Deloitte.
デロイト トーマツ

発行日：2016年9月26日

デロイトトーマツサイバーセキュリティ先端研究所
ニュースレター Vol.7

EU一般データ保護規則の概要

EU一般データ保護規則の概要

プライバシー保護の枠組みとしてこれまでEU加盟国に適用されてきたデータ保護指令に替わり、あらたに一般データ保護規則（GDPR: General Data Protection Regulation）が採択されました。適用が開始される2018年5月には、企業に対し今まで以上の義務が求められており、現地の従業員や顧客等の個人データを取り扱う企業においてはその内容を理解し対応を進めておくことが重要になっています。本稿では、GDPRで求められている要件を概説します。

1 GDPRの適用範囲（域外適用）

GDPRは、本社がEUの外に設置されていても次の場合には適用されることになっており、多くの日本企業がGDPRの適用対象になることが考えられます。

表1 域外適用

適用されるケース（例）	✓ 概要
グループの現地法人がEU域内に設立されている場合	EU域内の従業員または顧客の個人データを取り扱うグループの現地法人は、GDPRにもとづいた個人データの処理が求められます。
EU域内で個人データを収集し、日本で処理を行っている場合	Cookieを含む個人データを収集し日本でデータの処理を行う場合、GDPRにおいて「行動の監視」（monitoring）※1に該当すると考えられるため、GDPRにもとづいた個人データの処理が求められます。
EU域内に業務遂行に必要な機器がある場合	個人データを保存するサーバなど、業務遂行に必要な機器がEU域内に設置されている場合、GDPRにもとづいた個人データの処理が求められます。
EU域内へ日本から直接、商品やサービスを提供している場合	Webサイトを通じて日本から直接、商品・サービスをEU域内の個人に提供している場合、GDPRにもとづいた個人データの処理が求められます。

※1 特に個人の意思決定を収集するため、もしくは個人の嗜好、行動および態度を分析または予測するためにインターネット上で自然人を追跡し、プロファイリングすること

(2)データ主体の権利の尊重

管理者は、個人データにかかわるデータ主体の権利を尊重しなくてはなりません。

表3 データ主体の権利

権利	✓ 概要
同意の有効性に関する権利	管理者に個人データを提供するにあたり、必要な情報の提供を受けることができます。
制限権	管理者に対して個人データの処理を制限することができます。
異議権	管理者または第三者によって追求される正当な利益の目的のための処理の必要性にもとづく自己の個人データの処理について異議を唱えることができます。
削除権	管理者に対して自己に関する個人データを遅滞なく削除するよう求めることができます。
アクセス権	自己の個人データへアクセスすることができます。
訂正権	不正確な自己の個人データに関する訂正を管理者に求めることができます。
データポータビリティの権利	自己に関わる個人データを、機械によって読み取り可能な形式で受け取ることができます。
自動化された個人の判断に関する権利	自己に対する多大な影響を生じうるプロファイリングを含む自動処理のみにもとづいた判断の対象にならないよう求めることができます。

(3)データセキュリティに関する義務

管理者は、取り扱う個人データについて、データセキュリティに関する義務を負うこととされています。

表4 データセキュリティに関する義務

義務		✓ 概要
侵害発生前	リスクに対して適切なセキュリティレベルを確保する技術的かつ組織的措置の実施	☑仮名化、暗号化、システム復元力の確保などの措置の実施、およびこれらの措置の定期的な検査
侵害発生後	個人データ窃盗などの個人の自由および権利にとっての危険性が高い侵害に関する通知	☑不当な遅滞なく、可能な場合には侵害に気づいてから72時間以内に監督機関へ通知する義務 ☑不当な遅滞なく、データ主体にその旨を通知する義務（処理者の場合は管理者へ通知する義務）

またこれらの他にも、管理者は所定の契機に応じてデータ影響保護評価を行うこととされています。

2 企業に求められる主な要件

GDPRでは、管理者※2に求められる要件として (1) 説明責任、(2) データ主体※3の権利の尊重、(3)データセキュリティに関する義務、(4)その他の義務 が定められています。

(1)説明責任

管理者は、個人データの処理の原則を遵守することに責任を負っており、また必要に応じてそれらの原則に遵守していることを当局に示す必要があります。

表2 個人データの処理の原則

原則	✓ 概要
適法性、公平性および透明性	適法※4、公平かつ透明性のある方法で処理すること
目的の限定	特定的で、明確かつ正当な理由のために収集され、それらの目的にそぐわない方法でそれ以上の処理を行わないこと
データの限定	処理を行う目的に関し、十分で関連性があり必要最低限に限定されていること
正確性	正確で、必要であれば常に最新状態に更新しておくこと。不正確な個人データは遅滞なく削除または訂正すること
保管の限定	処理の目的に必要な期間以上、データ主体の識別が可能な状態で保管をしないこと
完全性と機密性	不正なまたは違法な処理からの保護、不慮の損失、破壊からの保護を含み、個人データの適切なセキュリティが確保される形で処理すること

※2　管理者とは、単独または合同で個人データ処理の目的と手段を決定する者のことであり、概ね個人データを取り扱う事業者を指します。
また処理者とは、管理者に代わり、個人データ処理を行う者を指します。
※3　データ主体とは、個人データが関連する当該個人（本人）のことを指します。
※4　個人データの処理が適法であることについては、次の定めがあります。
1. その処理にデータ主体が同意した場合
2. 次の処理が必要とされる場合
- 管理者の法的な義務を果たすため
- データ主体または他の自然人の重大な利益を保護するため
- 公共の利益あるいは管理者に属する公式な権限の行使として実行する作業の履行のため　等

なお、データ主体による同意とは、管理者の身元や個人データが処理される目的、第三国への移転等について知らされたうえで、データの処理について、データ主体が発言または明快な肯定的行動によって同意を示すことを意味します。

(4) その他の義務

(a)域外移転に関する対応

EU内にいる者の個人データを域外に移転することは原則禁じられています。これに対して、(i)移転先の国・地域が十分性認定※5を得ているか、または(ii)所定の方法を採用することにより例外的に移転が可能とされます。本稿執筆時点で日本は十分性認定が得られていないため、日本に移転する場合には上記(ii)所定の方法を採用することにより域外移転を行うことが必要と考えられます。

表5 域外移転の方法

方法	概要
明確な同意	移転される個人データのすべてのデータ主体から域外移転に関する明確な同意を得る。
拘束的企業準則 (Binding Corporate Rules: BCR)	移転先を含めた企業グループにおける統一的な個人データの取り扱い規範(BCR)を定め、それを文書化し、監督機関に承認を得る。
標準契約 (Standard Data Protection Clause: SDPC)	所定の契約フォーマットをもとに移転元と移転先の間で契約(SDPC)を締結する。
認証 (Certification)	欧州データ保護会議※6または監督機関が定めた基準にもとづいて認証された移転先には域外移転が可能になる。
行動規範 (Codes of Conduct)	業界団体等がその特質を踏まえ、GDPRの遵守を目的とした行動規範を作成し、監督機関がそれを承認した場合、行動規範の範囲内で域外移転が可能になる。

※5 EUにより、個人データ保護の水準が十分であると認められた国・地域には、個人データを移転することが可能になっている。そのような十分性が認められた国・地域は本稿執筆時点で、スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージー島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランドとなっています。

※6 欧州データ保護会議(European Data Protection Board: EDPB)は、データ保護指令のもとで個人データの取り扱い等に関し意見を提示してきた第29条作業部会が改組されて設立される組織。

(b)データ保護責任者の選任

管理者または処理者の中心となる業務が、データ主体の定期的・系統的な監視を必要とするような個人データの処理から成り立っている場合や、特別な個人データを処理する場合には、データ保護責任者の設置が求められています。

(c)代理人の選任

EU域内に本社や子会社等が存在しない場合であって、GDPRの適用対象となる場合(具体的には、例えばEU域内で個人データを収集し日本で処理を行っている場合、EU域内へ日本から商品やサービスを直接提供している場合等)には、データ主体が居住するEU加盟国の1つにおいて代理人を任命することが求められています。

3 制裁金

GDPRの執行にあたって、次のような制裁金が定められています。これによれば、GDPRの違反時には最大で全世界の年間売上高の4%または2,000万ユーロのいずれか高い方という非常に高額な制裁金が科されることになっています。

表6 制裁金

制裁金	違反の内容
企業の全世界年間売上高の2%以下または€1,000万以下のいずれか高い方	☑GDPR要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合 ☑監督機関に協力しない場合 ☑セキュリティ違反を監督機関に通知しなかった場合、データ主体に通知しなかった場合 ☑データ保護影響評価を行なわなかった場合 など
企業の全世界年間売上高の4%以下または€2000万以下のいずれか高い方	☑個人データの処理の原則を遵守しなかった場合 ☑特別な個人データの処理の条件を遵守しなかった場合 ☑データ主体の権利およびその行使の手順を尊重しなかった場合 ☑個人データの移転の条件に従わなかった場合 ☑監督機関の命令に従わなかった場合 など

4 おわりに

GDPRは、EU域内の人にかかわる個人データを取り扱う企業にとって大きなインパクトを与える法制度であり、組織の広い範囲で注意深く対応を検討する必要がある一方で適用までの時間が限られている状態です。関係する企業においては、求められている要件に確実にかつ効率的に対応を進めることが重要になっています。

執筆者のプロフィール

デロイト トーマツ サイバーセキュリティ先端研究所

主任研究員　大場 敏行

国内大手製造業をはじめ、様々な業界、業種のクライアントに対して、個人情報保護、情報セキュリティに関するコンサルティング業務に従事。マイナバー法導入にあたり、地方自治体向けに特定個人情報保護評価支援を提供。
公認情報システム監査人(CISA)、情報セキュリティスペシャリスト

国内ネットワーク

有限責任監査法人トーマツ

東　京　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1112
大　阪　〒541-0042　大阪府大阪市中央区今橋4-1-1 淀屋橋三井ビルディング　Tel:06-4560-6021
名古屋　〒450-8530　愛知県名古屋市中村区名駅3-13-5 名古屋ダイヤビルディング3号館　Tel:052-565-5517
福　岡　〒810-0001　福岡県福岡市中央区天神1-4-2 エルガーラ　Tel:092-751-1517

デロイト トーマツ リスクサービス株式会社

本　社　〒100-0005　東京都千代田区丸の内3-3-1 新東京ビル　Tel:03-6213-1300
名古屋　〒450-6337　愛知県名古屋市中村区名駅一丁目1号　JPタワー名古屋　Tel:052-565-5950

201609