HealthEngine 社による患者データの不正利用及びレビュー操作の疑いについての訴訟[133]

HealthEngine 社は、顧客情報を患者に十分開示することなく、民間の医療保険ブローカーに提供したとして、連邦裁判所から損害賠償の支払いを命じられた。

3. コミッショナーによる 7-Eleven Store 社の調査開始（2021 年 10 月 12 日付正誤表あり、[2021] AICmr 50 （2021 年 9 月 29 日））[134]

7-Eleven Stores 社は、同意なしにセンシティブ情報を収集し、個人情報が収集される目的及び状況を個人に通知していなかった。7-Eleven Stores 社は 700 店舗で顔認証技術を導入しており、及びこの技術から得られた生体情報はセンシティブ情報に該当するとされた。

---

[132] http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html
[133] https://www.accc.gov.au/media-release/healthengine-in-court-for-allegedly-misusing-patient-data-and-manipulating-reviews
[134] https://www.oaic.gov.au/__data/assets/pdf_file/0021/10686/Commissioner-initiated-investigation-into-Eleven-Stores-Pty-Ltd-Privacy.pdf

4. Jeremy Lee　対　Superior Wood 社 [2019] FWCFB 2946

Fair Work Commission は、雇用主がセンシティブな情報を収集するためには、従業員の同意が必要であり、及びその同意は常に自発的なものでなければならないと判断した。この事例では、従業員のサインオン方法として指紋スキャナーを利用すること、及びこの技術を利用した生体情報の収集について議論された。

5. Construction, Forestry, Maritime, Mining and Energy Union　対　BHP Coal 社 t/a BHP Billiton Mitsubishi Alliance [2022] FWC 81

裁判所は、従業員の同意が懲戒処分又は解雇の脅しによるものである場合、その同意は無効であると判断した。

6. Robinson　対　Metro Trains Melbourne 社 t/a Metro Trains Melbourne [2022] FWC 1614

裁判所は、Metro Trains 社による従業員の予防接種状況の収集は、プライバシー法の違反ではないと判断した。「センシティブ情報」には健康情報も含まれるが、予防接種状況の収集は、法律によりそのような情報の収集を許可するプライバシー原則第 3.4 条(a)（情報の収集がオーストラリアの法律又は裁判所の命令により、要求又は許可されている場合）が適用され、許容される。

## VII.　その他（上記の他、センシティブデータの取扱いに適用される規律）

該当なし。

# 第9章.　韓国

## I.　総論

### 1.　個人情報の保護に関する法令等

個人情報の保護に関する包括的な法令として、個人情報保護法（Personal Information Protection Act）（以下「PIPA」という）[135]及び個人情報保護施行令（Enforcement Decree of the Personal Information Protection Act）（以下「施行令」という）[136]が存在し、個人情報保護委員会（Personal Information Protection Commission。以下「PIPC」という）から個人情報保護標準ガイドライン（Standard Personal Information Protection Guidelines）[137]が公表されている。これらの法令等は公的部門、民間部門のいずれも対象としている（個人情報保護法第 2 条第 5 項が、同法が民間部門に適用されるだけでなく、公共部門にも適用されることを規定し、また、個人情報保護委員会が発行した「2020 年個人情報保護に関する法令、ガイドライン及び告示の解説」（2020 Commentary about Laws, Guidelines and Public Notifications on Protection of Personal Information。以下「PIPC 解説書」）では、同法が官民双方に適用される一般法であることを説明している）。

### 2.　センシティブデータの取扱いに対する規制の趣旨

「センシティブ情報」は、社会的差別又は重大な人権侵害を引き起こす可能性があり、より厳格な保護が必要な機微な個人情報である（PIPC 解説書 157 頁）。したがって、センシティブ情報の処理は、別途データ主体の同意を得ている場合、又は適用される法律によりセンシティブ情報の処理が要求又は許可されている場合を除き、原則として禁止されている（PIPA 第 23 条）。

「個人識別情報」は、公共の利益のために個人に付与されるものであるが、その利便性から公共部門のみならず民間部門においても広く収集・利用され、その結果、情報が漏えいして損害を与える事例が増加している（PIPC 解説書 166 頁）。そこで、これらの情報の不正利用を防止し、本来の目的に沿い忠実に利用するため、住民登録番号など、法律に基づき個人を特定できる情報については、別途同意を得た場合又は法令により必要と認められた場合を除き、その処理は原則として禁止されている（PIPA 第 24 条及び第 24 条の 2）。

## II.　センシティブデータの範囲―総論

個人情報保護法は、「個人情報」[138]（Personal Information）とは別に、「センシティブ情報」（Sensitive Information）（PIPA 第 23 条、施行令第 18 条）及び「個人識別情報」（personally identifiable

---

[135] https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4+%EB%B3%B4%ED%98%B8%EB%B2%95#undefined（原文）、https://elaw.klri.re.kr/kor_service/lawView.do?hseq=53044&lang=ENG（英訳）。なお、本章脚注に含まれている資料の英訳リンク先は、Korea Legislation Research Institute（韓国法制研究院）の公表している英訳のページである。

[136] https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4+%EB%B3%B4%ED%98%B8%EB%B2%95#undefined（原文）、https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54521&lang=ENG（英訳）

[137] https://law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%ED%91%9C%EC%A4%80%20%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EC%A7%80%EC%B9%A8#liBgcolor0

[138] 「個人情報」については PIPA 第 2 条において次の通り定義されている。「1.　『個人情報』とは、生存する個人に関する次のいずれかの情報をいう。(a) 氏名、住民登録番号、画像等により特定の個人を識別することができる情報、(b) それ自体では特定の個人を識別できない場合でも、他の情報と容易に照合することができ、それにより特定の個人を識別することができる情報（この場合、組み合わせの容易性の有無は、他の情報を調達できる可能性等、個人を識別するために用いられる時間、費用、技術等を合理的に考慮して判断する）、(c) 上記(a)又は(b)の情報であって、下記 1-2 に従って仮

information）（PIPA 第 24 条、施行令第 19 条）をそれぞれ次の通り定義し、個人情報に関する規制とは別に規制を設けている。

「センシティブ情報」とは、思想、信条、政治的意見、労働組合又は政党への加入又は脱退、健康、性生活等に関する情報、及び大統領令で定めるその他の個人情報のうち、データ主体のプライバシーを著しく侵害する可能性のある情報をいう（PIPA 第 23 条）。大統領令とは、施行令を指し、施行令第 18 条が、遺伝子検査などから得られる DNA 情報、犯罪歴に関する情報、個人の識別を目的とした個人の身体、生理又は行動の特徴に関する情報の特定の技術処理の結果得られた情報、人種又は民族の出自に関する情報が、個人情報のうち、データ主体のプライバシーを著しく侵害する可能性のある情報に該当すると定めている。

「個人識別情報」とは、住民登録番号、旅券番号、運転免許証番号、外国人登録番号をいう。

1. センシティブデータの範囲一覧

PIPC の公表しているセンシティブ情報についての解説の資料として、PIPC 解説書において、一部のデータ項目に関する説明が存在する。データ項目に関する資料上の解説は、以下の表の通りである。

<table>
<tr><td colspan="2">（資料の名称・URL）<br>名称：2020 年個人情報保護に関する法令、ガイドライン及び告示の解説（157 頁から 173 頁参照）。<br>URL：https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS217&mCode=D010030000&nttId=6968</td></tr>
<tr><td>データ項目</td><td>資料上の解説（具体例／趣旨／範囲など）</td></tr>
<tr><td>思想・信条に関する情報（Information on ideology/belief）</td><td>個人の価値観や信念、考え方などが依拠する根拠であって、個人が様々な思想やイデオロギー傾向、宗教的信念に関する情報として堅く信じ、保持したいと思う情報</td></tr>
<tr><td>政治的意見に関する情報（Information on political opinion）</td><td>政治的な事項に関する立場についての情報、又は特定の政党を支持するかどうかについての情報</td></tr>
<tr><td>労働組合又は政党への加入又は脱退に関する情報（Information on admission to, or withdrawal from, a trade union or political party）</td><td>労働組合又は政党への加入又は脱退に関する情報<br>労働組合又は政党への加入を確認できる情報（組合又は政党の会費の支払いの詳細及び労働組合又は政党への加入又は脱退に関する直接的な情報を含む）</td></tr>
<tr><td>健康、性生活等に関する情報（Information on health, sex life, etc.）</td><td>個人の過去及び現在の病歴、身体的／精神的障害、性的指向などに関する情報<br>• 含まれるもの：発達障害者の氏名及び住所、重度障害者の氏名、住所及び電話番号、高齢者介護等級認定者の氏名、等級、等級認定日及び等級有効期限、性犯罪被害者支援事業に関する資料（当該事業対象者の氏名、生年月日、年齢及び住所）<br>• 含まれないもの：血液型</td></tr>
<tr><td>遺伝子検査などから得られる DNA 情報（DNA information acquired from genetic testing, etc.）</td><td>個人情報保護法は、センシティブ情報に分類される「遺伝子検査などから得られる DNA 情報」を定義していないが、同じ語を用いている生命倫理安全法（第 2 条第 11 項、第 2 条第 14 項、第 2 条第 15 項）では、「遺伝子検査により得られた DNA 情報」とは、「個人の遺伝的特徴に関する情報であって、当該個人のヒト材料（人体から採取され、若しくは収集された組織、細胞、血液及び体液を含むヒト構成物、又は血清、血漿、染色体、DNA（Deoxyribonucleic Acid）、RNA（Ribonucleic</td></tr>
</table>

名化されることにより、原状回復のための情報の利用又は結合を行わなければ特定の個人を識別することができなくなるもの」「1-2. 『仮名化』とは、個人情報の一部を削除し、又は全部若しくは一部を置き換えることにより、追加情報なしに特定の個人を識別することができないように加工する手続をいう。」

| | |
|---|---|
| | Acid）及びタンパク質等から分離したもの）により分析することにより得られるもの」をいうとされる。 |
| 犯罪歴に関する情報（Crime history） | 刑事罰の失効等に関する法律[139]第 2 条第 5 項に基づく犯罪歴の記録に該当する情報、すなわち、罰金以上の刑の宣告、免除又は執行猶予、保護観察、執行猶予の経過又は取消し、没収、追徴、社会奉仕命令、教育修了命令等の判決・処分に関する情報 |
| 個人の識別を目的とした個人の身体、生理又は行動の特徴に関する情報の特定の技術処理の結果得られた情報（Information resulting from specific technical processing of data relating to the physical, physiological or behavioral characteristics of an individual for the purpose of identifying such individual） | 本人確認又は認証のために、本人の顔、指紋、虹彩、筆跡など、他人と区別できる特徴を抽出する技術で処理された情報<br>例えば、写真や顔画像などは、それ自体はセンシティブ情報ではないが、個人を確認又は識別するための特定の技術により処理した結果、特徴に関する情報が生成される場合、その情報はセンシティブ情報に該当する。<br>したがって、顔認識により年齢及び性別を推定し、カスタマイズされた広告を提供するサービスや、ステッカー又は特殊効果を有するカメラアプリケーションにより、利用者の顔を自動認識して写真や顔画像などを加工することは、センシティブ情報の処理には該当しない。 |
| 人種又は民族の出自に関する情報（Information on racial or ethnic origin） | 人種とは、人類を地域や身体的特徴によって分類したものをいう。民族とは、ある地域で長い間集団生活を送る中で、共通の言語や文化に基づいて歴史的に形成された社会集団であり、必ずしも血統又は国家単位としての国民と一致するものではない。 |

学者・有識者・実務家の資料（論文・記事等）のうち、上記の PIPC により公表されている資料と同程度又はそれ以上の影響力を実務上有しているものとして、以下のような資料が存在する。

| （資料の名称・URL）名称：『個人情報保護法』No-Hyung Park　Parkyoungsa　2020 年（293 頁から 299 頁を参照） | |
|---|---|
| データ項目 | 資料上の解説（具体例／趣旨／範囲など） |
| 健康に関する情報 | 車椅子での移動が必要であるというホテルの予約記録、又は特定の個人が薬物中毒者であるという社会福祉記録は、センシティブ情報に該当する。 |
| 性生活に関する情報 | 個人の性的嗜好、性行為の頻度などに関する情報を含む。 |
| 人種又は民族の出自に関する情報 | 人種が、肌の色を含む個人の身体的特徴に基づく概念であり、変わることがないのに対し、民族は、祖先、文化、宗教を含む個人のアイデンティティに基づく概念であり、変わることがある。旅客がコーシャフードを希望したという航空会社の記録は、民族情報に該当する。 |
| （資料の名称・URL）名称：『個人情報保護法』（改訂版）Yong-Hak Kim　Cheongho Books　2021 年（49 頁から 50 頁を参照） | |
| データ項目 | 資料上の解説（具体例／趣旨／範囲など） |
| 個人の識別を目的とした個人の身体、生理又は行動の特徴に関する情報の特定技術処理の結果得られた情報 | 身体情報には顔、身長などの情報、生理情報には指紋、虹彩、静脈、網膜などの情報、行動情報には歩行、筆跡などの情報が含まれる。 |

[139] 刑事罰の失効等に関する法律 https://elaw.klri.re.kr/kor_service/lawView.do?hseq=46412&lang=ENG (英訳)

2. センシティブデータを推知させる情報（推知情報）について

「センシティブ情報」を推知させる情報も、センシティブデータに分類されると考えられる。

例えば、PIPA 第 23 条第 1 項では、「健康に関する情報」を「センシティブ情報」と規定しているが、PIPC の決議（2021-123-047 番）では、個人が診療を受ける医療機関の名称（病院名）及び診療開始日に関する情報は、特定の疾病名又は医学的見解を直接示すものではないものの、その情報から病気の種類の予測や、その病気の発症時期及びある時期の健康状態を推測することができることから、健康に関する情報として、「センシティブ情報」に該当するものと結論づけている。

## III. センシティブデータの範囲―各論

### 1. 健康に関するデータ

#### (1) センシティブデータへの該当性　どこまでのデータが該当するか

健康に関するデータは、センシティブデータに該当する。PIPA 第 23 条 1 項は、健康に関する情報がセンシティブデータに該当することを規定している。

(i)　医師その他の医療関連職務従事者（以下「医師等」）が行った検査結果

医師等が行った検査結果は、センシティブデータに該当する。

PIPA 第 23 条第 1 項によれば、個人の健康に関する情報が「センシティブ情報」に該当する。健康に関する情報は、その情報を誰が作成又は入手したかによって、特に区別されていない。従って、個人の健康に関する情報であれば、PIPA の「センシティブ情報」に該当すると考えられる。

健康情報については、PIPC が公表した「保健医療情報等の利用に関するガイドライン（2020 年 9 月）」により詳細な記述があり、そのガイドラインによると、健康情報には以下のものが含まれる。

- 医療法（Medical Service Act）に基づく診療記録及び電子強制記録、その他病院で作成された治療内容を示し、又は容易に推察できる記録（診療内容が記載された病院の領収書）
- 国民健康保険サービス、健康保険審査評価サービス、その他の民間保険会社等が収集する保険請求資料、 又は保険契約の加入に使用される健康、病気、怪我に関する資料
- 健康診断資料、健康診断結果情報
- 医師の診断による健康状態についての情報、医療機器により測定された健康状態についての情報、又は保険請求記録もしくはアルゴリズム又は他の推論によって把握又は推論される健康状態についての情報
- 健康状態又は習慣を把握するための機器を通じて収集される情報（歩数、心拍数、酸素飽和率、血糖値、血圧値、心電図等）
- 一般的に健康情報とみなされないが、病気の診断、治療、予防、管理に用いられるその他の情報（音声記録等）

これらのリストはあくまで例であり、すべてを網羅するものではない。

(ii)　事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

事業者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。PIPA 第 23 条第 1 項によれば、個人の健康に関する情報が「センシティブ情報」に該当する。健康に関する情報は、その情報を誰が作成又は入手したかによって、特に区別されていない。従って、個人の健康に関する情報であれば、PIPA の「センシティブ情報」に該当すると考えられる。

(iii)　消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）

消費者が市販の検査機器を利用して行った検査結果（医師等の判断を介していない検査結果）は、センシティブデータに該当する。PIPA 第 23 条第 1 項によれば、個人の健康に関する情報が「センシティブ情報」に該当する。健康に関する情報は、その情報を誰が作成又は入手したかによって、特に区別されていない。従って、個人の健康に関する情報であれば、PIPA の「センシティブ情報」に該当すると考えられる。

(iv)　消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態

消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態はセンシティブデータに該当する。PIPA 第 23 条第 1 項によれば、個人の健康に関する情報が「センシティブ情報」に該当する。健康に関する情報は、その情報を誰が作成又は入手したかによって、特に区別されていない。従って、個人の健康に関する情報であれば、PIPA の「センシティブ情報」に該当すると考えられる。例えば、家族の病歴、喫煙の有無、妊娠の有無及びその可能性、服薬の有無、健康状態などの健康情報などは、医師等の判断や市販の検査機器を解することがなくとも、健康に関する情報に該当すると考えられ、センシティブデータに該当する。

(v)　予防接種の接種有無（予防接種の接種者如何により、センシティブデータ該当性に差異はあるか）

予防接種の接種有無がセンシティブデータに該当するかは、条件による。

予防接種に関する情報、接種日、副反応及びその発生日などの情報は、健康に関する情報として、センシティブ情報に該当すると考えられうるため、センシティブデータに該当する可能性がある。

韓国政府は、予防接種に関する情報が PIPA 第 23 条の「センシティブ情報」に該当するかどうかについて、公式見解を示していない。しかし、一定の予防接種に関する情報は、上記の「保健医療情報利用ガイドライン（2020 年 9 月）」に規定されているもののうち、「一般的に健康情報とみなされないが、病気の診断、治療、予防、管理に用いられるその他の情報（音声記録等）」に該当する可能性がある。PIPC は、「予防接種情報の収集がセンシティブ情報の処理に該当するか否かの質問」に対する回答として、「企業が従業員に予防接種休暇を与えるために予防接種情報を含む個人データを収集する場合は、一般の個人データの収集・処理手順に従って当該情報を収集する必要がある。ただし、場合によっては予防接種情報が個人の健康状態に影響を与える情報でありえ、その場合の予防接種情報は、センシティブ情報に該当しうるものと考えられる」と説明した（2021 KISA REPORT volume 09, 07「Covid-19 の予防接種情報は特別な保護が必要な個人情報か？- センシティブ情報の意味を考えるために」（Is Covid-19 vaccination information personal data which requires special protection? – To think about the meaning of sensitive information））。

(2)　趣旨

健康に関するデータの処理の過程で、個人のプライベート及び秘密の領域まで侵害される可能性があるためと考えられる。

(3)　追加的規律（該当する場合）

医療法[140]では、医療機関が医療法に基づいて収集したセンシティブ情報は、その処理が法律上必要とされ又は許容されるため、別途の同意なしに処理できるものとされている（PIPA 第 23 条第 1 項第 2 号、医療法第 21 条第 3 項）。

[140] 医療法
（https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9

健康及び医療サービスに関するフレームワーク法[141]では、健康・医療記録へのアクセスを要求できるものとされている（健康及び医療サービスに関するフレームワーク法第 11 条）。要求できるのは原則として本人であるが、本人が請求できない場合には、配偶者、直系尊属、直系卑属、配偶者の直系尊属が、これらの者に該当する者がいない場合には本人が指定した代理人が、本人のために請求することができる。

2. 遺伝子に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

遺伝子に関するデータは、遺伝子検査などから得られる DNA 情報であれば、センシティブデータに該当する（PIPA 第 23 条第 1 項）。

(i) 医師等が行った遺伝子検査の検査結果

医師等が行った遺伝子検査の検査結果は、センシティブデータに該当する。PIPA 第 23 条第 1 項は、遺伝子検査などから得られる DNA 情報がセンシティブ情報に該当することを規定しており、医師等が行った遺伝子検査の検査結果はこれに該当すると解される。

(ii) 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果（医師等の判断を介していない検査結果）

消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果は、センシティブデータに該当する。PIPA 第 23 条第 1 項は、遺伝子検査などから得られる DNA 情報がセンシティブ情報に該当することを規定しており、遺伝子検査キットを利用して行った遺伝子検査の検査結果はこれに該当すると解される。

(iii) 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報

消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報は、遺伝子検査などから得られる DNA 情報としてはセンシティブデータに該当しない。ただし、健康に関するデータとしてセンシティブデータに該当する可能性が高い。

上記 II. 1 への回答で詳述したとおり、個人情報保護法は、センシティブ情報に分類される「遺伝子検査などから得られる DNA 情報」を定義していないが、同じ語を用いている生命倫理安全法（第 2 条第 11 項、第 2 条第 14 項、第 2 条第 15 項）では、「遺伝子検査により得られた DNA 情報」とは、「個人の遺伝的特徴に関する情報であって、当該個人のヒト材料（人体から採取され、若しくは収集された組織、細胞、血液及び体液を含むヒト構成物、又は血清、血漿、染色体、DNA（Deoxyribonucleic Acid）、RNA（Ribonucleic Acid）及びタンパク質等から分離したもの）により分析することにより得られるもの」をいうとされ、センシティブ情報の該当性判断においても、同様の定義が用いられると解される。かかる解釈に従えば、本設問の想定する情報はかかる遺伝子検査などから得られる DNA 情報の定義には該当しないと考えられるためである。

C%EC%9D%B8%EC%A0%95%EB%B3%B4+%EB%B3%B4%ED%98%B8%EB%B2%95#J21:0、https://elaw.klri.re.kr/kor_service/lawView.do?hseq=60889&lang=ENG（英訳））

[141] 健康及び医療サービスに関するフレームワーク法（https://www.law.go.kr/LSW/LsiJoLinkP.do?lsNm=%EB%B3%B4%EA%B1%B4%EC%9D%98%EB%A3%8C%EA%B8%B0%EB%B3%B8%EB%B2%95&paras=1&docType=JO&languageType=KO&joNo=001100000、（https://elaw.klri.re.kr/kor_service/lawView.do?hseq=54790&lang=ENG（英訳））

ただし、本設問の想定する情報は健康に関する情報に該当する可能性があり（上記 III. 1(iv)参照）、センシティブ情報に該当すると判断される可能性があると考えられる。

(2) 趣旨

遺伝子に関するデータの処理の過程で、個人のプライベート及び秘密の領域まで侵害される可能性があるためと考えられる。

(3) 追加的規律（該当する場合）

生命倫理安全法[142]では、次のような定めが存在する。

- 遺伝情報に基づく差別の禁止（生命倫理安全法第 46 条）
- 遺伝情報を本人の同意なく研究者に提供する場合の個人情報の匿名化（遺伝情報を提供する者に課される義務）（生命倫理安全法第 38 条第 2 項及び第 43 条第 2 項）。
- 遺伝情報の匿名化及び個人情報の保護に関するガイドラインの作成義務（遺伝情報を受領する一定の機関に課される義務）（生命倫理安全法第 44 条第 2 項及び第 4 項）等。

3. 性生活・性的指向に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

性生活・性的指向に関するデータは、センシティブデータに該当する。PIPA 第 23 条第 1 項は、性生活等に関する情報がセンシティブデータに該当することを規定している。

(2) 趣旨

性生活・性的指向に関するデータを処理する過程で、個人のプライベート及び秘密の領域まで侵害される可能性があるためと考えられる。

(3) 追加的規律（該当する場合）

特に見当たらない。

4. 労働組合への加入に関するデータ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

労働組合への加入に関するデータは、センシティブデータに該当する。PIPA 第 23 条第 1 項は、労働組合への加入に関する情報がセンシティブデータに該当することを規定している（上記 II. 1 参照）。

[142] 生命倫理安全法
（https://www.law.go.kr/LSW/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%83%9D%EB%AA%85%EC%9C%A4%EB%A6%AC%EB%B2%95#undefined）

(2) 趣旨

特定の労働組合又は政党への加入又は脱退に関する情報は、社会的差別を引き起こす可能性があるためと考えられる。

(3) 追加的規律（該当する場合）

特に見当たらない。

5. 自然人を一意に識別することを目的とする生体データ

(1) センシティブデータへの該当性　どこまでのデータが該当するか

自然人を一意に識別することを目的とする生体データは、センシティブデータに該当する。PIPA 第 23 条第 1 項は、個人の識別を目的とした個人の身体、生理又は行動の特徴に関する情報の特定の技術処理の結果得られた情報がセンシティブデータに該当することを規定している（上記 II. 1 参照）。

(2) 趣旨

生体情報は、個人を識別するために利用される。また、生体情報は、他の個人情報と異なり、生存中の個人と関連づけられ、氏名、住所、識別番号又はパスワードと異なり、変更できない。したがって、生体情報の漏えいは回復不能な損害をもたらす可能性が高く、別途規制する必要性が考慮されたためと考えられる[143]。

(3) 追加的規律（該当する場合）

特に見当たらない。

6. 金融口座番号、クレジットカード番号等（金融・財産に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

金融・財産に関するデータは、センシティブデータに該当しない。

(2) 趣旨

該当なし。

[143] Il-Hwan Kim, the Study on the Improvement of Legislation for the Protection and Use of the Biometric Information, European Constitution Study Vol. 20, Aug. 2019（출처: 생체인식정보의 보호와 이용에 관한 법제정비방안에 관한 연구, 김일환, 유럽헌법연구 제 30 호, 2019. 8.）

(3) 追加的規律（該当する場合）

特に見当たらない。

7. クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ）

(1) センシティブデータへの該当性　どこまでのデータが該当するか

信用に関するデータは、センシティブデータに該当しない。

(2) 趣旨

該当なし。

(3) 追加的規律（該当する場合）

信用情報の利用及び保護に関する法律[144]では、信用情報会社などによる信用情報の収集・加工に関する原則を定めている（信用情報の利用及び保護に関する法律第 15 条）。

8. 政府等の金銭的保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

政府等の金銭的保護を受けている事実に関する情報は、センシティブデータに該当しない。

(2) 趣旨

該当なし。

(3) 追加的規律（該当する場合）

特に見当たらない。

9. 成年後見制度の保護を受けている事実に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

成年後見制度の保護を受けている事実に関する情報は、センシティブデータに該当する可能性がある。

[144] 信用情報の利用及び保護に関する法律（https://www.law.go.kr/LSW/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%8B%A0%EC%9A%A9%EC%A0%95%EB%B3%B4#undefined（原文）、https://elaw.klri.re.kr/kor_service/lawView.do?hseq=49486&lang=ENG（英訳））

当該情報自体がセンシティブ情報に該当するかどうかは PIPA 上規定されていない。したがって、成年後見制度の保護を受けている事実又はこれに準ずる保護を受けている事実に関する情報は、「センシティブ情報」に該当する類型の他の情報を含まなければ、センシティブ情報には該当しない。例えば、かかる情報が健康に関する情報を含んでいる場合であれば、PIPA の「センシティブ情報」に該当すると解される。

(2) 趣旨

該当なし。

(3) 追加的規律（該当する場合）

特に見当たらない。

10. 児童に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

児童に関する情報は、センシティブデータに該当しない。

(2) 趣旨

該当なし。

(3) 追加的規律（該当する場合）

PIPA は、14 歳未満の児童の個人情報の収集、利用又は提供について、当該児童の法定代理人の同意を得る義務（PIPA 第 22 条第 6 項、第 39 条の 3 第 4 項）、当該法定代理人が閲覧・アクセスなどを求める権利（PIPA 第 38 条）、個人情報の処理に関する事項を通知するにあたり理解可能な様式でわかりやすい文言を用いる義務などを定めている（PIPA 第 39 条の 3 第 5 項）。

位置情報の保護及び利用に関する法律[145]では、14 歳未満の児童の位置情報の収集、利用又は提供について、その法定代理人の同意を得る義務が定められている（位置情報の保護及び利用に関する法律第 25 条）。

11. オンライン行動履歴に関する情報

(1) センシティブデータへの該当性　どこまでのデータが該当するか

オンライン行動履歴に関する情報は、センシティブデータに該当しない。

[145] 位置情報の保護及び利用に関する法律（https://www.law.go.kr/LSW/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%9C%84%EC%B9%98%EC%A0%95%EB%B3%B4#undefined、英訳（https://elaw.klri.re.kr/kor_service/lawView.do?hseq=55914&lang=ENG））

(2) 趣旨

該当なし。

(3) 追加的規律（該当する場合）

特に見当たらない。

## IV. センシティブデータの取扱いに適用される規律

### 1. 取得

PIPA 及び施行令の通常の個人情報の処理の規律に加えて、センシティブデータの処理は別途の個別規定により、より厳格に制限される。この点については以下の設問 V. 1 への回答を参照。

### 2. 利用

上記 IV. 1 参照。

### 3. 第三者提供

上記 IV. 1 参照。

### 4. 管理

管理について、について、センシティブデータの取扱いに適用される追加的な規律は本調査の限りでは特に見当たらない。

### 5. 漏えい等

漏えい等について、センシティブデータの取扱いに適用される追加的な規律は本調査の限りでは特に見当たらない。

## V. 本人同意、プロファイリング

### 1. 本人同意

(1) センシティブデータ規制（上記III）との関係

原則として、PIPA 第 23 条は「センシティブ情報」の処理を、PIPA 第 24 条は「個人識別情報」の処理を、それぞれ禁止している。ただし、（i）別途データ主体の同意がある場合、又は（ii）適用法令により処理が要求又は許可されている場合には、処理を行うことができる（PIPA 第 23 条及び第 24 条がそれぞれその旨を定めている）。なお、住民登録番号（resident registration number）については、PIPA 第 24

条の 2 第 1 項各号のいずれかに該当する場合（住民登録番号の処理が法律上特に要求又は許可されている場合など）を除き、処理できないと定められている（同条第 2 項各号）。

(2) 要件一般

「センシティブ情報」及び「個人識別情報」の処理に対する同意は、他の個人情報の処理への同意とは別に取得しなければならないとされている（PIPA 第 23 条第 1 項第 1 号及び第 24 条第 1 項第 1 号）。

(3) 情報提供

一般的な個人情報の処理に関する同意を得る際と同様に、「センシティブ情報」及び「個人識別情報」の処理に関する同意を得る際には以下の情報をデータ主体に提供する必要がある。

- 収集/利用の場合。個人情報の収集/利用目的、収集される具体的な個人情報、保有及び利用期間、データ主体の同意の拒否権、及び（もしあれば）同意の拒否による不利益（PIPA 第 23 条第 1 項第 1 号、第 24 条第 1 項第 1 号、第 15 条第 2 項）。
- 第三者への提供の場合。個人情報の受領者、個人情報の受領者の利用目的、提供される特定の個人情報、受領者の個人情報の保有及び利用期間、データ主体の同意の拒否権及び（もしあれば）同意の拒否による不利益（PIPA 第 23 条第 1 項第 1 号、第 24 条第 1 項第 1 号、第 17 条第 2 項）。

(4) 形式

施行令において、データ主体の同意をどのように取得すべきかが具体的に規定されている（PIPA 第 22 条第 7 項及び施行令第 17 条第 1 項各号）。なお、データ主体の同意を書面で取得する必要はないが、書面で得る場合には、住民登録番号以外の「センシティブ情報」及び「個人識別情報」を含め、施行令第 17 条第 2 項に規定された事項を個人情報の処理方法に関する告示[146]第 4 条に規定された方法で分かりやすく表示することが求められている（PIPA 第 22 条第 2 項、施行令第 17 条第 2 項、個人情報の処理方法に関する告示第 4 条）。

また、施行令第 17 条第 1 項が同意を取得するにあたっての要求している様式が書面等の明確な方法であることからすると、原則として、同意はデータ主体の明示的な同意である必要があると解される。ただし、社会的規範に照らしてデータ主体が同意の意思を有していたと解釈される場合には、データ対象者の黙示的な同意をもって明示的な同意に代えられる場合がある。

個人情報管理者は、データ主体から直接名刺その他これに類する媒体（以下、「名刺など」という）の交付を受けてデータ主体の個人情報を取得する場合には、名刺などの交付の状況からみて、社会通念上データ主体に同意の意思があったと認められる範囲内で利用できる（個人情報保護標準ガイドライン第 6 条第 3 項）。

オンラインのウェブサイトなどの公的な媒体又は公共の場所において個人情報を収集する場合、データ主体による同意の意思が明示されている又はウェブサイトなどの表示内容に照らしてデータ主体が社会通念上同意の意思を有していると認められる範囲内において、個人情報管理者は当該個人情報を利用できる（個人情報保護標準ガイドライン第 6 条第 4 項）。

[146] 個人情報の処理方法に関する告示
（https://law.go.kr/admRulSc.do?menuId=5&subMenuId=41&tabMenuId=183&query=%ED%91%9C%EC%A4%80%20%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%20%EB%B3%B4%ED%98%B8%EC%A7%80%EC%B9%A8#liBgcolor0）

なお、韓国実務上、データ主体や第三者が「既に開示した個人情報」（例えば、中古品取引のウェブサイトにおいて品物とともに開示した自らの電話番号などがこれに当たる。PIPC 解説書 83 頁）という類型が認識されているところ、この「すでに開示した個人情報」の処理について、最高裁判所は、データ主体が自己の個人情報の処理に同意していることが客観的に認められる範囲内において、データ主体の黙示の同意があったものといえ、さらなる個別の同意は不要と解するのが相当であるとしている（最高裁判所 2016 年 8 月 17 日判決 2014 ダ 235080 号）。

(5) 個別同意の必要性

個人情報管理者がデータ主体の同意を得ようとする場合、個人情報管理者は同意を必要とする事項ごとに、データ主体が同意を求められている対象を明確に認識できる方法でデータ主体に同意を求め、事項毎に個別の同意を得なければならない（PIPA 第 22 条第 1 項）。

事項毎の同意としては、個人情報の収集/利用、第三者への提供、国外にある第三者への提供、マーケティング目的の個人情報の処理への同意、及び法定代理人の同意が含まれる。

(6) 同意撤回

データ主体は、個人情報管理者に対して自己の個人情報の処理の停止を求める権利を有し（PIPA 第 37 条）、特に情報通信ネットワークの利用促進及び情報保護に関する法律[147]第 2 条第 1 項第 3 号に基づく情報通信サービス提供者による個人情報の処理の場合、データ主体は当該サービス提供者に与えられた個人情報の収集、利用、提供などに関する同意を撤回する権利を有する（PIPA 第 39 条の 7）。

処理の停止を求める権利は、個人情報の処理活動の全面的な停止を要求する権利を指し、同意を撤回する権利よりも範囲が広く認められている（PIPC 解説書 381 頁）。

データ主体は、同意を撤回する権利の行使により、自分が同意した事項について同意を撤回できる。一方、処理の停止を求める権利については、その行使により、データ主体が個人情報の処理に同意したか否かにかかわらず、個人情報管理者によるすべての個人情報の処理の停止を要求できる。

(7) その他留意事項

該当なし。

2. プロファイリング

(1) プロファイリング・データ分析に適用される規律

PIPA は、プロファイリング及び自動的な意思決定に関する事項については規定していない。

もっとも、同法は「インターネットアクセスデータファイルを含む個人情報の自動収集ツールの設置及び運用並びにその拒否に関する事項」がある場合、当該事項を含む個人情報処理方針を策定・公開しなければならないとする（PIPA 第 30 条第 1 項第 7 号）。

上記規定はプロファイリングそのものに関するものではないが、プロファイリングを可能にする手段を規制していることから、このような規定は間接的にプロファイリングと関連しているといえよう。また、

[147] 情報通信ネットワークの利用促進及び情報保護に関する法律（https://www.law.go.kr/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4+%EB%B3%B4%ED%98%B8%EB%B2%95#undefined、英訳（https://elaw.klri.re.kr/kor_service/lawView.do?hseq=55570&lang=ENG））

信用情報の利用及び保護に関する法律[148]は、信用情報に関わる自動評価に関する事項を規定している。

なお、現在プロファイリングを規制しようとする試みがなされており、様々な関連法案が国会に提出されている。

(2) プロファイリング・データ分析により生成されたデータが、センシティブデータに該当しうるか

プロファイリングなどによって生成されたデータが PIPA 第 23 条第 1 項及び施行令第 18 条に規定された「センシティブ情報」に該当する場合には、センシティブデータに該当すると考えられる。

(3) プロファイリング・データ分析によりセンシティブデータを生成した場合、いかなる規律が適用されるか

PIPA のセンシティブ情報の処理に関する規定が適用される。

## VI. センシティブデータの取扱いに係る裁判例・決定等

ツイッター上の情報が PIPA の「センシティブ情報」に該当するかどうかが争われた事案がある（ソウル中央地判 2014 年 9 月 11 日 2013 ゴハップ 577・1060（合）号）。当該事案では、次のような判断が裁判所により示されている。

- ツイッター上の情報には、ツイッターのユーザーがツイッターのメッセージを通じて表明した思想、信条、政治的意見などが含まれる可能性がある。
- しかし、データ主体が自らの意思で既にツイッターを通じて自分のツイッターのメッセージの内容を公開している限り、当該内容が個人情報保護法上のセンシティブ情報に該当すると結論づけるのは不合理である。

その理由として、PIPA が本人の同意なしに「センシティブ情報」の取り扱いを制限する目的は、憲法が保護する権利であるプライバシーと良心の自由の侵害を防止するためであるところ、今回のケースでは、ツイッターの情報は本人が自発的に開示したものであり、PIPA の趣旨に照らして「センシティブ情報」とはいえないとしたものと解される。加えて、裁判所は、ツイッターに投稿された情報が、本来的に「センシティブ情報」となる遺伝に関する情報や犯罪記録に関する情報とは性質が異なると判断した。

この地方裁判所の判決は高等裁判所及び最高裁判所に上訴されたが、いずれにおいても、上記のツイッターにおける投稿は「センシティブ情報」に該当しないことを前提として判断が下されており、上記部分の判断は確定したものと解される。

## VII. その他（上記の他、センシティブデータの取扱いに適用される規律）

該当なし。

[148] 信用情報の利用及び保護に関する法律（https://www.law.go.kr/LSW/lsSc.do?section=&menuId=1&subMenuId=15&tabMenuId=81&eventGubun=060101&query=%EC%8B%A0%EC%9A%A9%EC%A0%95%EB%B3%B4#undefined、英訳（https://elaw.klri.re.kr/kor_service/lawView.do?hseq=49486&lang=ENG））

## 第10章.　別紙 - 比較表

センシティブデータへの該当性を検討した具体的なデータの例についてまとめると以下のとおりである。なお、この別表は参照の便宜のために概括的に該当性の評価をまとめて記載するものであり、具体的な該当性やその可能性については報告書本文を参照されたい。

凡例

| | |
|---|---|
| | 定義上、該当する又は該当する可能性がある |
| | 定義上、一定の条件において、該当する又は該当する可能性がある |
| | 定義上、該当しない又は該当する可能性が低い |

| No. | データの種類 | EU | ADPPA | CCPA | 中国 | インド | ブラジル | オーストラリア | 韓国 |
|---|---|---|---|---|---|---|---|---|---|
| 1 (i) | 医師等が行った検査結果 | | | | | | | | |
| 1 (ii) | 事業者が市販の検査機器を利用して行った検査結果 | | | | | | | | |
| 1 (iii) | 消費者が市販の検査機器を利用して行った検査結果 | | | | | | | | |
| 1 (iv) | 消費者が医師等の判断及び市販の検査機器を介することなく自ら判断した健康状態 | | | | | | | | |

| No. | データの種類 | EU | ADPPA | CCPA | 中国 | インド | ブラジル | オーストラリア | 韓国 |
|---|---|---|---|---|---|---|---|---|---|
| 1 (v) | 予防接種の接種有無 | | | | | | | | |
| 2 (i) | 医師等が行った遺伝子検査の検査結果 | | | | | | | | |
| 2 (ii) | 消費者が市販の遺伝子検査キットを利用して行った遺伝子検査の検査結果 | | | | | | | | |
| 2 (iii) | 消費者が医師等の判断及び市販の遺伝子検査キットを介することなく自ら判断した遺伝に関する情報 | | | | | | | | |
| 3 | 性生活・性的指向に関するデータ | | | | | | | | |
| 4 | 労働組合への加入に関するデータ | | | | | | | | |
| 5 | 自然人を一意に識別することを目的とする生体データ | | | | | | | | |
| 6 | 金融口座番号、クレジットカード番号等（金融・財産に関するデータ） | | | | | | | | |
| 7 | クレジットやローン等の取引情報、破産手続等に関する情報等（信用に関するデータ） | | | | | | | | |
| 8 | 政府等の金銭的保護を受けている事実に関する情報 | | | | | | | | |

| No. | データの種類 | EU | ADPPA | CCPA | 中国 | インド | ブラジル | オーストラリア | 韓国 |
|---|---|---|---|---|---|---|---|---|---|
| 9 | 成年後見制度の保護を受けている事実に関する情報 | | | | | | | | |
| 10 | 児童に関する情報 | | | | | | | | |
| 11 | オンライン行動履歴に関する情報 | | | | | | | | |