EUにおける個人情報保護を中心に

2023年12月1日

弁護士　苗村博子

講義目次

1. EUの個人情報保護法制概略と中核GDPR執行状況
2. GDPRが保護するデータとは？
3. GDPRの適用対象者と個人データの範囲
4. GDPRがデータ主体に認める権利
5. 管理者(Controller)と処理者(Processor)
6. GDPRの懸念するデータの移転
7. 個人データ侵害（Data Breach）発生への対応
8. GDPR違反に対する制裁

EUの個人情報保護法制の概略と中核　GDPRの執行状況

ＥＵにおける個人情報の保護法制

①General Data Protection Regulation （GDPR）
2018年5月25日から施行
個人情報保護委員会が仮訳

GDPR施行前には，1995年以降のデータ保護指令（正式にはDirective 95/46/EC）

②Regulation on Privacy and communications and repealing Directive 2002/58/EC （ePrivacy 規則案）(こちらはまだ、欧州議会でRegulationとはされていない）

- GDPRは、EU+ノルウェー，アイスランド，リヒテンシュタイン（合わせEEA） （以下、EU域内としているが実体はEEA域内）
- GDPR施行後もその執行は，各国の当局が行う。

GDPRの執行状況（違反理由別）

https://cms.law/en/int/publication/gdpr-enforcement-tracker-report/numbers-and-figures

			2022年3月現在
	違反理由	件数	課徴金額の平均€
①	データ処理の法的根拠が十分でない	342	1,267,217
②	データ処理に関する一般原則の不遵守	223	3,545,986
③	情報の安全確保に対する十分な技術的組織的方策がとられていない	198	401,522
④	データ保有者の権利を十分に満たしていない	95	178,810
⑤	情報告知の義務を尽くしていない分でない	87	2,701,756
⑥	監督官庁への協力義務を尽くしていない	40	5,898
⑦	データに関する違反についての告知義務違反	22	67,231
⑧	データ保護担当者（DPO）の不選任	12	29,217
⑨	データ処理契約が十分なものでない	6	167,763

課徴金額の高額１～８位の事例

企業名	執行国	課徴金額		
Amazon Europe Core S.à.r.l.	ルクセンブルグ	€ 746,000,000	2021年7月	②
Meta Platform Inc.	アイルランド	€ 405,000,000	2022年5月	②
Meta Platform Ireland Ltd.	アイルランド	€ 390,000,000	2023年4月	②
Meta Platform Ireland Ltd.	アイルランド	€ 265,000,000	2022年11月	④
WhatsApp Ireland Ltd.	アイルランド	€ 225,000,000	2021年９月	④
Google LLC	フランス	€90, 0 00,000	2021年３月	①
Facebook Ireland Ltd.	フランス	€ 60,000,000	2021年12月	①
Google Ireland Ltd.	フランス	€ 60,000,000	2021年10月	①

課徴金額の高額９～１３位の事例

企業名	執行国	課徴金額		
Google LLC.	フランス	€ 50,000,000	2019年1月	①
H&M Hennes &Namurits Online Shop	ドイツ	€ 35,258,708	2020年10月	①
TIM	イタリア	€27,800,000	2020年1月	①
Enel Energia S.p.A	イタリア	€26,500,000	2020年10月	①
British Airways	英国	€ 22,046,000	2020年10月	③

GDPRが保護するデータとは？

「個人データ」の情報の種類（4条1項、前文30項）

- 一つ又は複数の要素で、自然人（natural person)の個人を識別しうるすべての情報
  - 氏名
  - ID番号
  - 所在地に関する情報
  - オンライン識別子（cookie)
    又は
  - 身体的、精神的、遺伝的、経済的、文化的、社会的な、いずれかの特徴を参照することにより

GDPRの適用対象者と個人データの範囲

GDPRの適用対象者

個人データの管理者（Controller）か処理者（Processor）

EUに拠点があるか否かで保護対象となる個人データが異なる

保護される個人データの地理的範囲 1 EU域内に拠点がある場合（３条1項）

- 拠点の意味（前文22項）
  ①安定的な仕組みを通じて行われる-EU域内の物理的な場所，
  ②実効的かつ現実の活動の実施場所-個人データの処理に関連があること。
- 法系式を問わない（子会社，支店，駐在事務所等）。全くのオンラインのみで有れば①を欠く?!
- EU域内での拠点の活動が，個人データの処理と密接に関連していること
  - 特にEU域内で収益を上げている場合

- EU域内の個人のデータに限られない
  - このEUの拠点の活動の過程における個人データの処理に適用される
  - EU域外の管理者がEU域内の処理者にEU域外の個人データの処理を依頼する場合は含まない

保護される個人データの地理的範囲２E 管理者として拠点がない場合（3条2項）

- EU域内のデータ主体の個人データに限られる
  - EU域内の人をターゲットとしている場合
  - 「域内の」は国籍、居住場所を指すのではなく、その処理がされたときにEU域内に存在したこと
- EU域内の個人をターゲットとして物やサービスを提供すること
  - 有償か無償かを問わない
- EU域内の個人のEU域内での行動をモニターすること
  - 行動ターゲティング、位置情報サービス、クッキー等を用いたオンライン上での追跡等

代理人の選任ーEU域外の管理者や処理者（２７条）

- EU域内に、書面により，代理人を置かなければならない。ただし以下の場合は不要
  - 継続的でない小規模のもの
  - 公的機関によるもの

- 処理対象となる個人データのデータ主体の所在する加盟国に設置。

- 管理者、処理者に代わって、データ主体の要請、監督機関、データ主体に対応する。
  - 法的専門家であることは要求されていないが、情報漏洩などが発生した場合に、直ちに対応できる体制が取れる者を選任する必要がある。

GDPRがデータ主体に認める権利

データ主体が具体的に管理者に要求しうる権利

- データ主体が、データと管理に関する目的等の開示を要求する権利（１５条）
- 不正確かつ不完全な情報の修正を求める権利（１６条）
- データの消去を求める権利（１７条）
- 処理について制限を要求する権利（１８条）
- データポータビリティを要求する権利（２０条）
- 異議を申立てる権利（２１条）

GDPRがデータ保護を要請する処理（processing）

GDPRにおける処理（2条、4条2項）

- 全部または一部が自動的な手段による個人データの処理がなされること

- 取得、記録、編集、構成、保存、変更、復旧、参照、使用、送信による開示、配布、それ以外の方法で利用可能にすること、整理または変更、制限、破棄
- （すべてが）自動的に行われるか否かを問わない

- 個人データの（第三国や国際機関への）移転以外のすべての処理と考えるべき

処理に関する原則（5条）

1項	(a)	適法性、公正性及び透明性	データ処理に関するすべての情報、コミュニケーションが容易にアクセス可能であって、容易に理解可能で、明確かつ平易な言葉で述べられること
	(b)	目的の限定	目的が特定され、明確で正当な理由がある場合に限定されていること
	(c)	データの最小化	最小限のデータのみ処理されること
	(d)	正確性	情報の正確性を保つための措置（間違った情報の削除など）がとられていること
	(e)	記録保存の原則	目的に必要な範囲で必要な期間のみ個人が識別できる形で保管されること
	(f)	完全性、機密性	セキュリティの確保
2項		アカウンタビリティ	管理者は1項について責任を負い、証明する義務を負う

合法的な処理のための要件（6条）

(a)	データ主体が同意を与えている場合	厳格な要件
(b)	契約の履行，データ主体の要請に応じて処理が必要な場合	ネット販売の商品の配送のためのデータの提供など
(c)	管理者が負う法的義務の履行のため	EU法または該当するEU加盟国法のみ
(d)	データ主体や他の自然人の重大な利益のために必要な場合	感染症や，自然災害対策等の緊急事態
(e)	公益や管理者の公的権限の行使に必要な場合	政党員の名簿など
(f)	管理者又は第三者の正当な利益(legitimate Interest)の確保のため	データ主体の基本的権利または自由の保護（特に子供のデータ）が優先

GDPRにおける同意と同意による処理

GDPRの定義する同意（4条11）

データ主体の意思表示が、

- 任意性ー不適切な圧力がないこと
- 特定性
- 事前説明を受けていること
  - 管理者の身元、データ処理の目的、対象データの項目
  - 同意撤回権の告知
  - 自動処理（プロファイルを含む）
  - 第三国移転のリスク（可能性があれば）
- 不明瞭でないものであること

同意による処理のための条件（７条）

- 同意が書面による宣言形式で行われるときは、わかりやすい平易な言葉で同意を求めること
- 同意は、いつでも撤回できる。同意に当たっては、この撤回の権利を明示的に伝えなければならない。
- 契約の履行に必要のない個人データまで同意対象としていないかの検証が必要。

正当な利益（Legitimate Interest)とは（前文47～49項）

- 個人情報に優先する合法的な目的のために必要な処理
  - 顧客や従業員のデータをマーケティングに用いる（may be) (前文47項）
  - 企業グループで内部的な業務管理のための関係会社間（EU 域内）での移動（前文48項）
  - ネットワークおよび情報の安全上の理由等（前文49項）

- 正当な利益と考え得るかについての検討項目(前文47項）
  - データの主体が予期できるか否かがポイント
  - 以下は避けるべき
    - データ主体が異議を述べるような使用
    - 使用目的を予期できずまた理解できない
    - そのようなデータ処理が害悪を発生させる
    - 公的機関はこの正当な利益に依拠することはできない

管理者(CONTROLLER)と処理者(PROCESSOR)

管理者

- 管理者（Controller）の定義（4条（7））
  - 自然人か法人、公的機関等で―法人であれば、法人それ自体法人内の担当者ではない
  - 個人データの処理の
  - **目的（Ｗｈｙ）と方法（Ｈｏｗ）を、**
  - 単独でまたは他の者と共同で
  - 決定する者
- 現実に個人データの処理について決定している者が管理者とされる。
  - 法律事務所？

処理者

- 処理者（Processor）の定義（4条（8））
  - 管理者とは別の人または組織で、管理者を代理して個人データを処理する者
    - 関係会社間でも「別」となりうる。

管理者の義務（24条，28条1項）

- 個人データの保護がGDPRに則って行われることを確実にするための技術的、組織的な措置を取る義務を負う。

- このための行動指針を策定しなければならない。

- （管理者が委託できる）個人データの処理者は、管理者の個人データの保護がGDPRに則って行われることを確実にするための技術的、組織的な措置を実施することを約束できる者のみ

適切な処理者の選択のために

- 処理者候補者のアセスメント
  - 処理者の行動指針，業務の条件，処理状況の記録，記録の管理指針，情報セキュリティ指針，外部監査の報告書，ISO27000の様な信頼の置ける国際的な認証の取得など
- 契約後の定期的なモニタリング
- SCC s （Standard Contract Clause)
- （標準契約条項）（28条（7））
- 但し，SCC s でブランクとなっている、「処理」欄についてはなるべく具体的に。

処理者の義務

- （管理者が委託できる）処理者は、管理者の個人データの保護がGDPRに則って行われることを確実にするための技術的、組織的な措置を実施することを約束できる者のみ（28条1項）
- 処理の再委託は、事前に書面で管理者が同意した場合のみ(28条2項)
  - 再委託先の変更については，管理者の異議を認め、その手続を定めておくべき。
  - 処理者と再委託先との間でも処理契約，同等の秘密保持義務を課した処理契約が必要。

データ処理担当者（DPO）の選任（37条）

- 義務的選任
  - 私企業の場合
    - 中心業務が大規模にデータ主体の定期的、体系的モニタリングを必要とする場合、または
    - センシティブ情報を大規模に処理する場合

- 任意の選任も可能だが特別の地位を与え、責任もあるため、任意の選任には注意が必要

GDPRの懸念するデータの移転

GDPRが対応を求める移転とは？（４４条）

- 処理がなされ（てい）る個人データを、第三国や国際機関に移転するには、この規則で定める対応を、情報の管理者と処理を行う者の双方が行っていることが必要。
  - この第三国等への移転には、そこから先への転送も含まれる。

対応を要しない第三国や国際機関（４５条）

- 欧州委員会が個人データの保護に十分な措置（adequate level of protection)を取っていると認めてそれを公表している国や機関
  - 日本　　〇（2019年1月23日発効）
  - UK　　○（2021年6月28日発効）（4年間に限定）
  - アメリカ　　×（2020年7月16日のEU司法裁判所の判断）

当局の承認を要しない保護措置１（４６条２項）

(a)	公的機関の執行文書	公的機関の法的拘束力及び執行力のある文書
(b)	拘束的企業準則	47条に従って作成された法的拘束力のある会社のルール
(c)	欧州委のSCCs契約	2021年6月27日に採択
(d)	監督機関によるSCCs	
(e)	承認された行動規範	40条に従って承認された、データ主体の権利行使等を可能にする手続を定める行動規範
(f)	承認された認証措置	42条により承認された認データ主体の権利行使等を可能にする認証措置

EU委員会のSCC s （４６条２項ｃ）

- Standard Contractual Clauses
- 　　管理者と処理者間の契約(28条3，4項)

- 2021年6月27日から実施決定
  - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0915&from=EN
- 実施決定の付属書類として後半にSCC s が掲載されている。
- 2022年末までに現行の契約をこのSCC s に準拠したものに変更する必要がある。
- それまでのものは、GDPR下ではなく、旧指令下で採択されたSCC s

当局の承認を要する保護措置（４６条３項）

- 管理者か処理者が、個人データの主体に対し、権利行使、かつ賠償を求めるための、以下のいずれかの措置を講じなければならない。
- 各国の監督機関の認定が求められる措置
  - データの管理者または処理者と、第三国等で情報を受領する者との間で、契約条項がある場合
  - 行使等を可能にする公的手続があり、個人データの主体と公的機関の間に、行使等を可能にする行政的な取決めがあること

2020年7月16日CJEUのSchremesII判決

- Schremes事件は，Schremes氏が持つFacebookのアカウントの個人情報が，同社のアイルランドの子会社から本社に移転され，情報機関の監視対象とすることができたことについて，問題視し，この本社移転が，GDPR違反だとして，DPAに訴え，仮禁止命令を得た。アイルランドの高裁からの求めに応じてCJEUが判断。
- まず、2015年10月にそれまで、それまで十分性認定がないものの、米国に認めてきた、米国への移転をセーフハーバーについて2015年、CJEUは無効とした（Schremes事件）。
- そこでその後、Privacy　Shieldという枠組みが考え出されていた。

2020年7月16日CJEUのSchremesII判決

- この判断を受けて、再度Schremes氏からの申し立てがなされ、SchremesII事件に至る。この事件では、同氏は、プライバシーシールドとともに会社間で結ばれていたＳＣＣｓについても無効だと主張。再度ＣＪＥＵの判断が求められた。
- 2020年の判決で、プライバシーシールドでは十分なデータ保護がなされないとして、無効と判断。
- （旧指令下での）標準契約条項（SCCｓ）は有効とされ、これに依拠したデータ移転を認める
  - 但し，EU法上要求されるのと同程度のデータ保護
  - 移転先でSCC遵守ができない場合に移転の中止

  がなされる場合に限る

EU委員会と米国政府のデータ移転の枠組の合意の共同発表（2022年3月）

１この新枠組みの下では、GDPRで保護される個人情報が、EUとこの枠組みに参加する米国企業間で、自由かつ安全に個人情報を移転できる。

２米国の情報機関は新ルールとセーフガードに拘束され、ＥＵの個人の情報に対する権利と国家の安全保障のための手続きを整備する

３データ保護の監視裁判所の創設といった、ＥＵの個人情報が保護の違反に対する救済制度を置く。

EU委員会と米国政府のデータ移転の枠組の合意の共同発表（2022年3月）

４米国商務省を通じて出される個人情報保護の原則の厳守についてＥＵから個人情報の移転を受ける各企業にはデータ処理に関して強固な義務が課される。

５継続的な監視システム

６法的な書類化

米国側の対応の進展

- 米国情報機関が不当に個人データにアクセスした場合、

個人から申し出があれば、調査開始。

・独立した権限を有する裁判所が判断。

（バイデン大統領が2022年10月7日に上述の点についての大統領令に署名したとの報道）翌日の日経新聞より。

2023年7月のこのデータ枠組みに十分性が認定された。

個人データ侵害（DATA BREACH）発生への対応

データ保護影響評価義務(DPIA)(35条)

- ガイドライン https://www.jetro.go.jp/ext_images/world/europe/eu/gdpr/pdf/dpia.pdf

- データ処理が個人の権利及び自由に対して高度のリスクを生じさせる可能性が高い場合

- 事前にDPIAを行わなければならない。
  - 予定されている処理と目的の説明
  - 目的と処理の必要性と比例性の評価
  - データ主体の権利及び自由に対するリスクの評価
  - リスクに対する保護措置、安全管理措置等の手段

- 外部委託も認められる。

個人データの侵害（Data Breach）（4条12号）

- 処理した個人データがコントロールできない状況にあること
  - 偶発的または違法な形で
  - 移転、保存、その他の処理がなされた個人データに対して
  - 破壊、喪失、改変、無権限の開示またはアクセスにつながるような安全上の侵害
    - 機密性の侵害
    - 完全性の侵害
    - 可用性の侵害

個人データ侵害に対する対応(1)(33条)

- 管理者が個人データの侵害の発生を認識した時から
- 遅滞なく（ガイドラインでは72時間以内を推奨）
- 管理者の拠点、EU域内に拠点がない場合は代理人の拠点のある加盟国の管轄当局に対して
- 以下の点を通知する。
  - 侵害の性質
  - データ保護責任者か情報が入手できる窓口の氏名と詳細な連絡先
  - 侵害により引き起こされうる結果
  - 講じられた措置
- 段階的通知も認められている

個人データ侵害に対する対応(2)(34条)

- 個人データの侵害により、自然人の権利または自由に高いリスクをもたらす可能性が高い場合
- 認識した時から遅滞なく（ガイドラインではできるだけ早く）
- メールやSNSで直接に
- データ主体に以下の点を通知する。
  - 侵害の性質
  - データ保護責任者か情報が入手できる窓口の氏名と詳細な連絡先
  - 侵害により引き起こされうる結果
  - 講じられた措置

GDPR違反に対する制裁

GDPRで定める義務への違反に対する罰則（行政罰）

- 管理者、処理者の義務違反についてなど（83条4項）
  - 1000万ユーロか、前年の世界の売上げの２%のどちらか大きい額

- 認められていない処理（5，6，7条）や許されていない第三国等への移転についてなど（83条5項）
  - 2000万ユーロか前年の世界の売上げの４%のどちらか大きい額

ご清聴ありがとうございました。

お問い合わせは以下のアドレスまで

namura@namura-law.jp

弁護士　苗村　博子

NAMURA & PARTNERS
LEGAL PROFESSIONAL CORPORATION