GDPR がもたらす日本への影響

平成 30 年 6 月 18 日（月）

亜細亜大学　加藤隆之

はじめに

GDPR が 5 月 25 日に施行されたが、それが域外適用規定を設けているため、日本でも関心が高まっている。マスコミや専門家が煽っている感もあるので、本セミナーで GDPR がもたらす日本への影響とリスクを見極める機会としてもらえると幸いです。

本日私がお話しする主な項目は次の通りです。

1　GDPR 適用範囲の確認

2　規制対象とされた場合の法的責任（制裁金を中心として）

3　法的責任回避の手段？

1　GDPR 適用範囲の確認

（1）条文の確認

第 3 条　地理的範囲

1. 本規則は、EU 域内の管理者又は取扱者の事業所の活動に関連してなされる個人データの取扱いに適用される。この場合、その取扱いが EU 域内又は域外でなされるか否かについては問わない。
2. 本規則は、取扱い活動が次に掲げる項目に関連している場合、EU 域内に拠点のない管理者又は取扱者による EU 域内のデータ主体の個人データの取扱いに適用される。
   (a) データ主体に支払いが求められるか否かにかかわらず、EU 域内のデータ主体に対して商品又はサービスを提供すること。
   (b) EU 域内で行われるデータ主体の行動を監視すること。
3. 本規則は、EU 域内に拠点を持たないが、国際公法により加盟国の国内法が適用される場所に拠点を有する管理者による個人データの取扱いに適用される。

Article 3 Territorial scope

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.
2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

1 項は、1995 年データ保護指令の適用範囲を超えるものではない。また、3 項は、マン島などを念頭に置いているものと考えられるため、日本企業に関係がない。よって、問題は、2 項である。

（2）2 項の問題点

①曖昧性

・「data subjects who are in the Union」が保護の対象

→旅行者、日本人なども含む？その意義は？

Cf. 前文（2）

The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.

日本人が EU 域内で日本のショッピングサイトで商品を購入した場合は？

・「the processing activities are related to」(a)(b)が規制の対象行為

→(a)(b)に関連する（are related to）取扱いとは？

・(b)「monitoring」

→この言葉の意味は？

②1995 年データ保護指令との相違

・1995 年データ保護指令では、個人データの EEA 域外移転について、移転元を規制することに照準を当てていた。

・ところが、GDPR では、移転先をも GDPR の直接の規制対象に含めた点で、大きな転換があるように思われる。3 条 2 項の文言が曖昧ゆえに、その規制対象が広汎に及ぶ恐れもある。

→これが非常に厄介な問題を生む。

（3）実際的問題

域外適用によって GDPR の規制を受けた場合、すべての義務の履行が本当にできるのか、また、それをどのようにして、世界中に散らばっている企業のデータの取り扱いをデータ監督機関が監視、監督できるのかについては、十分な検討が必要なはずである。

→論理的障壁

物理的障壁

リソースの限界や言語の壁

（4）原理的問題

①属地主義と属人主義

刑法を例にとって考えてみる。

・属地主義の原則

・属人主義の例外　→　すべての者の国外犯（2 条）

通貨偽造罪など

国民の国外犯（属人主義、3 条）

現住建造物放火罪、強制わいせつ罪など

外国人の国民に対する国外犯（3 条の 2）

強制わいせつ罪、殺人罪、傷害罪など

公務員の国外犯（4 条）

虚偽公文書作成罪、公務員職権乱用罪など

②GDPR 国家の権限としての対人高権と領土高権

・GDPR は、属地主義、属人主義いずれも超えて規制する。

→上記におけるすべての者の国外犯と同じような理念

必要性は十分？

インターネットの特殊性

・他国の対人高権や領土高権と抵触しない？

→他国も同様の規定を設けた場合

2　適用された場合の法的責任（制裁金を中心として）

（1）法的責任の種類（一般論）

・民事責任　→　損害賠償責任など

・刑事責任　→　刑事処罰

・行政責任　→　営業停止、営業停止処分など

（2）制裁金

・GDPR では、民事責任（82 条）、刑事責任（84 条）、さらに、行政責任として、制裁金（83 条）に関する定めを置いている（制裁金については、参考資料の条文を参照）。

→プラス、顧客からの信用を失う。Too much!!

・この制裁金制度には、高額性、曖昧性、広汎性という問題がある。

・制裁金が科される場合を明らかにするため、2017 年 10 月に、欧州委員会は「規則における制裁金の適用及び設定に関するガイドライン」（Guidelines on the application and setting of

administrative fines for the purposes of the Regulation）が制定された（個人情報保護委員会のホームページで和訳も入手可能、https://www.ppc.go.jp/files/pdf/seisaikin_guideline.pdf）。

→読んでも、いかなる場合に制裁金が科されるか、ほとんどわからない。

（3）日本企業への適用

・EU 域内で活動している企業はあり得る。

→これまでも例がある。

1995 年データ保護指令時代以上にリスクが高まるかは、GDPR の運用いかんなので不透明。

だが、高額なので、恐らく、データ監督機関は頑張って制裁金を課そうとするだろう。

ターゲットは、EU に拠点を有する大企業の可能性大。

・EU 域外でのみ活動している企業に対するリスクは、当面、極めて低い。

→なぜ日本企業？中国企業、インド企業、フィリピン企業はという公平性の問題。

EU のデータ監督機関は、強制執行が可能？

・日本企業は制裁金決定を争える？

Yes　監督機関に対する不服申立ての権利（77 条）

実効的司法的救済の権利（78 条、79 条）

But　EU 域内に何も拠点がない場合には？

3　法的責任回避の手段？

（1）EU 域外への個人データ移転方法

46 条及び 49 条では、主に次のような場合に、個人データを移転できると定めている。

・十分性認定を受けた国への移転

・拘束的企業ルール（Binding Corporate Rules、BCR）

・標準データ保護条項（Standard Data Protection Clauses、SDPC）

・同意

→ 同意取得が難しくない企業は、この要件を充足した書面（形式）さえ整えれば良い。

もっとも、同意の撤回は自由なので、業態によっては、この点についてシステム構築ができて、それでビジネスに支障がなければ、同意の利用が最も便宜であろう。

（2）日本制度と十分性の認定

日本の個人情報保護制度が、今年の夏くらいに十分性決定を欧州委員会から受けるといわれている。この場合に、日本企業はいかなる影響（恩恵？）を受けるのか。

・GDPR の域外適用を受けない企業にとっては、EEA から自由にデータが送られてくる。

・GDPR の域外適用を受ける企業にとっては、論理的に考えると、十分性認定は、EEA からのデータ移転に関する事柄であるから、GDPR の適用を免れることはないはず。

→とすると、日本の個人情報保護制度の遵守では不十分であり、それにない GDPR の義務をさらに履践しなければならないことになる。

たとえば、忘れられる権利、データ・ポータビリティの権利、自動判断に服しない権利、データ保護違反通知などが考えられる。

しかし、これはいささか奇妙でもある。十分性の認定を受けた国では、EU 水準のデータ保護を確保していると判断されたのではないか？だとすると、その国に存在する企業は、その国の制度を守っていればよいはずではないか？

参考資料

GDPR 制裁金に関する条文の翻訳（加藤訳）

第 83 条　制裁金の一般条件

1. 各監督機関は、第 4 項、第 5 項及び第 6 項で定める本規則の違反に関して、本条に従った制裁金の賦課が、個々の事案において、実効的、比例的なものであり、かつ抑止的効果を有するよう確保しなければならない。
2. 制裁金は、個々の事案の状況により、第 58 条第 2 項(a)号から(h)号及び(j)号で定める措置に加え、又はこれに代えて科されるものとする。個々の事案において、制裁金を科すか否かについて、また、制裁金の額について決定するにあたっては、次に掲げる事項を考慮しなければならない。
   (a) 当該取扱いの性質及び目的並びに影響を受けたデータ主体の数及びデータ主体の受けた損害の程度を勘案した当該違反行為の性質、重大性及び期間。
   (b) 当該違反行為の故意又は過失の特徴。
   (c) データ主体の受けた損害を軽減させるために当該管理者及び取扱者がとった行動。
   (d) 第 25 条及び第 32 条に従って管理者及び取扱者が実施した技術的及び組織的対策を勘案した当該管理者及び取扱者の責任の程度。
   (e) 当該管理者又は取扱者による関連する以前の違反行為。
   (f) 当該違反行為の是正及び違反により生じ得る悪影響軽減のためになした監督機関との協力の程度。
   (g) 当該違反行為によって影響を受ける個人データの種類。
   (h) 当該違反行為が監督機関へ知らされた方法。特に管理者又は取扱者が当該違反行為を通知したか否か、もし通知したのならその範囲。
   (i) 同じ事項に関して、当該管理者又は取扱者に対して事前に第 58 条第 2 項で定められた措置が命じられていた場合、それら措置の遵守。
   (j) 第 40 条によって承認された行為規範又は第 42 条による承認された認証メカニズムの遵守。
   (k) 当該違反行為から直接又は間接を問わず得られた財政上の利益又は避けられた損失のように、当該事案の状況に該当する悪化又は軽減要素。
3. 管理者又は取扱者が故意に又は過失で、同じ又は連鎖した取扱い作業に関して、本規則の複数の規定に違反した場合、制裁金の総額は重大な違反に対して定められた額を超えてはならない。
4. 次に掲げる規定の違反行為に対しては、第 2 項に従って、1,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 2%のいずれか高額な方を限度として、制裁金を科すものとする。
   (a)第 8 条、第 11 条、第 25 条、第 26 条、第 27 条、第 28 条、第 29 条、第 30 条、第 31 条、第 32 条、第 33 条、第 34 条、第 35 条、第 36 条、第 37 条、第 38 条、第 39 条、第 42 条及び第 43 条における管理者及び取扱者の義務。
   (b)第 42 条及び第 43 条における認証機関の義務。
   (c)第 41 条第 4 項における監視団体の義務。
5. 次に掲げる規定の違反行為に対しては、第 2 項に従って、2,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%のいずれか高額な方を限度として、制裁金として科すものとする。
   (a)第 5 条、第 6 条、第 7 条及び第 9 条における、同意の条件を含む基本的取扱い原則。

(b)第 12 条から第 22 条におけるデータ主体の権利。

(c)第 44 条から第 49 条に従った第三国又は国際機関の取得者への個人データ移転。

(d)第 9 章に基づき採択された加盟国の国内法の義務。

(e)第 58 条第 2 項に従った監督機関による取扱いに関する一時的若しくは一定期間の制限若しくは命令、若しくはデータ流通の停止に従わないこと[1]、又は第 58 条第 1 項に違反してアクセスの提供を履行しないこと。

6. 第 58 条第 2 項で定める監督機関による命令の不遵守に対しては、本条第 2 項に従い、2,000 万ユーロ、又は事業である場合、前会計年度の全世界年間売上高の 4%のいずれか高額な方を限度として、制裁金を科すものとする。
7. 第 58 条第 2 項による監督機関の是正権限を妨げることなく、各加盟国は、当該加盟国に設置された公的機関若しくは団体に制裁金を科すか否か、また、いかなる程度制裁金を科すかについて定めることができる。
8. 本条に基づく監督機関による権限の行使は、実効的な司法的救済及び適正手続を含む、EU 法及び加盟国の国内法に従った適切な手続的保護措置に従うものとする。
9. 加盟国の法体系が制裁金の定めを欠く場合、本条は、管轄監督機関によって主導されかつ管轄国内裁判所によって科される罰金という方法で適用することができる。この場合、これらの法的制度は、実効的であり、かつ、監督機関によって科される制裁金と同等の効果をもつよう確保されていなければならない。いかなる場合でも、これらの科される罰金は、実効的、比例的なものであり、かつ抑止的効果を有するものでなければならない。これらに該当する加盟国は、2018 年 5 月 25 日までに本項に従って加盟国が採用する国内法の規定、及び、その後の改正法又はそれらの規定に影響を及ぼす改正についても、遅滞なく、欧州委員会に通知しなければならない。

Article 83 General conditions for imposing administrative fines

1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
   (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
   (b) the intentional or negligent character of the infringement;
   (c) any action taken by the controller or processor to mitigate the damage suffered by data

[1] この部分については、次項の第 6 項において解釈上含まれるように思われるが、別途明記されている理由については明らかではない。

subjects;

(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

(e) any relevant previous infringements by the controller or processor;

(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

(g) the categories of personal data affected by the infringement;

(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

(i) in case measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringments of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to

provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.