スイス連邦データ保護法改正案の内容および EU「一般データ保護規則」との比較

2018 年 3 月

日本貿易振興機構（ジェトロ）
ジュネーブ事務所
海外調査部　欧州ロシア CIS 課

欧州経済領域（European Economic Area：EEA、EU 加盟国 28 カ国、ノルウェー、アイスランド、リヒテンシュタイン）においては、欧州連合（European Union）（以下「EU」という。）の「一般データ保護規則（General Data Protection Regulation：GDPR）」の 2018 年 5 月 25 日適用開始に向けた準備が進められているが、スイスは同規則の適用地域ではない。スイスにおいては現在、スイス連邦の連邦データ保護法（Federal Act on Data Protection）（以下「FADP」という。）を改正し、GDPR の内容を踏まえた新しい連邦データ保護法（Federal Data Protection Act）（以下「FDPA」という。）を成立させる手続きが進んでいる。

本レポートは、同規則に詳しいギブソン・ダン・クラッチャー法律事務所ブリュッセルオフィスに作成を委託し、スイスの法律事務所である Walder Wyss Ltd.からのスイス法に関する法的助言に基づき、GDPR の内容とスイス連邦の新しい連邦データ保護法（Federal Data Protection Act）の法案（以下「FDPA 法案」という。）の内容（2018 年 1 月 8 日時点の情報）とを比較し、まとめた。欧州ビジネスにおいて、スイスにおける個人データを取り扱う企業の対応検討に役立てば幸いである。

【免責条項】

本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用ください。

ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承ください。 禁無断転載

Copyright (C) 2018 JETRO. All rights reserved

目次

Copyright (C) 2018 JETRO. All rights reserved

1. FDPA と GDPR の相違点

「一般データ保護規則（GDPR）」は、EU における個人情報（データ）の処理および EU からの個人データの移転を規制するために EU の立法機関によって採択された規則である。その適用対象は、EU の 28 加盟国に、ノルウェー、アイスランドおよびリヒテンシュタインを加えた欧州経済領域（European Economic Area）（以下「EEA」という。）である。すなわち、GDPR は、EEA に関する規則であり、各加盟国に直接適用される。

スイスは、EU 加盟国に囲まれているものの、EU あるいは EEA の加盟国ではない。したがって、スイスは、GDPR の適用対象外であり、スイスにおける会社および組織は個人データの処理に関する GDPR の規制に直ちに拘束されるものではない。

もっとも、GDPR は、第 3 条第 2 項に基づく域外適用の規定によって、スイスの会社および組織に適用される場合がある。

民間部門による個人データの処理は、連邦データ保護法（Federal Act on Data Protection）（以下「FADP」という。）および連邦データ保護令（Federal Data Protection Ordinance）（以下「FDPO」という。）による規律を受ける。規制対象となる特定の市場におけるその他の法律の多くの規定も、民間部門による個人データの処理に関するルールを設けている。

現行の FADP については、新しい連邦データ保護法（Federal Data Protection Act）の法案（以下「FDPA 法案」という。）に基づいて、現在改正作業が行われている。本章では、FDPA 法案と GDPR を比較し、全体的な相違点を解説する。

（１）FDPA の運用体制、GDPR との主な相違点

FDPA 法案は、スイスで設立される会社および組織に対して直接的に適用されるルールを規定する。FDPA 法案に規定されるルールの実際の運用は、同法案で規定される義務にかかる特定の要件を規定する複数の法令によって実施されるものと考えられる。

一方、EEA 内においては、GDPR が EEA 内の個人データの処理に関して優位性のある規制となる。その運用は、EU および EEA 加盟国において採択される法律（例えば、未成年者の同意に関する分野）、欧州委員会によって採択される法規制（例えば、データ保護に関する認証メカニズムのための要件の設定）、欧州データ保護会議（European Data Protection Board）により採択される決定（意見、紛争解決に関する決定等）などを含む様々な方法に則って実施されることになる。

① 法的枠組

FDPA 法案は、2017 年 9 月 15 日、スイスの連邦参事会（Federal Council）によってスイスの公用語である以下の言語で公表された。

Copyright (C) 2018 JETRO. All rights reserved

- フランス語：https://www.ejpd.admin.ch/ejpd/fr/home/aktuell/news/2017/2017-09-150.html
- ドイツ語：https://www.ejpd.admin.ch/ejpd/de/home/aktuell/news/2017/2017-09-150.html
- イタリア語：https://www.ejpd.admin.ch/ejpd/it/home/aktuell/news/2017/2017-09-150.html

FDPA 法案の非公式な英語版も、以下のウェブサイトで閲覧可能である：
https://www.dataprotection.ch/fileadmin/dataprotection.ch/user_upload/redaktion/Docs/Swiss_Data_Protection_Act__draft_of_September_2017__Walder_Wyss_convenience_translation_V010.pdf?v=1507206202 （スイスの法律事務所 Walder Wyss Ltd. ウェブサイト）

FDPA 法案が最終的に採択されるまでの間、現行の FADP（1992 年 6 月 19 日）が適用される。連邦参事会は、2018 年 8 月に FDPA 法案を成立させることを暫定的な目標としている（下記 6 参照）。

他方で、GDPR は、2016 年 5 月 4 日、EU の官報において公表されており、以下のウェブサイトにおいて閲覧可能である：http://eur-lex.europa.eu/eli/reg/2016/679/oj

GDPR は、2018 年 5 月 25 日から適用開始となる。

② 監督当局

FDPA 法案は、連邦データ保護情報コミッショナー（Federal Data Protection and Information Commissioner）（以下「コミッショナー」という。）をスイス連邦の監督当局に指定する。

コミッショナーは、FDPA 法案において、一定の場合に、拘束力のある決定を行うことができる（現在、コミッショナーの勧告および見解は法的拘束力を有しない）。もっとも、コミッショナーは、現行法および FDPA 法案のいずれにおいても、制裁金を課す権限を有しない。スイスにおいては、当該権限は刑事裁判官に委ねられる。

GDPR とは異なり、FADP は、行政上の制裁ではなく個人の刑事責任を規定する。これらの異なったアプローチは、法改正後に相互に向き合うことになる。FDPA 法案第 54 条および第 55 条に基づいて、コミッショナーではなく刑事裁判官が個人による苦情申立を受け、特定のデータ保護に関する義務の意図的な違反に対して最大で 25 万スイスフランの罰金を科すことができる。一定の場合において、罰金が 5 万スイスフランを超えないときは、裁判官は対象となる個人の起訴を猶予し、かわりに法人に対して罰金の支払を命じることができる。コミッショナーに関するウェブサイトは、以下で閲覧可能である（https://www.edoeb.admin.ch/edoeb/en/home/the-fdpic/task.html. ）。ウェブサイト上で必要な情報を確認できない場合には、コミッショナーに対して電子メール（info@edoeb.admin.ch）または相談サービス窓口（+41 (0)58 462 43 95）を通じて問い合わせることができる。但し、コミッショナーは FDPA 違反事案を調査する立場でもあるため、コミッショナーに対して問い合わせを行ったことが引き金となって執行が行われる可能性があることを認識する必要がある。

Copyright (C) 2018 JETRO. All rights reserved

これに対して、GDPR においては、監督および執行に関する権限は、EEA 加盟国における監督当局に委ねられている。調査に関する決議または決定の採択について複数の加盟国の監督当局間で異なる状況が生じた場合には、欧州データ保護会議（EDPB）[1]が当該問題に関する最終的な決定を採択する権限を有する。

（2）内容面における主な相違点

FDPA 法案と GDPR の内容面での主な相違点は、以下の通りである。

① 適用範囲

FDPA 法案は、スイスで設立されるすべての会社および組織に対して適用される。また、スイスの国際私法に関する法律（第 139 条第 1 項および第 3 項）によれば、データ主体は、以下の場合において、外国の会社および組織に対して現行の FADP および FDPO の適用を選択することができる。

- データ主体がスイスに通常居住している場合（管理者または処理者がスイスにおいて損害が発生する可能性を予見できる場合に限る）、
- 管理者または処理者がスイスに通常居住しているかまたは登録された事務所を有する場合、または
- データ処理から生じる損害がスイスにおいて発生する場合（管理者または処理者がスイスにおいて損害が発生する可能性を予見できる場合に限る）

本規定（スイスの国際私法に関する法律第 139 条第 1 項および第 3 項）は FDPA 法案により廃止または影響を受けるものとされていないことから、FDPA 法案が成立した場合においても適用が継続するものと考えられる。

他方で、GDPR は、以下のいずれかが満たされる場合に、個人データの処理について適用される（第 3 条）。

- GDPR は EEA 内の管理者または処理者の事業所の活動に関連してなされる個人データの処理に適用される（この場合、その処理が EEA 内または EEA 外でなされるか否かについては問わない）。
- GDPR は EEA 内に拠点のない管理者または処理者による EEA 内に所在するデータ主体の個人データの処理に適用される。ただし、処理活動が以下に記載する事項に関連しているものに限られる。

[1] 現行のデータ保護指令に基づく第 29 条作業部会（加盟各国の監督機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関（EDPS）の代表によって構成され、特定の問題に関して共通の解釈と分析を提供することにより、EU 加盟国のデータ保護法の解釈にある程度の調和をもたらす）の後継組織。

Copyright (C) 2018 JETRO. All rights reserved

- EEA 内に所在するデータ主体に対する商品又はサービスの提供に関する処理（データ主体に支払が要求されるか否かについては問わない）
- EEA 内で行われるデータ主体の行動の監視に関する処理

結論として、FDPA 法案およびスイスの法制度と GDPR の間においては、地理的適用範囲について相違点が存在する。特に、外国で設立された会社および組織による個人データの処理については、双方の法制度により規定されたルールの相違点は以下の通りである。

- スイスの国際私法は、以下の通り、処理行為の効果を判断基準とする：管理者または処理者がスイスにおける損害の発生を予見できたか。
- GDPR は、以下の通り、処理行為の目的を判断基準とする：データ処理行為が EEA における商品もしくはサービスの提供または EEA 内におけるデータ主体の行動の監視に関連するか。

もっとも、実務上は、これらのルールは同様の帰結を導くものと考えられる。すなわち、スイスまたは EEA 内のデータ主体の個人データの処理が生じることを合理的に予見可能な会社および組織は、FDPA 法案または GDPR の適用を受ける可能性がある。

②「個人データ」および「センシティブな個人データ」の定義

a. 個人データ

FADP の個人データの定義は FDPA 法案において大きく修正されている。FDPA 法案第 4 条第(a)号は、個人データについて、「識別されたまたは識別され得る自然人に関するすべての情報」であると定義する。他方、現行の FADP においては法人に関するデータも個人データに含まれる。

この定義は GDPR の定義と比較すると簡潔な内容であるが、GDPR 第 4 条第 1 号における「識別されたまたは識別され得る自然人（「データ主体」）に関するすべての情報」という個人データの定義の重要部分を捉えている。また、GDPR では、「識別し得る自然人とは、自然人の氏名、識別番号、位置データ、オンライン識別子、または物理的、生理学的、遺伝的、精神的、経済的、文化的または社会的なアイデンティティに関する特有の一つまたは複数の要素を参照することによって、直接的または間接的に識別し得る者」という明確化のための規定を設けている。

実務上は、FDPA 法案および GDPR における個人データの定義に関して違いはないと考えられる。

b. センシティブな個人データ

FDPA 法案第 4 条第(b)号は、センシティブな個人データについて、以下のカテゴリーの個人データを含むものとして定義する。

- 宗教的、思想的、政治的または労働組合に関連する見解または活動に関するデータ
- 健康、親密な関係性（intimate sphere）、人種的または民族的素性に関するデータ
- 遺伝子データ

Copyright (C) 2018 JETRO. All rights reserved

- 自然人を明確に識別する生体データ
- 行政上または刑事上の手続および制裁に関するデータ
- 社会保障対策に関するデータ

これに対して、GDPR 第 9 条は、特別カテゴリーの個人データを以下のように定義する：「人種的素性もしくは民族的素性、政治的思想、宗教的もしくは哲学的信条、または労働組合員資格に関する個人データ、および遺伝データ、自然人の一意な識別を目的とした生体データ、健康データまたは自然人の性生活もしくは性的指向に関するデータ」。

有罪判決および犯罪に関する個人データの処理については、GDPR 第 10 条に基づく特別な措置が必要となる。

結論として、FDPA 法案のセンシティブな個人データの定義は、以下のように、GDPR における特別カテゴリーの個人データよりも広いカテゴリーを含む概念である。

- 「親密な関係性」に関する個人データとは、GDPR で規定される「性生活または性的志向」よりも広範な情報を含むものである。すなわち、FDPA 法案においては、個人にとって心情的に非常に重要なデータであり、当該個人が選ばれた少数の者に対してのみ知らせたデータ（例えば、恐怖、夢、セラピー等）が含まれる。
- 自然人を明確に識別する生体データ（例えば、写真）（GDPR は、一意に自然人を識別することを目的とする生体データのみを対象とする）
- 行政上または刑事上の手続および制裁に関するデータ（GDPR は刑事記録に関するデータについて特別な措置を規定するとしても、行政上手続および制裁はセンシティブな個人データに含まれない）
- 社会保障対策に関する措置（GDPR は、この類型のデータがセンシティブな個人データに該当するとは考えていない）

③ データ主体の同意

同意は、FDPA 法案および GDPR の双方において個人データの処理（FDPA 法案第 27 条および GDPR 第 6 条）および域外移転（FDPA 法案第 14 条および GDPR 第 49 条）のための法的根拠として承認されている。但し後述（２.）の通り、GDPR とは異なり、FDPA 法案は、個人データの処理に関して法的根拠が常に必要であるとは規定していない。

FDPA 法案は、同意について非常に簡潔な規定を設けている。第 5 条第 6 項によれば、データ主体の同意が必要な場合には、同意が十分な情報が提供された後に一つまたは複数の処理活動について自由にかつ明確に行われた場合においてのみ有効である。センシティブな個人データまたはプロファイリングに関する処理については、同意は明示的に行われなければならない。

GDPR は、同意の有効性に関する条件について、以下の通りより詳細な内容を規定する。

- 第 4 条第 11 号は、同意について、自由に与えられ、特定的に、情報提供を受けたうえでかつ曖昧でないデータ主体の意思表示を意味するものであり、その意思は、当該データ主体が、陳述または明らかな積極的行為によって、自己に係る個人データの処理に関する合意

Copyright (C) 2018 JETRO. All rights reserved

を表示するものであると定義する。FDPA 法案とは異なり、同意は特定的であり、積極的行為によって表示されなければならない。

- 第 7 条は、同意を取得したことを組織が立証する責任を負う旨を規定する。また、同意の撤回は、当該撤回がなされる以前に行われた処理活動の適法性に影響を及ぼすことなく行われる。
- 同意は、以下の特定の場合にさらに規制される。
    - データ主体の同意が他の事項にも関係する書面において与えられている場合、その同意の要請は、明瞭かつ平易な文言を用い、理解しやすくかつ容易にアクセスし得る形で、その他の事項と明らかに区別できる方法によって明示されなければならない（第 7 条第 2 項）。
    - 子供に対する直接的な情報社会サービスの提供に関連する場合、同意に基づく子供の個人データの処理については子供が少なくとも 16 歳である場合に適法とされる。EEA 加盟国は、国内法において、当該年齢を 13 歳まで引き下げることが可能である。子供が 16 歳または加盟国法が定めるその他の年齢未満である場合、同意に基づく処理は、当該子供について保護責任を有する者により与えられまたは承認された同意があるときに限り適法である。

以上の通り、GDPR に基づく同意に関する要件は、FDPA 法案における要件よりも厳格な内容を規定している。

④ データ侵害に関する通知

データ侵害に関する管轄監督当局への通知については、FDPA 法案および GDPR においていくつかの相違点が存在する。

- FDPA 法案第 22 条によれば、管理者はデータ主体のプライバシーまたは基本的権利に対する高いリスクが生じる可能性があるデータ侵害（*probable to result in a **high risk** to the privacy or the fundamental rights of the data subject*）については可能な限り速やかにコミッショナーに対して通知を行わなければならない。他方で、GDPR 第 13 条では、管理者は自然人の権利および自由に対するリスクが生じる可能性が低い場合（*unlikely to result in a **risk** to the rights and freedoms of natural persons*）でない限り、データ侵害について通知を行わなければならない。言い換えると、GDPR におけるデータ侵害通知の要件（リスクの有無）は、FDPA 法案におけるデータ侵害通知の要件（高いリスクの有無）よりも厳格であるといえる。
- FDPA 法案および GDPR のいずれにおいても監督当局に対する可能な限り速やかな通知を行う義務が規定されているが、FDPA 法案では具体的な期限の定めはないのに対し、GDPR は侵害を認識した後から 72 時間という期限も定めている。
- FDPA 法案および GDPR では共に、管理者がデータ主体に対してもデータ侵害の事実を通知しなければならない場合について定めている。FDPA 法案は、データ主体を保護するための通知は義務であると規定する。これに対して、GDPR は、自然人の権利および自由に対する高いリスクが生じる可能性がある場合にのみ当該通知が義務的となる。

Copyright (C) 2018 JETRO. All rights reserved

- GDPR は、データ侵害通知の義務違反に対する制裁を規定するが（第 84 条第 4 項）、FDPA 法案は刑事的制裁を行うことを想定しない。

結論として、データ侵害通知については、データ主体へのデータ侵害通知などの一定の例外を除き、一般的に GDPR は FDPA 法案よりも厳格なルールを規定している。

⑤ データ主体の権利（データポータビリティ、削除権等）

a. 情報通知

FDPA 法案第 17 条および第 19 条は、会社および組織によるデータ主体に対する情報通知義務を規定する。このような積極的な情報通知の義務は、GDPR 第 13 条および第 14 条と共通性がある。もっとも、FDPA 法案は、域外移転に関する情報通知義務について、GDPR よりも厳しい内容を規定する。GDPR においては、個人データを域外に移転する可能性について情報通知すれば十分とされる。他方で、FDPA 法案は、個人データを受領する国を列挙することを義務付けることを想定している（FDPA 法案第 17 条第 4 項、GDPR 第 13 条第 1 項第 f 号）。

また、FDPA 法案の文言は、GDPR よりも不明確である。GDPR は提供されるべき情報を限定列挙しているが（例えば、GDPR は、データ主体は幅広く情報提供されなければならず、適用されるデータ保護ポリシー、データ処理に関する詳細な法的根拠等の詳細に関する情報提供を受けなければならないとする）、FDPA 法案は、データ主体が同法案に従った権利を主張し、個人データの処理の透明性を確保するために必要なすべての情報がデータ主体に提供されるべきであると規定する。当該情報には、例えば、以下のものが含まれる。

- 管理者の識別情報および連絡先情報
- 処理の目的
- 個人データが開示される受領者または受領者の属性（もしあれば）
- 処理される個人データの種類（処理される個人データがデータ主体から収集されない場合に限る）

結論として、個人データの移転に関して提供されるべき情報は FDPA 法案の方がより厳格であり（FDPA 法案では、データ輸入が行われる国を列挙する必要がある）、GDPR の方が義務の範囲が限定的かつ明確であるといえる。

b. データ主体のその他の権利

FDPA 法案第 4 章（第 23 条から第 25 条）は、データ主体に個人データへのアクセス権を認めている。しかし、当該権利は広い範囲で制限されており、メディア分野における例外規定や会社および組織が情報へのアクセスを拒否、制限または延期できる可能性について定めている。FDPA 法案第 28 条第 1 項によれば、データ主体は、(a)修正を禁止する法令が存在する場合または(b)個人データが公の利益のためにアーカイブを目的として処理されるものである場合を除き、誤った個人データを修正することができる。データ主体は削除権も有しており、FDPA 法案第 26 条第 2 項第 b 号は、管理者または処理者が、データ主体が表示した意図に反して個人データの処理を行った場合、プライバシー侵害を構成するものと規定する。最後に、FDPA 法案 19 条では、データ主体は、自動化判断（自動化された処理のみに基づき、データ主体に法的効果

Copyright (C) 2018 JETRO. All rights reserved

または重要な影響を与える判断）に関して情報提供されなければならず、当該判断は自然人によって審査されることを要求する機会が与えられなければならないことが規定される。

GDPR においても、個人データへのアクセス権、削除権、制限権および異議権ならびに自動化判断の対象とならない権利が規定されており（第 16 条、第 21 条、第 22 条）、FDPA 法案は GDPR に基本的に沿ったものであるといえる。もっとも、FDPA 法案とは異なり、GDPR はデータポータビリティの権利を規定する（GDPR 第 20 条）。

結論として、GDPR は、データ主体の権利について、より広範かつ詳細な内容を規定しており、FDPA 法案は GDPR の内容をある程度反映しているといえる。

⑥ データ保護影響評価

FDPA 法案（第 20 条）および GDPR（第 35 条）は、意図するデータ処理がデータ主体のプライバシーまたは基本的権利に対する高いリスクをもたらす可能性がある場合は、データ保護影響評価（Data Protection Impact Assessment、以下「DPIA」という。）が必要であると規定する。双方の規制は、DPIA の要否に関する評価はデータ処理に関して、特に以下のような特定の条件に基づいて行われることを想定する。

- 大量のセンシティブな個人データの処理を行うか
- プロファイリングを行うか
- 広範な公の空間において系統的な監視を行うか

DPIA の内容に関して、GDPR は、FDPA 法案にはない要件を規定する。(i)処理の内容の記載、(ii)データ主体のプライバシーまたは基本的権利に関するリスク評価、(iii)データ主体のプライバシーまたは基本的権利を保護するための対策に加え、GDPR は、(iv)DPIA が目的との関係で処理業務の必要性および比例性の評価についても記載することを求めている。GDPR は、DPIA の実施義務違反に対する制裁を規定するが（第 83 条第 4 項第 a 号）、FDPA 法案は刑事的制裁を行うことを想定していない。

結論として、FDPA 法案における DPIA のルールは、GDPR よりも比較的緩和された内容であるといえる。

⑦ 制裁

コミッショナーは、自らの主導でまたは要請に基づいて事案の調査を行うことができ、調査に関して以下の事項を要請することができる（FDPA 法案第 44 条）。

- 調査のために必要なすべての処理活動および個人データに関する情報、文書および明細
- 敷地および施設へのアクセス
- 証人に対する質問
- 専門家による評価

Copyright (C) 2018 JETRO. All rights reserved

データ保護に関する規制の違反があった場合、コミッショナーは一定の制裁措置を発動する権限を有する（FDPA 法案第 45 条）。

- 処理に関する完全または部分的な修正、留保または終了および個人データの完全または部分的な削除または破壊を行う旨の命令
- 一定の場合において、外国に対する開示の延期または禁止を行う旨の命令
- 域外移転に関する保護措置に関する情報提供を行う旨の命令
- セキュリティ対策を講じる旨の命令
- データ処理および自動的意思決定についてデータ主体に対して積極的な情報提供を行う旨の命令
- 影響評価の実施に関する命令（コミッショナーとの相談を含む）
- データ侵害が生じた場合にデータ主体への情報提供を行う旨の命令
- アクセスの要請に関してデータ主体に情報提供を行う旨の命令

上記の調査手続は、行政手続法によって規律される。コミッショナーの決定については、連邦行政裁判所に異議申立を行い、救済措置を受けることができる。コミッショナーおよび影響を受けるデータ主体は、連邦行政裁判所の決定に対して異議を申し立てることができる。

上記以外には、データ保護法はスイスにおいてコミッショナーではなく通常の裁判所を通じて執行可能なものである（スイスでは、データ保護法違反については法人に対する行政的制裁ではなく個人に対する刑事責任が追及されることから、制裁金は刑事上の罰金として科される）。その結果、コミッショナーは制裁金を課す権限を現在および法改正後も有しない（当該権限は刑事裁判官に委ねられる）。GDPR においては、一般的に、各 EEA 加盟国の監督当局が GDPR の違反を調査し、制裁金を課す権限を有する。もっとも、一定の場合に例外がある。例えば、デンマークにおいては、制裁金は管轄する国内裁判所によって刑事上の罰金として科すことが可能であり、エストニアでは、制裁金は軽犯罪に係る手続の枠組において監督当局によって課され得る。

制裁金の基準についても、FDPA 法案および GDPR ではルールが大きく異なる。

FDPA 法案によれば、データ保護に関する不正に対する刑事上の制裁が非常に強化されることになる。FDPA 法案の特定の規定に関する違反については、最大で 25 万スイスフランの罰金が個人に対して科される可能性がある。一定の場合において、罰金が 5 万スイスフランを超えないときは、当局は個人の起訴を猶予し、法人に対して罰金の支払を命じることができる。

これに対して、GDPR においては、監督当局によって課される制裁金は非常に高額なものとなり、違反行為の種類に応じて、最大で 1,000 万ユーロもしくはグループ会社の全世界売上高の 2%のうち高い方の金額、または最大で 2,000 万ユーロもしくはグループ会社の全世界売上高の 4%のうち高い方の金額が課される可能性がある。

結論として、FDPA 法案と GDPR の間には、制裁金について以下の相違点が存在する。

- 制裁金を課すための手続（FDPA 法案は裁判手続であるのに対して、GDPR では行政手続である）
- 制裁金の法的性質（FDPA 法案では個人の責任であるのに対して、GDPR では管理者・事業者の責任である）

Copyright (C) 2018 JETRO. All rights reserved

- 制裁金のレベル（FDPA 法案では 25 万スイスフランであるのに対して、GDPR では最大で 2000 万ユーロまたは全世界売上高の 4%である）

2. スイスにおける個人データの処理

FDPA 法案第 5 条第 1 項から第 5 項は、個人データの処理に関する基本原則を列挙しており、この内容は GDPR 第 5 条第 1 項の規定と概ね同等の内容である。

- 個人データは、適法に処理されなければならない。
- 処理は誠実に行われ、比例的な内容でなければならない。
- 個人データは、データ主体にとって明確な特定の目的のためにのみ収集することができる。個人データは、当該目的と適合する方法においてのみ処理することができる。
- 処理の目的のために必要でなくなり次第速やかに破壊または匿名化しなければならない。
- 個人データを処理する者は、個人データが正確であることを確認しなければならない。個人データを処理する者は、収集または処理の目的に関して不正確または不適合な個人データが修正、消去または破壊されるようにすべての適切な対策を講じなければならない。

FDPA 法案においては、一般的なルールとして、プライバシーに対する違法な侵害をもたらすものでない限り、個人データの処理のための法的根拠（同意等）は必要とされないことに留意する必要がある。これに対して、GDPR においては、データ処理は常に法的根拠が必要となる。スイス法によれば、処理が違法な場合においてのみ、同意、スイス法または優越的な私的利益もしくはスイスの公共の利益のいずれかによって正当化されなければならない。処理が上記の基本原則のいずれかに違反する場合、違法な処理となり、正当化が必要になると考えられる。

重要なことは、FDPA 法案は、設計および設定によるデータ保護に関する義務についても規定しており（GDPR 第 25 条と広く同等の内容である）、データ処理がデータ保護に関するルールを充足するように会社および組織が技術的かつ組織的な対策を行うことを義務付けている点である。また、GDPR は設計および設定によるプライバシー保護の義務の違反に対する制裁を規定しているが（GDPR 第 83 条第 4 項(a)）、FDPA 法案では刑事的制裁を行うことは想定していない。

FDPA 法案第 17 条から第 19 条は、会社および組織によるデータ主体に対する情報通知義務が規定される。

データ主体は、個人データに関するアクセス、修正、削除を要求する権利および自動的意思決定の対象とならない権利を有する（FDPA 法案第 19 条、第 23 条から第 28 条）。GDPR と異なり、FDPA 法案はデータポータビリティの権利を規定していない。

結論として、FDPA 法案と GDPR の間には、個人データの処理に関するルールについて多くの相違点が存在する。

Copyright (C) 2018 JETRO. All rights reserved

3. スイスと EU の間の個人データの越境的移転

EU および EEA 加盟国は、自然人に関する個人データのスイス外への域外移転について、現在のところ十分なレベルのデータ保護が提供されているとみなされている。しかしながら、コミッショナーの見解および厳格なアプローチにおいては、現行の FDPA の下では、EU および EEA 加盟国であっても法人に関する個人データについては十分なレベルの保護が提供されているとはみなされない。これは、現行の FDPA においては、「個人データ」の概念は、識別されたまたは識別され得る自然人に関する情報だけでなく、識別されたまたは識別され得る**法人**に関する情報も対象となるとされているためである。FDPA 法案においてこの点は改正される見込みであるが、現状では欧州またはその他の外国データ保護法制と対照的なルールとなっている。

したがって、法人に関する個人データが EU もしくは EEA に移転する場合または自然人に関する個人データが EEA 外に移転する場合（受領者が十分性認定のある国にいない限り）、たとえ企業グループ内における個人データの移転であったとしても、その他の正当化事由が存在しない限り、追加的な保護措置（EU の標準契約条項、スイスデータ保護法における要件の充足等）が提供されなければならない。さらに、契約上の保護措置に関してはコミッショナーに対して事前に通知しなければならない（現行 FDPA 第 6 条第 3 項、現行 FDPO 第 6 条第 3 項）。コミッショナーに対する通知を行わなかった場合には、刑事的制裁を受ける可能性がある。もっとも、前述の通り、FDPA 法案においては、識別された、または識別され得る自然人に関する情報のみが規制の対象となるため、法人に関する個人情報の域外移転は FADP 改正後は規制対象から外れる。

<u>スイスに対する EU による十分性認定に関する見通し</u>

GDPR 第 45 条第 9 項では、Directive 95/46/EC 第 25 条第 6 項に基づく十分性認定は、GDPR に従って欧州委員会が修正、改訂または廃止するまで有効とされている。したがって、スイスに関して Directive 95/46/EC に基づき採択された十分性認定は、欧州委員会が FDPA 法案を受けて十分性認定の修正等を行わない限り、有効である。現状では、欧州委員会によりスイスの十分性認定の見直しを行う動きは見られない。

FDPA 法案および GDPR において類似のルールが採択されており、FDPA 法案が現在の規定案に基づいて成立する見込みであることからすると、GDPR および FDPA の双方を遵守するために、スイス内の個人データを処理する会社は GDPR の基準にまで処理行為のコンプライアンス体制を高めることが望ましい。もっとも、現行の FADP および FDPA 法案における特別規定についても引き続き遵守する必要がある。

4. スイスと日本の間における個人データの越境的移転

FDPA 法案および GDPR は、下記のいずれかの条件により個人データの域外移転を行うことが可能となる。

- データ輸入者が十分なレベルのデータ保護を提供するとみなされた国に設立されていること（FDPA 法案第 13 条第 1 項、GDPR 第 45 条）

Copyright (C) 2018 JETRO. All rights reserved

- データ輸入者が適切な保護措置により拘束されること（契約上の措置または公法等）（FDPA 法案第 13 条第 2 項、GDPR 第 46 条）
- 法令上の例外に該当すること（同意等）（FDPA 法案第 14 条、第 49 条）

これに加えて、GDPR は下記の通り特定の規定を設けている。

- GDPR は、第三国が十分なレベルの保護を提供するとみなされること、データ輸入者が適切な保護措置を提供していること等の詳細な条件を規定しており、FDPA 法案よりも詳細な内容となっている。例えば、GDPR は、拘束的企業準則（第 47 条）の要件を規律する規定を設けている。FDPA 法案は、第三国によるデータ保護の十分性を決定する十分性の認定については連邦参事会に委ねている。
- GDPR は、個人データの移転が反復せず、限定された数のデータ主体に関してのみ行われるものであり、管理者が追求するやむを得ない正当な利益のために必要であり、当該利益がデータ主体の利益並びに権利および自由によって優越されず、管理者がデータ移転に関するすべての状況を評価し、その評価に基づいて個人データ保護に関する適切な保護措置が規定されている場合においても、個人データの移転を認めている（第 49 条第 1 項後段）。

FDPA 法案においても、個人データの域外移転についてはコミッショナーに対する通知義務が適用されることに留意する必要がある。当該義務の違反は、罰金の対象となり得る。

FDPA 法案における十分性認定

FDPA 法案において、第三国に関するデータ保護の十分性についての方針を提供するのはコミッショナーではなくなる。FDPA 法案は、第三国がデータ保護に関する十分性を有するか否かの認定について連邦参事会[2]に権限を委任する。連邦参事会の認定は、拘束力を有する。日本が十分性を有するか否かの認定は、連邦参事会の判断に委ねられる。

日本に関する欧州委員会による十分性の認定は、スイス法において自動的に承認されるものではない。連邦参事会が欧州委員会の十分性認定に即した対応を行い、連邦参事会も十分性認定を行う可能性もあるが、今後の動向を検証する必要がある。

FDPA 法案の採択までの期間における実務対応

FDPA 法案と GDPR の両方の影響を受けることが予想される企業は、個人データの処理を GDPR に基づいて提供された基準に調整することが望ましいと考えられる。FDPA 法案が GDPR よりも緩和されたルールを規定する場合には、スイスのデータ主体について GDPR を超えた措置を講じる必要はないこととなり、FDPA 法案が GDPR を超えたルールを規定しているものについてのみスイスのデータ主体に関して追加の措置を講じるという対応が考えられる。

[2] スイスの内閣のこと

Copyright (C) 2018 JETRO. All rights reserved

5. スイスにおける個人データ保護法違反の事例

- Federal Supreme Court decision 4A_406/2014; 408/2014 (BGE 141 III 119) of 12 January 2015
  連邦最高裁判所は、アクセス権に基づき、特定のスイスの銀行と米国の間における租税紛争に関連して、米国司法省に移転された個人データを含むすべての書類の写しを従業員に提供することをスイスの銀行に義務づけた。
- Federal Supreme Court decision (BGE 139 II 7) of 17 January 2015
  従業員の個人データの処理に関して、連邦最高裁判所は、従業員による電子メールとインターネットの使用状況を3ヵ月間監視する（定期的なスクリーンショットを取ることを含む）ことは違法であり、比例的ではないと判断した。さらに、透明性の原則は、特定の透明性のある状況下において、監視を可能にする社内方針によって監視が根拠付けられていることを要求しているとされた。
- Swiss Federal Administrative Court decisions A-6334/2014, A-6320/2014 and A-6315/2014 from 23 August 2016
  最近では、スイスのFederal Freedom of Information Act（2004年12月17日）に基づく公式文書へのアクセスの供与に関連するデータ保護の問題について、幾つかの裁判所の決定が下されている。2016年8月23日付けの3つの決定では、スイスの連邦行政裁判所は、FDPA第19条第4項(a)(b)の範囲に関して決定を行っている。連邦政府は、同規定に基づいて文書開示を拒絶または制限し、または(1)重要な公益または明らかにデータ主体の正当な利益にとって必要であること、もしくは(2)秘密保持または特別なデータ保護規制の法的義務が必要とすることという条件を満たす場合に開示を行う。本事案では、地方政府が、入札不正に関する民事の法的措置に関する証拠収集を行うために、スイスの競争当局によって調査および決定が行われた入札不正手続に関連する文書へのアクセスを要求した。スイス連邦行政裁判所は、反競争的行為の被害者は、スイスのFederal Cartel Act（1995年10月6日）における事業機密を含まず、かつ同法第49a条第2項のリニエンシー（課徴金減免制度）申立人により提供された情報を含まないことを条件として、情報へのアクセスが認められると判断した。
- Swiss Federal Administrative Court A-4232/2015 from 18 April 2017
  本事案の決定は、個人の人格に関するプロフィールおよび検索エンジンを通じた個人データの再生を行うことについて、スイスの経済情報プラットフォームおよび信用機関に対するコミッショナーの主張に関するものである。連邦行政裁判所は、データ主体の人格の重要な部分を組合せによって明らかにし、かつ個人の与信判断に関連しない個人データは、データ主体の同意なく公開することはできないと判断した。コミッショナーは、商業登記に登録された個人に関する経済情報プラットフォームおよび信用機関のデータは、公式のスイス連邦商業登記のデータが拒否されるのと同じ態様でのみ（検索名および「Zefix」との語句が検索ツールに入力された場合、特にグーグル等の検索エンジンはスイスの商業登記（i.e., www.zefix.ch)の結果のみを表示する）、検索エンジンにおいて表示されるべきであると主張した。スイスの連邦行政裁判所は、経済情報プラットフォームおよび信用機関は検索エンジンの検索結果の公開について限定的な影響力しか有していないと述べている。また、連邦行政裁判所は、検索エンジンによりデー

Copyright (C) 2018 JETRO. All rights reserved

タを発見する可能性について、透明性を向上させるものとして、データ保護の観点からは肯定的な効果があることを指摘した。

- The European Court of Human Rights (ECHR), in a ruling of 18 October 2016
  本判決は、公に規制される損害保険の分野におけるスイスの連邦最高裁判所の決定を覆した。スイスの連邦裁判所は、十分に詳細な法的根拠がないにもかかわらず、保険会社が保険の利益の受益者を秘密裏に監視する行為は適法であると判断していた。欧州人権裁判所の判断を受けて、連邦裁判所は、欧州人権裁判所の判断に沿って、連邦社会保障事務局（federal social security office）は傷害保険の受益者を秘密裏に監視する行為は違法であると判断した。スイス議会は、当該監視行為に関する法的根拠について要件等を規定する法案を現在作成中である。

6. 今後のスケジュール

FDPA 法案は、現在は議会による審査が行われており、2018 年 8 月上旬に発効することを暫定的に予定しているが、発効までにさらに時間がかかる可能性もある。FDPA 法案が最終的に成立するまでは、現行の FADP が適用される。

Copyright (C) 2018 JETRO. All rights reserved

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。

https://www.jetro.go.jp/form5/pub/ora2/20170108

「スイス連邦データ保護法改正案の内容および EU『一般データ保護規則』との比較」

作成者　日本貿易振興機構（ジェトロ）海外調査部 欧州ロシア CIS 課

〒107-6006　東京都港区赤坂 1- 12-32

Tel.03-3582-5569

2018.3

Copyright (C) 2018 JETRO. All rights reserved