GCP レター

今回のテーマ
【EU 一般データ保護規則（GDPR）】

第 44 号　2018 年 7 月 31 日発行

発行者
アドバイザリーボード
弦間昭彦[1)]、小林広幸[2)]
長谷川直樹[3)]、鈴木千恵子[4)]
1）日本医科大学
2）東海大学医学部
3）慶應義塾大学医学部 感染制御センター
4）浜松医科大学医学部附属病院
臨床研究管理センター

世界で最も厳しい個人情報に関する規制と言われる「EU一般データ保護規則（General Data Protection Regulation：GDPR）」が、5月25日に施行されました。製薬業界が扱う情報においても、臨床研究の患者データ、医薬情報担当者（MR）が取得した医師情報、製品への問い合わせの際の連絡先などが対象となり、大手製薬企業ではGDPRに対応するために個人情報の管理・保護の強化を行っています。今回は、GDPRについて見てゆきましょう。

GDPR とはなにか

GDPRは、欧州経済領域（European Economic Area：EEA※1）域内に所在する個人※2に関するデータ保護を目的とした規則です。GDPRでは、個人データのEEA域外移転（持ち出し）を原則禁止としたうえで、GDPRと同等の法制度を持っている国や地域に限って、移転（持ち出し）を認めています（これを十分性認定といいます）。現時点でスイス、カナダ、ニュージーランドなど11か国・地域が十分性認定を取得していますが、日本はまだ取得していません。国レベルで十分性認定を取得していない場合、企業は、個人から個別に移転の同意を取得したり、EU当局が用意した雛形を利用して特別な契約を締結しなければなりません。

日本では2017年5月に改正個人情報保護法が施行され、さらにEUからの個人データに対する保護を上乗せする指針を策定し、今秋を目途に、十分性認定を取得する予定です。

※1：欧州経済領域（EEA）とは、欧州連合（EU）28カ国にアイスランド、リヒテンシュタイン、ノルウェーの3カ国を加えた31カ国
※2：EEA域内に所在する個人とは、国籍や居住地を問わない。つまり、域外から出張や旅行でEEA域内の国を訪れている個人のデータも対象となる

《GDPRの定義》

GDPRを一言でいうと、「個人データ」の「処理」と「移転」を規制する法律です。

個人データとは？

EEA域内に所在する個人に関するあらゆる情報

- ✓名前
- ✓位置データ
- ✓メールアドレス
- ✓IPアドレス/クッキー※
- ✓クレジットカード情報
- ✓身体的/生理的/遺伝子的/精神的/経済的/文化的/社会的アイデンティティーに関する要素

※クッキー（Cookie）
WEBサイトのユーザー情報やアクセス履歴などの情報を追跡できるデータ。これを基に個人の識別が可能。GDPRでは個人データとして扱う。

処理とは？

自動的手段で行われるか否かにかかわらず、個人データに対して行われる全ての操作

- ✓メールアドレスの収集
- ✓クレジットカード情報の保管
- ✓顧客の連絡先詳細の変更
- ✓顧客の氏名の開示
- ✓上司の従業員業務評価の閲覧
- ✓全従業員の名前や写真、職務や事務所の住所などをリストで管理

移転とは？

第三国の第三者に対して個人データを閲覧可能にするためのあらゆる行為

- ✓個人データを含んだ文書を郵便またはメールで送付
- ✓従業員の人事情報をEEA域外にある拠点で閲覧

個人の権利と企業の義務

個人の主な権利

- ✓**削除権（忘れられる権利）**
- ✓**データポータビリティーの権利**
  自分の個人データをあるサイトから別のサイトに直接移転させることもできる
- ✓**異議を述べる権利**
  ダイレクトマーケティング※のために処理されることに対して異議を述べれば、管理者はその個人データをダイレクトマーケティングの目的のために処理できなくなる
- ✓**プロファイリングを含む自動処理に基づく決定に服さない権利**
  プロファイリングなどの対象にならないよう求めることができる権利を言います。
  ☞ プロファイリングとは、個人の仕事の実績、経済状況、健康、嗜好、関心、信頼、行動などを分析するために、個人データを自働処理することです。

※ダイレクトマーケティング（ターゲティング広告等）
Amazonなどのネット通販では、購入履歴を元に、お勧め商品を自動的に提案する機能がありますが、これをターゲティング広告と言います。

企業の主な義務

- ✓**個人データを適法、公正かつ透明性のある手段で処理する**
  - ▶個人にデータ処理の目的などを明示し同意を得ているか
  - ▶目的に照らして必要以上にデータを収集しない（データの最小化）
- ✓**処理の安全性確保**
- ✓**データ侵害の場合の監督機関への通知（72時間以内）**
- ✓**データ保護責任者の任命、域外の企業は代理人の任命**

引用：週刊ダイヤモンド 2018 年 6 月 2 日号

《GDPRの主なポイント》

☞ 個人の権利が拡充したこと
- ▶個人データの定義が広い（クッキーなども含む）・・・・上記「個人データとは？」参照
- ▶権利強化（削除権、データポータビリティーの権利など）・・・・上記「個人の主な権利」参照

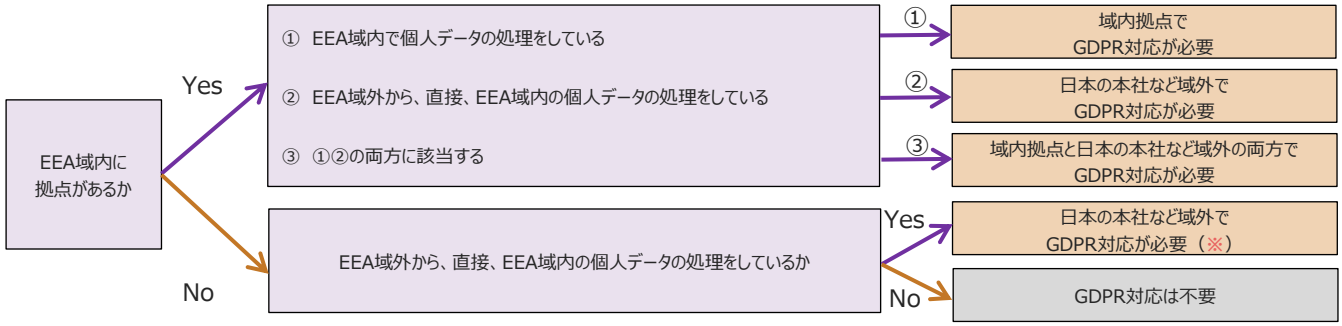
☞ 適用の対象範囲が広いこと
EEA域内に拠点が無い場合でも適用されます。また、以下のような場合においてもGDPRの対象となります。
▶出張や旅行でEEA域内に所在する日本人の個人データを日本に移転する場合
▶日本企業からEEA域内に出向した従業員の個人データ
▶日本からEEA域内に個人データを送付する場合（基準に沿って、EEA域内において処理されなければならない）
▶日本からEEA域内に個人データが送付され、EEA域内で処理された個人データを日本へ移転する場合

☞ 高額な制裁金が科せられること
最高で2000万ユーロ（約26億円）または国内外で年間総売上高の4%のいずれか高い方
→ 例えば、年間売上高1兆円の企業が個人データの処理において、適切なセキュリティー対策を講じていなかった場合、年間売上高の4%（400億円）の制裁金が科される可能性があります。

《過去に日本企業において制裁金を支払った事例》
2011年4月に発生した「PlayStation Network（PSN）がハッキングされ個人情報が流出した事件」に関して、2013年1月に、英国で個人情報の保護を管轄する政府機関(ICO)が、ソニーのゲーム部門 Sony Computer Entertainment Europe (SCEE) に対して、個人情報を扱う企業の義務を定めたデータ保護法の深刻な違反があったとして、25万ポンド（約3800万円)の制裁金の支払いを命じました。もしも、同様な事例がGDPR施行後に発生した場合には、高額な制裁金を科せられる恐れがあります。

GDPR 対応が必要か？

所属している組織が、GDPRへの対応が必要か否かについて、次のフローで確認してみましょう。



引用：週刊ダイヤモンド2018年6月2日号

※ EEA域内に拠点を持たない企業には、現地の情報が入りにくく、GDPRへの対策が最も遅れていると考えられています。これに当てはまるのは、EEA域内で収集した個人データの処理を日本で行っている場合や通販サイトや旅行会社など、日本からサービスを提供している場合などで、これらは明らかにGDPRの対象となります。

国内製薬企業のGDPR対策

国内製薬企業のGDPR対策について、6月21日付けのRIS FAXでは次のように紹介しています。（一部改変）

A社：「医療従事者、社員の個人データに影響が及ぶ」と見通し、グローバル個人情報保護責任者の指揮のもと、コンプライアンス、法務、情報システムの3部門による部門横断チームを結成し、対策を練っている。

B社：欧州のグループ会社とその他地域の会社で個人データをやり取りする場合、GDPRに基づいた契約締結の徹底、また従来からウェブサイト上のクッキー情報による閲覧者の行動分析をしないようにしている。

C社：クッキーを取得しているが、ウェブの行動分析にはグーグルアナリティクス（アクセス解析ツール）を2次利用している。

D社：英国子会社のデータ保護責任者を中心にデータ保護ポリシーやSOPを策定し、全社員対象に周知徹底を進めている。

医療機関においても、臨床研究において海外にある機関との間で個人情報を含んだ試料や情報のやり取りをする場合（例えば、遺伝子検査を海外の検査機関で実施する場合など）や、EEA域内で開催された学会などに参加して名刺交換を行い、その名刺の情報をデータベース化した場合には、GDPRの対象になり、EEA域内に拠点がなくても、無関係とは言い切れません。GDPRの対応が必要か、確認してみてはいかがでしょうか。

アドバイザリーボード運営事務局からのお知らせ

今回のGCPレターはいかがでしたか。
GCPレターに対するご意見、ご指摘、ご感想などがございましたら、アドバイザリーボード運営事務局までお寄せ願います。

アドバイザリーボード運営事務局のメールアドレス：
ssi-advisory_board@j-smo.com

GCPレターのバックナンバー：
https://www.j-smo.com/advisoryboard/archive/

【次回の発行予定】

毎日、暑い日が続いていますが、熱中症に気を付けて、お過ごしください。
次回のGCPレターは2018年9月28日発行予定です。
楽しみにして下さい。

Site Support Institute
医薬の進歩に、Human Valueを。
住所：東京都港区芝浦 1-1-1 浜松町ビルディング
TEL：03-6779-8160（代表）
URL：https://www.j-smo.com/
CMIC シミックグループ サイトサポート・インスティテュート株式会社