ＥＵ域内にいる個人の個人データを取り扱う企業の皆さまへ

GDPRの施行について

- **GDPR (一般データ保護規則)は、EU域内(※1)にいる個人の個人データを保護するためのEUにおける統一的ルールであり、2018年5月25日より施行されます。**
- **EUの個人データを取り扱う場合、EU域内に子会社や支店等の拠点を有している日本企業はもとより、そのような拠点を有しない日本企業にもGDPRが適用される可能性があり、内容を把握した上で対応を検討する必要があります。**
- **EUの個人データを取り扱わない場合、GDPRへの対応は必要ありません。**

➢ GDPRは、EU域内でビジネスを行い、EU域内にいる個人の個人データ(※2) を取得する中小・零細企業を含む日本企業に対しても、幅広く適用されます。

➢ GDPRの適用範囲
①EU域内に子会社や支店等の拠点（※3）を有している場合
②EU域内に拠点を有しておらず、以下のいずれかに該当する場合
(1)EU域内にいる個人に対して商品やサービスを提供している（※4）場合
(2)EU域内の個人の行動を監視する場合(例：アプリやウェブサイトにおける個人の行動履歴や購買履歴の追跡等)

事業者の義務について

GDPRは、主に個人データの取扱い又はEU域内から域外の第三国等への移転(※5) のために満たすべき義務を定めています。

事業者の義務の例	
通知	個人データを取得する際には、取扱者は、当該データを取り扱う目的、保管する期間等を通知しなければなりません。
同意	本人から個人データの取扱いについて明確な同意を得る必要があります。
アクセス権	本人が自らの個人情報にアクセス（開示等）できるようにしなければなりません。
センシティブデータ	センシティブデータ(健康、人種、性的指向、信仰、政治的信条に関する情報等）については原則として取扱いが禁止されます。
代理人選任義務	GDPRの適用があるEU域内に拠点のない事業者は、原則として、EU域内の代理人を書面により選任しなければなりません。
個人データ侵害の通知義務	個人データの侵害が発生した場合、原則として、72時間以内に、管轄監督機関に通知しなければなりません。高いリスクを引き起こし得る場合、本人に個人データの侵害について通知しなければなりません。
データ保護オフィサー	一定の場合には、組織内部においてGDPRの遵守を監視するデータ保護責任者を選任しなければなりません。

➢ 制裁強化
GDPRの重大な義務に違反した企業には、最大2000万ユーロ又は全世界売上の4%のいずれか高い方までの金額が制裁金として課される可能性があります。

※1　この書面でいう「EU」とは、EU加盟国28か国の他、アイスランド、リヒテンシュタイン及びノルウェーも含みます。
※2 「個人データ」とは、「識別された又は識別され得る自然人に関するあらゆる情報」を意味します。（例：氏名、識別番号、位置データ、オンライン識別子(IPアドレス、クッキー識別子）等）
※3　EUに複数の拠点がある場合、その主たる拠点があるEU加盟国の監督当局の監督を受ける等、執行の一貫性も図っています。
※4　どのような言語や通貨が使用されているか、EU域内の個人に関する言及があるか、商品やサービスの提供範囲等を考慮して判断され、単に英語のウェブサイトを載せているだけでは適用されません。
※5　個人データのEU域外への移転は、①移転先の国や地域に「十分性」（法整備などに基づき、十分に個人データ保護を講じていること）が認められている場合、②企業間の契約条項等で適切な保護措置を確保している場合及び③本人が明示的に同意している等の例外事由がある場合に認められています。なお、日本は、日本EU双方の個人情報保護制度の保護水準が十分であることを認める相互認証を行うことをEUと協議しております(2018年2月現在)。

GDPRにおいては、前述の他、様々な義務や個人に関する新しい権利を規定していることから、2018年5月25日のGDPR施行に向け、自社の事業がGDPRの適用対象となるか否か、適用対象となる場合にどのような対応が取りうるか等の検討を進める必要があります。

GDPR対応の検討にあたっての参考資料

個人情報保護委員会
●GDPRの解説等
https://www.ppc.go.jp/enforcement/cooperation/cooperation/GDPR/

経済産業省
●「第18回データ流通促進WG～国境を越えるデータ流通の促進」（2017年12月）資料4-2
http://www.iotac.jp/wg/data/

●「平成２９年度ＥＵとの規制協力を推進するための調査報告書」
http://www.meti.go.jp/policy/mono_info_service/connected_industries/index.html

JETRO
●EU 一般データ保護規則（GDPR）について
https://www.jetro.go.jp/world/europe/eu/gdpr/

JIPDEC（一般財団法人日本情報経済社会推進協会）
●翻訳版GDPR（仮訳）
https://www.jipdec.or.jp/library/archives/gdpr.html

EU
●第29条作業部会（GDPRガイドライン等）
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083（2018年1月18日以前のサイト）
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1360（1月18日以降のサイト）

参考資料に関する問い合わせ窓口等について

●参考資料についてのお問い合わせは、以下までご連絡ください。

個人情報保護委員会
https://www.ppc.go.jp/application/pipldial/

経済産業省
http://www.meti.go.jp/main/take_action.html

JETRO
https://www.jetro.go.jp/contact/

JIPDEC
https://www.jipdec.or.jp/research_inquiry.html