Bird & Bird

GDPRの基礎総点検～今さら聞けないGDPRの基本のキ（ミュンヘン日本人会会員企業様向け 2018年7月）

バード・アンド・バード法律事務所
ブリュッセルオフィス
パートナー　弁護士　杉本 武重
直通 +32 (0)2 282 6076
携帯　+32 (0)499 054619
takeshige.sugimoto@twobirds.com

目次

Bird & Bird

I. GDPRの基本概念

EUデータ保護指令からGDPRへ

- **GDPR（General Data Protection Regulation: 一般データ保護規則）は「EU基本権憲章」というEU法体系の根幹をなす法において保障されている、個人データの保護に対する権利という基本的人権の保護を目的とした法律である。GDPRは、基本的人権という「EU基本権憲章」上の重要な価値を保障するため、違反に対し厳しい行政罰を定める。**
- **GDPR違反の場合の制裁金の上限額には2通りの類型があり、事業者以外の政府機関や事業者団体もGDPRの対象となる**
  - 1,000万ユーロ以下、または事業者の場合には前会計年度の全世界年間売上高の2%以下のいずれか高い方
  - 2,000万ユーロ以下、または事業者の場合には前会計年度の全世界年間売上高の4%以下のいずれか高い方

EUデータ保護指令 95/46/EC

（2018年5月24日まで）

- データ保護法は加盟国毎に異なる。31の加盟国法としてのデータ保護法が存在する。
- およそ40のデータ保護監督当局（Data Protection Supervisory Authority）が存在
- **第29条作業部会**（加盟国各国のデータ保護機関の代表、欧州委員会司法総局データ保護課の代表、欧州データ保護監察機関の代表によって構成される）（**EDPB**）は、特定の問題に関して共通の解釈と分析を提供することにより、EEA加盟国のデータ保護法の解釈にある程度の調和をもたらす。
- 限られた法的執行および小さな制裁

GDPR

（2018年5月25日から適用開始）

- 加盟国各国のデータ保護法は廃止（但し、一定の事項（雇用、ジャーナリズム、研究等）については加盟国が各国のデータ保護法を立法することができ、実際に立法が行われている）
- 指令よりも範囲を拡大
- 調和を増大させる。
- 企業に対して新たな説明責任を導入する。
- 個人の権利を強化する。
- 執行と制裁を増大させる（莫大な金額になりうる制裁金制度の導入）。
- 第29条作業部会は欧州データ保護会議（European Data Protection Board.「**EDPB**」）へと改組

Bird & Bird

GDPRを一言で説明すると？
「個人データ」の「処理」と「移転」に関する法律

- GDPRは、個人データを処理し、個人データを欧州経済領域(European Economic Area：EEA(EU加盟国28ヶ国＋アイスランド、リヒテンシュタイン、ノルウェー）から第三国に移転するために満たすべき法的要件を規定している。個人データの移転は原則として禁止されており、例外的に適法化される。

概念	説明	例
個人データ（第4条(1)および前文第26項から第30項）	**識別されたまたは識別可能な自然人に関連する全ての情報** **識別可能な自然人**とは、直接または間接的に識別される人である。個人が識別可能かどうかを判断するには、個人を直接または間接的に識別するために**管理者**またはそれ以外の者が適切に使用可能な全ての手段を考慮しなければならない。	– 名前 – 識別番号 – 所在地データ – 職業上のE-mailアドレス – オンライン識別子(IPアドレス / クッキー識別子) – 身体的/生理学的/遺伝子的/精神的/経済的/文化的/社会的固有性に関する要因
処理 (Processing)（第4条(2)）	GDPRは、処理がEU内で行われるか否かにかかわらず、EU内の**管理者**または**処理者**の拠点の活動に照らして個人データの処理に適用される（第3条(1); *Google Spain*, C-131/12） 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または組単位の操作**を意味する。	– E-mailアドレスの**収集** – クレジットカードの詳細の**保管** – 顧客の連絡先詳細の**変更** – 顧客の名前の**開示** – 上司の従業員業務評価の**閲覧** – データ主体のオンライン上の識別子の**削除** – 全従業員の名前、社内での職務、事業所の住所および写真を含む**ディレクトリの作成**
移転 (Transfer)	「個人データの移転」の概念は指令とGDPRのいずれにも定義されていない。あえて定義すると、**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**である	個人データを含んだ書面または電子形式の文書を郵便またはメールを通して送付する

GDPR違反の場合の制裁金の基準と違反行為の類型

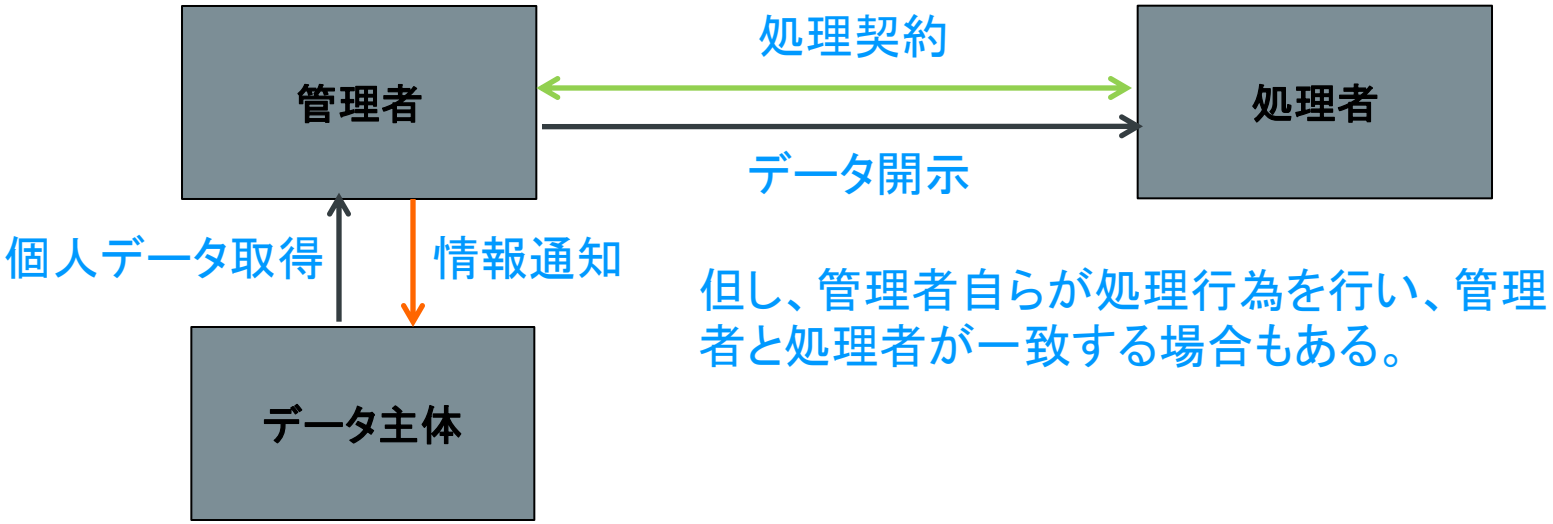
■ ポイント:「事業者の全世界年間売上高」とは、事業者グループの最終親会社に遡って、その最終親会社のグループをいう。例えば、日本企業の英国子会社によるGDPR違反の場合には日本本社のグループの全世界年間売上高となる。

制裁金の基準	違反行為の類型
管理者または処理者が、右記に当てはまる場合、1000万ユーロ以下、または事業者の場合には、事業者の全世界年間売上高の2%以下のいずれか高い方	▪ 16歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者による同意または許可が必要という条件に従わなかった場合(第8条) ▪ 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(第25条、第28条) ▪ 義務があるのにEU理人を選任しない場合(第27条) ▪ 責任に基づいて処理行為の記録を保持しない場合(第30条) ▪ 監督当局に協力しない場合(第31条) ▪ リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合(第32条) ▪ 個人データ侵害を義務があるのに監督当局に通知しなかった場合(第33条)、データ主体に通知しなかった場合(第34条) ▪ 義務があるのにデータ保護影響評価を行なわなかった場合(第35条) ▪ データ保護影響評価によって示されていたにも係わらず処理の前に監督当局に助言を求めなかった場合(第36条) ▪ データ保護責任者を選任しなかった場合、またはその職や役務を尊重しなかった場合 (第37～39条)
管理者または処理者が、右記に当てはまる場合、2000万ユーロ以下、または事業者の場合には、事業者の全世界年間売上高の4%以下のいずれか高い方	▪ データ処理に関する原則を遵守しなかった場合(第5条) ▪ 適法に個人データを処理しなかった場合(第6条) ▪ 同意の条件を遵守しなかった場合(第7条) ▪ 特別カテゴリーの個人データ処理の条件を遵守しなかった場合(第9条) ▪ 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(第12-22条) ▪ 個人データの移転の条件に従わなかった場合 (第44-49条) ▪ 第9章の下で採択された加盟国法に基づく義務に違反した場合 ▪ 監督当局の命令に従わなかった場合 (第58条(1)および(2))

GDPR上の登場人物の整理

- ポイント：自社が「管理者」か「処理者」か、「データ主体」が誰かを判断した上で、GDPRの論点の分析を行うことが重要。

概念	説明	例
データ主体	個人データが関連する当該個人	ABC社は自社従業員の個人データを処理している。この個人データが関連するABC社の従業員個人がデータ主体である。
管理者 （第4条(7)）	**単独または共同で個人データ処理の目的と手段を決定する。**管理者はデータ処理の適法性の責任を負いGDPR違反に対する責任を負う。	ABC社は自社従業員の個人データを処理している。雇用者としての義務を遂行するために処理を行っているため管理者に相当する。
処理者 （第4条(8)）	処理者は**自然人または法人であり、管理者を代理して、個人データの処理を行う。**	ABC社は他社のマーケティングツールの管理のためのデータ処理を専門業としている。この機能においてはABCは処理者であり、管理者を代理して処理を行う。



Bird & Bird

GDPRの適用範囲(第3条)

GDPR第3条についてはEDPBにおいてガイダンスを作成中

1. GDPRはEEA内の管理者または処理者の活動に関連してなされる個人データの処理に適用される。この場合、その処理がEEA域内又は域外でなされるか否かについては問わない
   - 「EEA内の管理者または処理者の活動に関連して」という概念は、非常に広範に解釈されうる。
2. GDPRはEEA内に拠点のない管理者又は処理者によるEEA内に所在するデータ主体の個人データの処理に適用される。ただし、処理活動が次に掲げる項目に関連しているものに限られる

(a) EEA内に所在するデータ主体に対する商品又はサービスの提供に関する処理。この場合、データ主体に支払が要求されるか否かについては問わない。

(b) EEA内で行われるデータ主体の行動の監視に関する処理

概念	説明	例
行動監視(前文第24項)	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**	以下の目的で顧客をプロファイリングする。 -自社のマーケティングの狙いを定める -詐欺を防ぐ -自社サービスの誤用を防ぐ -顧客の居住地、購買習慣または社会的交際範囲に関する情報の信憑性を確認
プロファイリング(第4条(4))	自然人に関連する特定の個人的側面を評価するために、特に当該自然人の職務遂行、経済的状況、健康、個人的嗜好、趣味、信頼性、態度、所在地または行動に関する特定の個人的な側面を評価するための当該個人データの使用により構成される個人データの自動処理のあらゆる形態	以下の目的で顧客をプロファイリングする。 -自社のマーケティングの狙いを定める -詐欺を防ぐ -自社サービスの誤用を防ぐ

仮名化データ(＝個人データ)と匿名化データ(＝非個人データ)

- ポイント:GDPR上の匿名化の基準である「不可逆的」な識別防止は厳しい基準であり、容易に匿名化ができたと考えないように注意が必要である。
- ポイント:GDPR上、仮名化は推奨されており、GDPR上の義務(例えば、個人データ侵害通知の場合の当局への通知義務)を軽減し、またはGDPR違反の場合の制裁金のリスクを低減させるために仮名化は有効な手法である。

概念	説明	例
仮名化データ(第4条(5)および前文第26項)	**仮名化**とは、識別されたまたは識別可能な個人に属するものではないことを保証するために、追加情報が別途保管され、かつ技術的および組織的対策の対象となっている限り、**かかる追加情報なしには、データがデータ主体に属するものと分からないように 個人データを処理することである。仮名化データは依然として個人データである**	「チャールズ・スペンサーは1967年4月3日に生まれ、二人の男の子と二人の女の子の4児の家族の父である」という文章は、以下のように仮名化されることができる。「324は二人の男の子と二人の女の子の4児の家族の父である」
匿名化データ(前文第26項、WP216の6頁)	**匿名化は不可逆的に識別を防止するもので、匿名化データは個人データではなく、**またGDPRの範囲内にも入らない。 EDPBは匿名化に不可欠な三つのリスクを検討している。以下の3つのリスクへの解決法(完全な匿名化過程)は、管理者および第三者が利用する最も可能性が高く合理的な手段によって実行される再特定化に対して堅固である。理想的な解決法はケースバイケースで決めるべきである。 **1.選び出し(Singling out)**: データセット中で個人を特定する一部または全部の記録を分離する可能性に対応する **2.照合可能性(Linkability)**:同一のデータ主体またはデータ主体の組(同一のデータベース中か二つの異なるデータベース中)に関する少なくとも二つの記録を結びつけることのできる能力 **3.推論(Inference)**:他の属性のセットの値から、ある属性の値を、高度の蓋然性をもって推論することができる可能性	データは暗号化されており、復号キーは既に廃棄されている

特別カテゴリーの個人データ（センシティブデータ）

概念	説明	例
特別カテゴリーの個人データ(センシティブデータ)(第9条(1))	**人種/種族的出身、政治的見解、宗教または哲学的信念、労働組合の組合員たる地位、遺伝子データ、生体データ、健康または性生活および性的嗜好を表す個人データ** 企業はかかるデータを例外を除き処理することができない	ABC社は自社従業員の個人データを処理し、労働組合に加入している者をリストアップする
遺伝子データ(第4条(13) および前文第34項)	**遺伝を受けたまたは後天的な個人の遺伝特性に関連する全ての個人データであり、**個人の生理機能または健康に関する固有の情報を提供するものであり、問題となる個人の生体試料の分析から明らかになるものである。	ABC社は臨床試験を行い個人のDNAを分析する
生体データ(第4条(14))	個人の固有の識別を可能にまたは確定する**特別な技術的処理から得られる個人の身体的、生理的または行動的特性に関連するあらゆる個人データ**	ABC社は顔画像を認識しそれをABC社のサーバに送信することによって個人を識別するカメラを作った。
健康に関するデータ (第4条(15) および前文第35項)	自然人の健康状態を明らかにする、ヘルスケアサービスの提供を含む**自然人の身体的または精神的健康に関連する個人データ**	発生源とは関係なく病気、障害、疾病リスク、病歴、臨床治療、或いは実際の生理的または生物医学的状態に関する全ての情報

代理人を選任する義務(第27条)

- EU域内に子会社や支店を持たない企業が代理人を選任する義務
  - 第3条第2項（GDPRの域外適用）が適用される場合、管理者または処理者は一定の場合にEU域内の代理人を書面で明示しなければならない（第27条第1項）
- 次のいずれかの場合には適用されない。
  - 第9条第1項で定める特別カテゴリーの個人データの処理または第10条で定める有罪判決および犯罪行為に関する個人データの処理を大規模に含まず、処理の性質、文脈、範囲および目的を考慮して自然人の権利または自由に対するリスクが生じそうにない、散発的になされる処理
  - 公的機関または団体
- 代理人は、データ主体が居住し、当該データ主体への商品やサービスの提供に関連して当該データ主体の個人データが処理されるか、または当該データ主体の行動が監視される加盟国の一つに拠点を持たなければならない（第27条第3項）
- 代理人はGDPR遵守に関し、管理者/処理者に加えて、または管理者/処理者の代わりに、特に監督当局およびデータ主体と対話をするため、一切の問題に取り組むために、管理者/処理者により委任される必要がある(第27条第4項)
- ポイント：EU域内に拠点を持つ企業に代理人選任義務が課せられる可能性は高くない。EDPBが今年秋に公表するGDPR第3条に関するガイダンスにおいて代理人選任義務の発生要件についても明確化される可能性が高い。

主導監督当局(第56条)

重要な概念:主導監督当局

- 「主導監督当局」は、例えば、データ主体がその個人データの処理に関して苦情を申し立てた場合に、越境的処理活動に対応する主な責任を有する機関である。
- 主導監督当局の特定は、EU域内の管理者の主たる拠点または単一の拠点の所在地の判断に依存する。GDPR第56条に以下の通り規定されている。

- *第60条の[協力]手続に基づき、管理者または処理者の主たる拠点または単一の拠点の監督当局が、管理者または処理者により実行される越境的処理に関する主導監督当局としての役割を果たす管轄権を有するものとする。*

主導監督当局(第56条)

重要な概念:主たる拠点

- GDPR第4条(16)において「主たる拠点」の意味が規定されている。
- *2か国以上の加盟国に拠点を有する管理者に関してはEU域内の集中管理の所在地を主たる拠点とみなすが、個人データの処理の目的および手段に関する決定がEU域内の他の拠点において行われており、その後者の拠点が当該決定を実行する権限を有する場合は、当該決定を行った拠点を主たる拠点とみなす。*
- *2か国以上の加盟国に拠点を有する処理者に関してはEU域内の集中管理の所在地、あるいはEU域内に集中管理がない処理者に関しては、処理者が本規則に基づく特定の義務の対象となる範囲において処理者の拠点の活動において主たる処理活動が行われるEU域内のその処理者の拠点*

主導監督当局(第56条)

特定のためのステップ: 管理者の「主たる拠点」の特定

- EU域内のデータ管理者の集中管理を最初に特定する必要がある。
- GDPRで示唆されるアプローチは、EU域内の集中管理は個人データの処理の目的および手段に関する決定が行われる場所であり、当該場所が当該決定を実施する権限を有するというものである。
- しかし、特定の処理活動の目的および手段に関する決定を集中管理以外の拠点が自立的に行う場合があり得る。これは、状況によっては、例えば異なる国において、異なる処理活動について、多国籍企業が別個の意思決定拠点を有する場合、二つ以上の監督当局が特定され得ることを意味する。その状況においては、企業が処理の目的および手段に関する決定がなされる場所を厳密に特定することが不可欠となる。
- 管理者の主たる拠点がEU域内の集中管理の所在地ではない場合
  - GDPR前文第36項は、管理者の主たる拠点を判定するために使われる主要因を明確化するために有用である。
- 処理がEU域内に本社を持つ事業者グループにより行われている場合
  - 処理の目的および手段が他の拠点により決定されている場合を除き、その統括指揮を有する拠点が個人データの処理に関する意思決定の中心地であると推定され、したがってそのグループの主たる拠点とみなされることになるであろう。親会社またはEU域内の事業者グループの運営上の本社がその集中管理の所在地となるので、その主たる拠点となる可能性が高い。

II. データマッピングで整理する GDPRコンプライアンス対応

Bird & Bird

1. GDPR遵守のための現状把握
—データマッピング

Bird & Bird

データマッピングとは

I. 目的：GDPR遵守のための現状を把握するための作業

■ ポイント：データマッピングとは、個人データの処理と移転の要件それぞれ を満 たすようにコンプライアンス対応を行うための準備

II. 方法：質問票を作成して送付・回収、インタビュー

■ ポイント：GDPR遵守のための現状を把握するためのチェックポイントを、個　人データの処理と個人データの移転とに分けて押さえる。

III. 範囲：貴社グループ全体

■ ポイント：貴社グループのEEA内の拠点をデータマッピングの優先対象とする

1. 貴社グループのEEA内の拠点全て
   - ■ 貴社グループのEEA内子会社
   - ■ 支店
   - ■ 駐在員事務所
2. 貴社グループのEEA外の拠点

GDPR遵守のための現状を把握するためのチェックポイント
個人データの処理

- ポイント：データマッピングを行いGDPR適用の対象となる個人データの処理を網羅的に洗い出す。その際に以下の事項を判断するための情報を集めておくことが重要である。
  1. 処理の原則を満たしているか？
  2. 処理の原則を遵守していることを説明できるか？
  3. 処理行為の記録を残しているか？残していないとして残せるか？
  4. 処理は法的根拠に基づいているか？
  5. データ主体（個人データが関連する当該個人）への情報通知は適切になされているか？
  6. データ主体の権利行使の要請に遅滞なく返答できるか？
  7. GDPRの要件を満たす処理者を使っているか？
  8. 処理者との業務委託契約はGDPRが要求する契約条項を含むか？
  9. 処理のセキュリティ要件を満たしているか？
  10. 個人データ漏洩の場合の監督当局やデータ主体への通知は可能か？
  11. データ保護影響評価の実施義務はないか？
  12. データ保護責任者の選任義務はあるか？誰を選任するか？

GDPR遵守のための現状を把握するためのチェックポイント(2)
個人データの移転

- ポイント：データマッピングを行いGDPR適用の対象となる個人データの移転を網羅的に洗い出す。その際に個人データの移転を適法化するために必要となる以下の情報を集めておくことが重要である。
  1. EEA域外への個人データの移転の目的は何か？
  2. 事業者グループのEEA内拠点からどこへの移転か？
     1. 事業者グループ内のEEA外拠点
     2. 事業者グループ外のEEA外拠点
  3. データ輸出者（事業者グループのEEA内拠点）は管理者？処理者？
  4. データ輸入者（事業者グループ内外のEEA外拠点）は？
  5. 標準契約条項（Standard Contractual Clauses: SCC）を締結しているか？
  6. 個人データの移転の内容は？
  7. 域外移転させる必要のない個人データを域外移転させていないか？

データマッピングの質問項目を作成する際のポイント

- 個人データの処理の目的毎に回答を求める。
  1. 個人データの処理の目的の特定
  2. どのようなデータ主体の個人データを処理しているか。
  3. 処理および移転の目的をデータ主体に通知したか。
  4. 処理する個人データの種類の詳細
  5. 個人データが含まれているデータベースの名称
  6. 特別カテゴリーの個人データの有無
  7. 個人データの保存期間の有無と程度
  8. 個人データの保存を行う法的義務の有無
- 個人データの移転の目的毎に回答を求める。
  1. 事業者グループ内での移転
  2. 事業者グループ外での移転、等

データマッピングの過程

- ポイント：データマッピングの開始から完了までには約2か月から3か月かかることが一般的

1. 質問票の作成
2. 質問票の回答義務者の大まかな特定

- ポイント：EEA拠点一つにつき回答者義務者一人ではあまりワークしない。EEA拠点内の部門毎に回答してもらうと、きちんとした回答が得られる。ここはEEA拠点内のマンパワーにもよるため、現状を踏まえて判断する。
  - 人事、IT、営業、マーケティング、総務、法務、経理のそれぞれの部署が様々な個人データを様々な目的で処理

3. （質問票に関する社内セミナー、説明会、電話会議）
4. 質問票の配布、締切の設定：最低2~3週間
5. 質問票の回収、回答内容の検討
6. 追加質問の送付、回答内容の詳細な検討

- ポイント：EEA内拠点でのインタビューを併用すると短期間に充実したデータマッピングを行うことが可能

データマッピングの結果として何ができるか？

- ポイント：データマッピングの結果を可能な限り多くGDPR遵守に直接つなげる。
  - 個人データの処理
    - GDPRの適用対象となる個人データの処理行為のリストアップ
    - 個人データの処理行為の記録のドラフト作成（記録保持義務への対応）
    - 個人データの処理行為ごとに法的根拠の有無の判断と見直し
    - 個人データの処理のうち同意の取得が必要な場合を特定
    - データ主体に対する情報通知が困難と思われる場合を特定
    - 外注契約の見直しが必要となる第三者（処理者）を特定
    - データ保護影響評価の実行義務の有無を判定
    - データ保護責任者の選任義務の有無を判定
  - 個人データの移転
    - 事業者グループのEEA内拠点からEEA外の事業者への個人データの移転の流れを特定
    - 事業者グループ内での個人データのEEA域外への移転について欧州委員会が決定したデータ移転契約（標準契約条項（Standard Contractual Clauses, “SCC”））使用のためのドラフトの作成

現状把握に基づく処理行為アセスメントレポートの記載事項（例）

各データ処理行為に関し、以下の事項を記載する

- データ処理行為の目的
- 当該処理行為に関し、貴社が管理者／処理者のいずれであるかの区別
- データ処理契約の要否
- 個人データとデータ主体
  - データ主体の種類及び数
  - 個人データの種類
- 個人データの保存期間とその分析
- 個人データ処理の法的根拠とその分析
- データ主体に対する情報通知（直接通知・間接通知のいずれが必要か）
- DPIA（Data Protection Impact Assessment：データ保護影響評価）の要否の分析
- データ侵害通知（越境的処理行為（複数の加盟国に関連するデータ処理行為）該当性、該当する監督当局の所在国）

その他の成果物等（例）

- 処理行為記録の作成（処理行為アセスメントレポートをベースに作成）
- データ主体に対する情報通知のサンプル作成
- 個人データ処理のための同意書サンプルの作成
- グループ間のSCCの作成（質問票Cの回答を元に作成）
- 処理契約の条項のサンプル作成
- データ侵害時マニュアルの作成
- 個人データ侵害が発生した場合、72時間以内に監督当局及びデータ主体への報告が必要
- 報告体制・手順をまとめたマニュアル、報告文書の作成
- データ主体による権利行使への対応マニュアルの作成
- プライバシーポリシー・個人データ処理に関する内部規程・トレーニング素材等の作成
- DPO（Data Protection Officer：データ保護責任者）の選任要否について助言
- DPIA（データ保護影響評価）の実施のための雛形提示、実施について助言

2. 個人データの処理の主なチェック項目

個人データの処理の主なチェック項目

1. 処理の原則を満たしているか？
2. 処理の原則を遵守していることを説明できるか？
3. 処理行為の記録を残しているか？残していないとして残せるか？
4. 処理は法的根拠に基づいているか？
5. データ主体への情報通知は適切になされているか？
6. データ主体の権利行使の要請に遅滞なく返答できるか？
7. GDPRの要件を満たす処理者を使っているか？
8. 処理者との業務委託契約はGDPRが要求する契約条項を含むか？
9. 処理のセキュリティ要件を満たしているか？
10. 個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？
11. データ保護影響評価の実施義務はないか？
12. データ保護責任者の選任義務はあるか？誰を選任するか？

1. 処理の原則を満たしているか？

- ポイント：管理者は、個人データ処理の原則の遵守に責任を負い、その遵守を実証できる必要がある。GDPRは単に遵守しているだけでよい法ではなく、どのように遵守しているかまで要求する。

原則	内容
適法性、公平性および透明性	適法、公平かつ透明性のある方法で処理すること(第5条(a))
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なわないこと(第5条(b))
データの限定	処理を行なう目的に関し、十分で関連性があり必要最小限に限定されていること(第5条(c))
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(第5条(d))
保管の限定	処理の目的に必要な期間以上、データ主体の識別可能な状態で保管をしないこと(第5条(e))
完全性と機密性	不正または違法な処理からの保護、不慮の損失、破壊、損失からの保護を含み、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(第5条(f))

2. 処理の原則を遵守していることを説明できるか？

- ポイント：EEA域内の拠点（子会社、支店および駐在員事務所）で、個人データを処理する場合、データ保護方針を策定する必要がある。
  - データ保護方針とは？
    - 個人データ保護規程（内部規程）
    - プライバシーポリシー
  - データ保護方針なしに、どのようにGDPRの処理の原則を遵守しているのかの説明は困難
- 具体的な対応の手順
  - 日本本社でGDPRに対応したデータ保護方針を制定・施行
    - 日本の個人情報保護規程とは別に、GDPR対応のデータ保護方針を作成し、EEA所在者の個人データの処理についてのみ適用する。
  - 日本企業のEEA域内の支店や駐在員事務所では、日本本社のGDPR対応のデータ保護方針を策定

3. 処理行為の記録を残しているか？残していないとして残せるか？
管理者の義務

- **ポイント：データマッピングを詳細に行い、処理行為の記録を残すことを意識した作業を行う。**
- **各管理者および、該当する場合、管理者の代理人は、管理下にある処理行為の記録を保持しなければならない。記録は次に掲げる情報のすべてを含む（第30条第1項）。**
  - 管理者の名前と連絡先の詳細。該当の場合、共同管理者、管理者の代理人およびデータ保護責任者を含む
  - 処理の目的
  - データ主体の種類と個人データの種類の概要
  - 第三国または国際機関における取得者を含め、個人データが開示されるまたは開示され得る取得者の種類
  - 該当する場合、第三国または国際機関を特定した形式による第三国または国際機関への個人データ移転、および、第49条第1項後段で定める移転の場合、適切な保護措置に関する文書
  - 可能であれば、データ種類ごとの削除までの予測される期限
  - 可能であれば、第32条第1項で定める技術的および組織的安全保護措置の概要
- **記録保持義務は、250名未満の人を雇用する企業/組織には適用されない。以下のいずれかの場合は250名未満の人を雇用する企業／組織にも適用される。**
  - 当該処理がデータ主体の権利および自由を危険にさらす可能性があり、
  - 処理が偶発的ではなく、または
  - 特別カテゴリーのデータ（人種/種族的出身、政治的見解、宗教または哲学的信念、労働組合の組合員たる地位、遺伝子データ、生体データ、健康または性生活および性的嗜好を表す個人データ）（例えば、健康診断の結果）または有罪判決および犯罪行為に関する個人データの処理を含む場合

3. 処理行為の記録を残しているか？残していないとして残せるか？
処理者の義務

- 各処理者および、該当する場合、処理者の代理人は管理者に代わって行うすべての種類の処理行為に関する記録について、次に掲げる事項を含め、保持しなければならない。
  - 処理者または複数処理者および処理者が代わりに実施している各管理者ならびに、該当する場合、管理者または処理者の代理人およびデータ保護責任者の名前と連絡先の詳細。
  - 各管理者の代わりに実施している処理の種類。
  - 該当する場合、第三国または国際機関を特定した形式によるその第三国または国際機関への個人データ移転および、第49条第1項後段で定める移転の場合、適切な保護措置に関する文書。
  - 可能であれば、第32条第1項で定める技術的および組織的安全保護措置の概要。
- 記録保持義務は、250名未満の人を雇用する企業/組織には適用されない。以下のいずれかの場合は250名未満の人を雇用する企業／組織にも適用される。
  - 当該処理がデータ主体の権利および自由を危険にさらす可能性があり、
  - 処理が偶発的ではなく、または
  - 特別カテゴリーのデータまたは有罪判決および犯罪行為に関する個人データの処理を含む場合

4. 処理は法的根拠に基づいているか?(1)

- ポイント:管理者/処理者は以下のいずれかの要件を満たす場合に個人データの処理を行うことができる。個々の個人データの処理がいずれかの要件を満たすかをチェックする。「同意」は撤回が自由であり、データポータビリティ権を発生させ、かつ削除権が広範に認められることにつながるため、可能な限り「正当な利益」を法的根拠とすることが望ましい場合が多い。
  - 1. データ主体が一または一以上の個別の目的のため、自己の個人データの処理に同意を与えた場合(第6条(1)(a))
  - 2.-5. 以下のいずれかの処理が必要とされる場合(第6条(1)(b)-(e))
    - 2. データ主体が当事者である契約の実行のため、または、データ主体の要請により契約締結前に段階を踏むため
    - 3. 管理者が負う法的義務を遵守するため
    - 4. 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
    - 5. 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
  - 6. データ処理は管理者あるいは第三者が追及する正当な利益の為に必要である場合。但し、例　外として、データ主体が子供であった場合のように、そのような利益が個人データの保護として、データ主体の利益または基本的人権および自由に優先される場合は除く(第6条(1)(f))。この点において、データを収集する時点でのデータ主体の合理的な予測が考慮されるべきである(前文第47項)
    - 指令第7条の管理者の正当な利益の考え方に関するEDPBの意見書(WP217)参照

4. 処理は法的根拠に基づいているか?(2) – 同意

- データ主体の同意とは、自由に与えられた、個別の、情報に基づく、不明瞭ではないデータ主体の意思表示によって、データ主体が発言または明快な肯定的行動により合意を示すことを意味する(第4条(11))。
  - 同意が情報に基づくものと認められるためには、データ主体は少なくとも管理者の身元と個人データが処理される目的について知っている必要がある(前文第42項。第13条・第14条参照)。
  - 同意が自由に与えられたか否かを検討する際、契約の履行としてデータ処理への同意が条件とされているかについて最大の注意が払われなければならない(第7条(4)、前文第43項)。
    - データ主体に実質的な選択の自由がなく、不利益を被ること無しに同意を撤回することが不可能な場合、同意は自由に与えられたものとみなされない(前文第42項)。
      - 監督当局は管理者が従業員から取得する同意については任意性について疑いを持っている。
      - 「個人データの処理の適法性」の「2. データ主体が当事者である契約の実行のため処理が必要な場合」の要件に依拠できる分は依拠する。そのうえで、正当な利益に依拠できるかを検討する。それでも処理の適法性を担保できないおそれがあれば同意を取得する。
- 同意が書面による声明として求められた場合、他の項目が問題となる。同意の依頼は、他の項目から明確に識別できる形で表記され、分かりやすい言葉で明瞭かつ簡潔に書かれていなければならない。声明の一部がGDPRに違反する場合、データ主体の同意に拘束力はない(第7条(2))
- データ処理の目的が複数である場合、同意を全ての処理目的について取得するべき(前文第32項)
- データ主体はその同意をいつでも撤回する権利を有する。同意の撤回は、撤回前のデータ処理の適法性に影響を与えるものではない。これらの点は、同意を行う前にデータ主体に知らされなければならない。同意の撤回は同意を行うときと同様に簡単でなくてはならない(第7条(3))
- 情報社会サービスに関連するデータ処理の対象が16歳未満の子供の場合、同意は子供に対し親の責任を有する者によって承認されなければならない(第8条(1))
  - 加盟国はこの年齢を法律により13歳未満とならない範囲でより低い年齢を規定することができる(第8条(1))
  - 管理者は、平均的な技術を考慮し、同意が子供に対し親の責任を有する者によって承認されたことを確認するために合理的な努力をする必要がある(第8条(2))

4. 処理は法的根拠に基づいているか?(3) – 特別カテゴリーの個人データの処理の適法性(第9条)

- 特別カテゴリーの個人データの処理は、以下の場合を除き、認められない。
  - データ主体が明示的同意をしている(第9条(2)(a))
    - 「明示的同意」は「個人が個人データの個別の使用または開示に対し同意するかまたは同意しないかという提案を示され、かつ当該個人が積極的に口頭または書面により質問に回答する全ての状況」を含む。
    - 通常、明示的同意は、手書きの署名付きの書面により与えられるが、これは必ずしも必要ではなく、口頭で与えることもできる(WP187の25頁)。
- 以下のいずれかの場合に処理が必要である。(「正当な利益」による処理が適法でない点が「個人データ」と異なる)
  - 雇用や社会保障における義務の履行または権利の行使の目的のために処理が必要な場合(ただし、データ主体の基本的権利および利益に対する適切な保護措置を定めたEU法もしくは加盟国法または労働協約によって認められている場合に限る)(b)
  - データ主体の重大な利益を保護する場合(c)
  - 処理が、政治的、哲学的、宗教的または労働組合の目的を有する非営利団体によって適切な保護措置を伴う適法な活動において実行され、当該処理が当該団体の(前の)構成員または当該目的との関係で当該団体と頻繁に接触していた者にのみ関係するものであること、および当該個人データが当該データ主体の同意なしに当該団体の外へ開示されないことを条件とする場合(d)
  - データがデータ主体により、明確な形で公開されている場合(e)
  - 法的請求の立証、行使または防御のため に必要である場合(f)
  - 処理が、重要な公的利益のために必要である場合(ただし、追求する目的に比例しており、データ保護に対する権利の核心を尊重し、かつデータ主体の基本的人権および利益を保護するための適切かつ具体的な措置を規定する、EU法および加盟国法に基づく場合に限る) (g)
  - 予防的なもしくは職務上の医療目的、従業員の業務遂行能力の評価、医療診断、ヘルス ケア、治療、ソーシャルケア、処置の提供にとって処理が必要な場合(ただし、EU法もしくは加盟国法または医療専門家との契約に基づく場合に限る) (h)
  - 公衆衛生の分野における公共の利益を理由として処理が必要である場合(ただし、データ主体の権利等、特に秘密保持を 保護するため適切かつ具体的対策を規定する EU法または加盟国法に基づく場合に限る)(i)
  - 第89条(1)による公共の利益でのアーカイブの目的、科学的または歴史調査目的、もしくは統計目的で必要である場合(ただし、追求する目的に比例しており、データ保護に対する権利の核心を尊重し、かつデータ主体の基本的人権および利益を保護するための適切かつ具体的な措置を規定する、EU法および加盟国法に基づく場合に限る) (j)

5. データ主体への情報通知は適切になされているか？

情報通知－データ主体から個人データを直接取得した場合

- ポイント：情報通知義務の中で「処理の目的および法的根拠」の情報が求められているため、個人データの処理の法的根拠は、予め整理・検討しておく必要がある。
- 情報通知義務：データ主体から個人データを収集する場合には管理者はデータ取得時に、以下の情報を提供する必要がある。
  - 管理者、ならびに(当てはまる場合には)代表者および／またはDPOの身元および連絡先詳細
  - 処理の目的および法的根拠
  - 処理の法的根拠である、管理者または第三者によって追求される正当な利益
  - 個人データの受領者または受領者のカテゴリー
  - 管理者の第三国または国際組織への個人データ移転の意思および、十分性決定の有無、または当てはまる場合、適切な保護措置への言及や当該コピーの入手方法または入手先
  - 個人データの保管期間、それが可能でない場合にはそのような期間の決定に使われる基準
  - 監督当局に苦情を申し立てる権利を含む、データ主体の権利
  - 同意をいつでも取り消すことのできる権利
  - プロファイリングおよび少なくとも関連する論理についての意味のある情報、ならびにデータ主体の当該処理に伴う想定上の結果その意義を含む、自動化判断の有無
  - 個人データの条項が法律上または契約上の義務であるかどうか、または契約を結ぶ必要のある義務であるか、データ主体がデータを提供する義務があるかどうか、ならびに提供しない場合に起こり得る結果
- ポイント：情報通知義務はデータ主体から個人データを直接取得したのではなく、別の管理者から取得する場合にも発生する。

6. データ主体の権利行使の要請に遅滞なく返答できるか？
データ主体が権利行使してきたときの対応マニュアルの作成

- ポイント：データ主体がデータ主体の権利（情報権、アクセス権、訂正権、削除権、データポータビリティの権利、異議権）を行使してきた場合には、原則として依頼を受け取ってから1ヶ月以内に対応しなければならない。
- データ主体の権利の行使があったときの対応マニュアルの作成
  - 管理者は、データ主体の権利を尊重する義務があるため、データ主体の権利行使のための管理者における連絡先を個人データ保護方針等で明らかにしておく必要がある。
  - 遅くとも依頼を受け取ってから1ヶ月以内、要求の複雑性または数を考慮し、必要に応じてさらに2ヶ月まで延長することができる。
  - 管理者は企業グループ内でデータ主体の権利行使があった場合に適切に対応するメカニズムを作る必要あり
- データ主体の苦情に対応することができるように内部の苦情対応手続の構築

6. データ主体の権利行使の要請に遅滞なく返答できるか？

データ主体の権利への対応(第12条第1項-第22条)

データ主体の権利	内容
情報権(第13条、第14条)	管理者はデータ主体から個人データを収集する場合に、個人データ入手時に、データ主体に一定の情報を提供しなければならない。
アクセス権(第15条)	管理者はデータ主体から処理が行われている個人データへのアクセスの請求があればそのコピーを提供しなければならない
訂正の権利 (第16条)	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権利を有する
削除権(第17条(1))	一定の場合、データ主体は自分に関する個人データの削除を遅滞なく管理者から得る権利を有する。
制限権(第18条)	データ主体は管理者に対して一定の場合に個人データ処理を制限する権利を有する。
データポータビリティの権利(第20条)	データ主体は自分に係わる個人データを、構造化され、一般的に使用され、機械可読なフォーマットで受け取る権利を有する。
異議権(第21条)	データ主体は管理者または第三者によって追求される適法な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱える権利を有する。
自動化された個人の判断に関する権利(第22条)	データ主体は、自分に対する法的影響を生じ得たり、自分に対する多大な影響を生じ得るような、プロファイリングを含む自動処理のみに基づいた判断の対象にならない権利を有する(例、人が介入しないオンライン上での借入申込やインターネットでの採用活動–前文第71項)。

6. データ主体の権利行使の要請に遅滞なく返答できるか？

制限権(第18条)および異議権(第21条)

制限権(第18条)

- **データ主体は管理者に対して以下の場合に個人データ処理を制限する権利を有する。**
  - 管理者がデータの正確性の検証を行なうことのできる期間中にデータの正確性についてデータ主体が異議を申し立てた場合
  - 処理が違法であり、データ主体がデータの削除に反対し、その代わりに使用の制限を要請した場合
  - 管理者が当該処理のために個人データが不要となったが、当該個人データが法的請求の立証、行使、防御のために個人データを必要としている場合
  - データ主体が管理者の適法な根拠がデータ主体のそれに優越するかどうかの確認を行う前の処理に反対した場合

異議権(第21条)

- **データ主体は管理者または第三者によって追求される適法な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱える権利を有する。**
  - 管理者が、データ主体の利益、権利、および自由に優先する処理のため、または法的請求の立証、行使、防御のために説得力のある適法な根拠を証明する場合を除く。
  - 異議権は、科学的研究/統計目的のための処理が公的利益の理由で遂行される業務の履行のために必要な場合には適用されない。

6. データ主体の権利行使の要請に遅滞なく返答できるか？

アクセス権（第15条）および訂正権（第16条）

アクセス権(第15条)

- **データ主体は自己の個人データのアクセス権を有している**(第15条(1))
- かかるデータが処理されている場合、データ主体は情報の権利を有している。
- 管理者は処理が行われている個人データのコピーを提供しなければならない。これは他人の権利・自由に悪影響を与えてはならない。
  - データ主体によってさらなるコピーの提供が要求された場合、管理者は事務手続費用に基づいた合理的な費用を請求できる

訂正権(第16条)

- **データ主体は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権利を有する**(第16条)
- データ主体は不完全な個人データを完全にすることを求める権利を有する
- 管理者は、データを開示した受取人に対して、不可能または比例的でない努力が必要とならない限り、全ての訂正について連絡しなければならない(第19条)

6. データ主体の権利行使の要請に遅滞なく返答できるか？
削除権(忘れられる権利)(第17条)

■ ポイント:削除権は、管理者が個人データの処理を「正当な利益」という法的根拠で行う場合は、行使が認められにくい。

削除権(第17条(1))

- **以下の場合、データ主体は自分に関する個人データの削除を遅滞なく管理者から得る権利を有する**
  - 処理の目的に関して、当該個人データがもはや必要ない場合。
  - データ主体が、第6 条第1 項(a)号又は第9 条第2 項(a)号による同意に基づく処理の同意を撤回し、かつ処理に関して他の法的根拠がない場合。
  - データ主体が、第21 条第1 項により不服を申立て、かつ処理に関して優先する法的根拠がない場合。又はデータ主体が第21 条第2 項により不服を申し立てる場合。
  - 個人データが不法に処理された場合
  - 個人データが、管理者が従うべきEU法又は加盟国の国内法における法的義務の遵守のため消去されなければならない場合。
  - 個人データが第8 条第1 項で定める情報社会サービスの提供に関して収集された場合。

データの公開を行なった場合にするべきこと(第17条(2))

- 管理者が個人データの公開を行ない、そのデータを削除する義務がある場合、管理者は、使用可能な技術および実施の費用を考慮し、技術的な措置、管理者が個人データのリンク、コピー、複写を削除することに関するデータ主体による要請があったことを、データを処理する管理者へ通知することを含む、合理的な措置をとらなければならない

適用除外(第17条(3))

- **削除権は、処理が以下の場合に必要である限度においては適用されない**
- 表現および情報の自由の権利の行使のため
- EUまたは管理者の対象となる加盟国の法律により、個人データの処理が必要となる法的義務の遵守、公共の利益のために遂行された任務、または管理者の授権された公権力行使のため
- 公衆衛生における公共の利益の目的
- 削除権が、その目的の達成を不可能にする、または著しく妨害する可能性がある場合の科学的／統計目的
- 法的請求の立証、行使または防御

6. データ主体の権利行使の要請に遅滞なく返答できるか？
データポータビリティの権利

- ポイント：データポータビリティの権利は、「正当な利益」という法的根拠に基づく個人データの処理との関係では発生しない。

データポータビリティの権利(第20条)

- データ主体は、当該データ主体が管理者に提供した当該データ主体に関する個人データについ て、構造化され、一般的に利用され機械可読性のある形式で受け取る権利があり、当該データ を、個人データが提供された管理者の妨害なしに、他の管理者に移行する権利がある。ただし、次に掲げる場合に限る。
  - 処理が同意に基づいている場合または契約に基づく場合で、かつ
  - 処理が自動手段で実行されている場合
- 当該データ主体のデータポータビリティーの権利が行使される場合、データ主体 は、技術的に実行可能であるならば、個人データを直接的に管理者から他の管理者に移行させる権利がある。

7. GDPRの要件を満たす処理者を使っているか？

処理者がGDPR対応を行っていることを確認する

- ポイント：個人データ処理を伴う業務を外注する場合または既に外注している場合には、外注先である第三者（処理者）によるGDPR対応状況について確認を行う。
- 管理者の代わりに処理が実施される場合、その管理者は、処理がGDPRの要件に合致し、データ主体の権利の保護を確実にする処理方法で、適切な技術的および組織的な対策を実施することを十分に保証する処理者のみを利用しなければならない（28条1項）。
- 管理者としては、自らが選任した処理者がGDPRに違反する場合には、当該違反の責任を問われかねない。
  - GDPRを遵守していないクラウドコンピューティングサーバを利用することのリスク

8. 処理者との業務委託契約はGDPRが要求する契約条項を含むか？

- ポイント：個人データ処理を伴う業務を外注する場合には、外注先である第三者（処理者）との間で締結する業務委託契約のひな型に下の条項が網羅されていることを確認する。既に個人データ処理を伴う業務を外注している場合には、外注先である第三者との業務委託契約の見直しを行う。
- 管理者から処理者への処理行為の委託は契約もしくはEU法または加盟国法（管理者に関する処理者を拘束し、処理の対象事項および期間、処理の性質および目的、個人データの種類およびデータ主体の種類ならびに管理者の義務および権利を定める法）に基づく法律行為に基づかなければならない（第28条第3項）。
  - 処理者が従うべきEU法または加盟国の国内法によって処理の実施が要求されていない限り、第三国または国際機関への個人データの移転に関することを含め、管理者からの文書化された指示においてのみ個人データを処理すること。当該法律によって処理の実施が要求されている場合、処理者は、当該法律が重要な公共の利益に基づき当該通知を禁止していないならば、処理する前に当該法的要件について管理者に通知しなければならない。
  - 個人データを処理することを許可された個人が機密保持を確約するか、または適切な法的機密保持義務下に置かれることを保証すること。
  - 第32 条（処理のセキュリティ）により要求されているすべての対策をとること。
  - 他の処理者を従事させることに関して第2項および第4項で定める条件を遵守すること。
  - 処理の性質を考慮し、可能な限り、管理者が第3章に定められたデータ主体の権利行使の要求に応じる義務を履行するため、適切な技術的および組織的対策によって管理者を支援すること。
  - 処理の性質および処理者の利用可能な情報を考慮し、第32条から第36条による義務の遵守を確実にすることにおいて管理者を支援すること。
  - 管理者の選択により、処理に関連したサービスの提供終了後にすべての個人データを消去または管理者に返却することおよび、EU法または加盟国の国内法が個人データの保存を要求しない場合に限り、存在する複製物を消去すること。
  - 本条項に定められた義務の遵守を証明するとともに、管理者または管理者により委任された他の監査人によって実施される調査を含めた監査への準備および寄与を行うために必要なすべての情報を管理者が入手可能にすること。

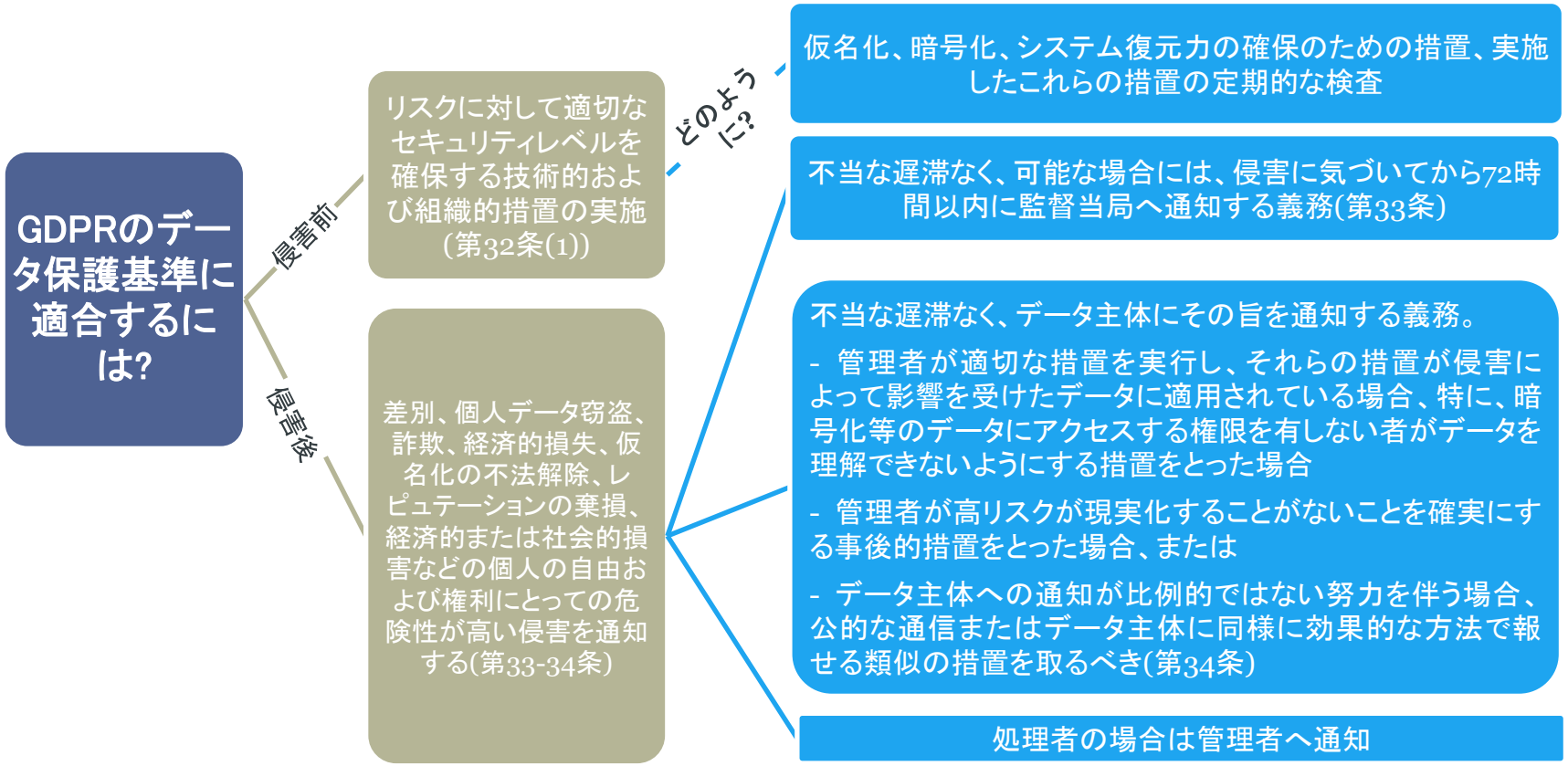
9. 処理のセキュリティ要件を満たしているか？

適切なセキュリティ対策の実施: セキュリティ・データマッピング

- ポイント：適切な処理のセキュリティ水準を確保することなしに、サイバーアタック等の個人データ漏えい事案を起こした場合、処理のセキュリティ水準の確保義務に反しGDPRに違反するとして制裁金を課せられるおそれがある。
- セキュリティ・データマッピング: GDPR32条に準拠したセキュリティ対策が講じられているかどうかについてのデータマッピング（データの棚卸し）作業
- セキュリティ違反によって欧州のデータ保護監督当局からデータ保護法違反に基づく制裁金決定を受ける可能性は現行のEUデータ保護指令の下でもあった。
- GDPR上の処理のセキュリティに関する管理者および処理者の義務は特に事業者にとって制裁金リスクが高いものと認識されていた。
- しかしながら、GDPR第32条（処理のセキュリティ）もGDPR前文83項も文言は抽象的であり、具体的に何を基準として対策をすればよいのかが不明確なままであった。
- 最近になってようやく、欧州におけるデータ保護監督当局・関係機関が定める個人データ処理のセキュリティに関するガイドラインが公表された。
  - THE CNIL'S GUIDES – 2018 EDITION SECURITY OF PERSONAL DATA（CNILガイド）（2018年4月に公表）
  - 個人データ処理のセキュリティに関するハンドブック（ENISAハンドブック）（2017年12月に公表）
- 個人データ侵害があった場合に処理のセキュリティに関する義務違反があったかなかったかについて比較的詳細な物差しが登場した以上、事業者として当該義務違反による制裁金リスクを低く抑えるためには、当局のガイドラインを踏まえて、個人データの処理のセキュリティに関する対策を取ることが必要である。

10. 個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？個人データ侵害通知マニュアルの作成

- ポイント：仮にサイバーアタックに遭い、個人データが漏えいした場合に、制限時間内に監督当局やデータ主体に通知できるように、個人データ侵害通知のマニュアルを作成し、トレーニングを行う。

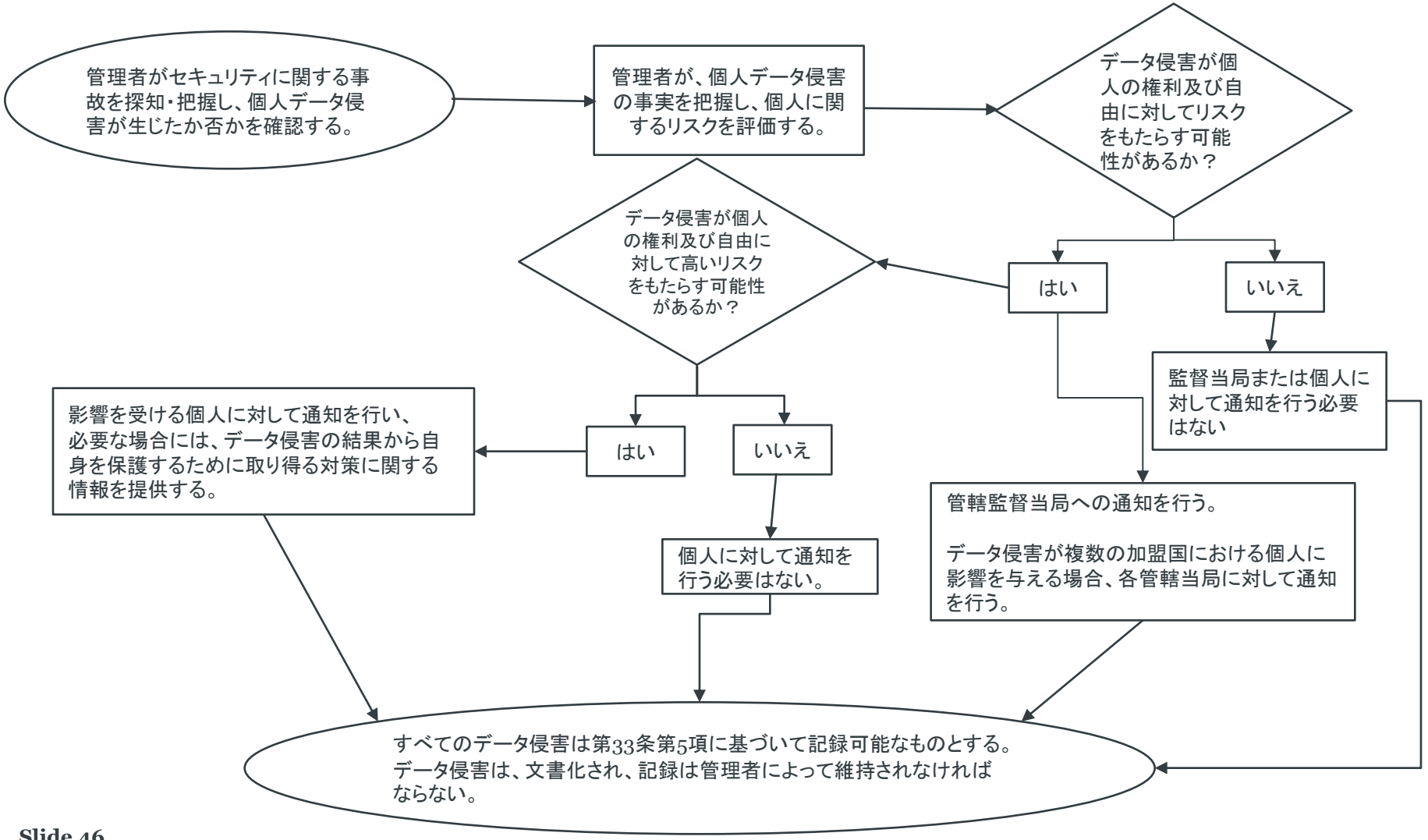


Bird & Bird

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？データ侵害に関するリスク評価において検討すべき要素

- **ポイント：個人データ侵害通知についてはEDPBのガイドラインが公表されており、それを踏まえて検討を行う。**
- 個人データの侵害が発生した場合、管理者は、不当な遅滞なく、可能であれば侵害を認識してから72時間以内に個人データの侵害を管轄監督当局に通知しなければならない。ただし、個人データの侵害が、**自然人の権利または自由に対してリスクを生じさせない場合を除く**（GDPR第33条第1項）。
- 個人データの侵害が**自然人の権利および自由に対して高いリスクを生じさせる可能性がある場合**、管理者は、不当に遅滞することなくデータ主体に対して個人データ侵害の事実を通知しなければならない（GDPR第34条第1項）。
- 一般的にデータ侵害のリスク評価においては、データ主体の権利及び自由に対するリスクの可能性および重大性について検討を行う必要がある（GDPR前文75項および76項）。リスクは、客観的な評価に基づいて行われるべきである。
- 考慮要素：
  - データ侵害の性質
  - 個人データの性質、センシティビティおよび量
  - 個人の識別に関する容易性
  - 個人に対する結果の重大性
  - 個人に関する特別な性質（例：子供または脆弱な個人）
  - 影響を受ける個人の数
  - 管理者の特別な性質（例：特別なカテゴリーの個人データを処理する医療機関）
- 一般的なポイント：データ侵害から生じる可能性のあるリスクを評価する場合、管理者は個人の権利および自由に対して生じ得る影響の重大性および影響の生じる可能性の組み合わせを検討しなければならない。データ侵害の結果がより重大であればリスクはより高く、同様に、影響が生じる可能性が大きければリスクも高まる。疑義がある場合には、管理者は慎重に対応して、通知を行うべきである。

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？通知義務に関するフローチャート



Bird & Bird

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？個人データ侵害の具体例と通知義務の有無

- ポイント：下記の具体例は、管理者が様々な個人データ侵害の場面において通知を行う必要性を判断するために有益である。これらの具体例は、個人の権利及び自由に対するリスクと高いリスクを区別するためにも有益といえる。
- ポイント：EDPBの個人データ侵害通知のガイドラインに記載されている具体例を参照する。

具体例	監督当局への通知が必要か？	データ主体への通知が必要か？	備考・推奨事項
i. 管理者は、個人データのアーカイブのバックアップを暗号化してCDに保存した。CDは、外部者が侵入した際に盗まれた。	不要。	不要。	個人データが最新技術（state of the art）のアルゴリズムによって暗号化されており、個人データのバックアップが存在し、固有のキーが侵害されていない限り、報告すべきデータ侵害とはならないと考えられる。もっとも、後に固有のキーが侵害を受けた場合、通知が必要となる。
ii. 個人データが、サイバー攻撃の際に管理者が管理する安全なウェブサイトから抽出された。管理者は、一つの加盟国において顧客を有している。	必要。個人に対して影響を及ぼす可能性がある場合、管轄監督当局の通知する。	必要。影響を受ける個人データの性質および個人が受ける可能性のある影響の重大性が高いか否かに応じて、個人に対して通知する。	リスクが高い場合、管理者は事案の状況に応じてデータ主体に対して通知を行うことをEDPBは推奨する。例えば、TV番組に関するニュースレターに関する守秘義務違反がある場合には通知は必要とされないと考えられるが、当該ニュースレターがデータ主体の政治的見解を開示することにつながる場合には通知が必要となると考えられる。
iii. 管理者のコール・センターにおいて数分間続いた短時間の停電によって、顧客が管理者に架電し、記録にアクセスすることができなかった。	不要。	不要。	本事案は通知すべき個人データ侵害ではないが、第33条第5項に基づいて記録する必要がある事故である。 適切な記録が管理者によって保管される必要がある。

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？個人データ侵害の具体例と通知義務の有無(2)

具体例	監督当局への通知が必要か？	データ主体への通知が必要か？	備考・推奨事項
iv. 管理者は、すべての個人データが暗号化されるランサムウェア攻撃を受けた。バックアップが利用できず、個人データは復元できない。調査において、ランサムウェアの機能は個人データを暗号化するだけであり、その他のマルウェアはシステムに存在しないことが明らかになった。	必要。個人データの利用可能性の喪失が生じることから個人に影響する可能性がある場合、管轄監督当局に対して通知を行う。	必要。影響を受ける個人データの性質および個人データの利用可能性に関して生じ得る影響やその他の発生し得る影響に応じて、個人に対して通知を行う。	バックアップが利用可能であり、適切な時間内に復元が可能である場合、個人データの利用可能性または機密性が永続的に失われるわけではないため、監督当局または個人に対する通知は必要ないと考えられる。もっとも、監督当局は、第32条に基づく広範なセキュリティ要件の遵守を評価するために調査を行うことを検討する可能性がある。
v. 個人が、銀行のコールセンターに対してデータ侵害について連絡を行った。個人は、他人の毎月の明細を受領している。 管理者は、短期の調査を行ったところ（24時間以内に完了）、個人データ侵害が発生しており、体系的なフローである場合には他の個人が影響を受けるまたはその可能性のあることについて合理的な確信をもって特定するに至った。	必要。	高いリスクがあり、その他の個人には影響しないことが明らかである場合、影響を受ける個人についてのみ通知を行う。	追加調査した後に、より多くの個人が影響を受けた事実が特定された場合、監督当局への追加の連絡を行う必要があり、他の個人に対する高いリスクがある場合には、管理者は他の個人に対して通知するための追加措置を行う。

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？個人データ侵害の具体例と通知義務の有無(3)

具体例	監督当局への通知が必要か？	データ主体への通知が必要か？	備考・推奨事項
vi. 複数国のオンライン・マーケットプレイスがサイバー攻撃を受け、ユーザー名、パスワードおよび購入履歴が攻撃者によってオンライン上に公開された。	必要。越境的な処理（cross-border processing）がなされている場合、主導監督当局に対して通知を行う。	必要。高いリスクをもたらす可能性があるため。	管理者は、措置を講じる必要がある（例えば、影響を受けるアカウントについてパスワードのリセットを強制すること、およびリスクを軽減するためのその他の措置）。
vii. ウェブサイト・ホスティング会社（データ処理者）がユーザーの承認を管理するコードに関してエラーを探知した。欠陥の影響によって、ユーザーは他のユーザーのアカウントの詳細にアクセス可能な状態になった。	処理者として、ウェブサイト・ホスティング会社は、影響を受ける依頼者（管理者）に対して不当に遅滞することなく通知しなければならない。 ウェブサイト・ホスティング会社が社内調査を実施することを前提とした場合、各管理者に関してデータ侵害が生じており、ホスティング会社（処理者）から通知を受け次第、各管理者は事実を認識するようになると考えられる可能性があることについて、影響を受ける管理者は合理的に確信を有しなければならない。管理者は監督当局に対して通知しなければならない。	個人に対する高いリスクがない場合、個人に対する通知は必要ない。	ウェブサイト・ホスティング会社（処理者）は、その他の通知義務について検討しなければならない（例：NIS指令に基づく通知義務）。 当該特定の管理者について脆弱性が不当に利用された証拠がない場合には、通知すべきデータ侵害は発生していないと考えられるが、記録すべき事項または第32条に関する不遵守事由に該当する可能性がある。

10.個人データ漏洩の場合への監督当局やデータ主体への通知は可能か？個人データ侵害の具体例と通知義務の有無(4)

具体例	監督当局への通知が必要か？	データ主体への通知が必要か？	備考・推奨事項
viii. 病院の医療記録が、サイバー攻撃によって30時間利用できない状態となった。	必要。患者の利益およびプライバシーに関する高いリスクが生じる可能性がある場合、病院は通知が義務付けられる。	必要。影響を受ける個人に通知する。	
ix. 5000名の生徒の個人データが、1000名以上が参加する誤ったメーリングリストに不注意によって送付された。	必要。監督当局に対する通知を行う。	必要。関係する個人データの範囲および種類ならびに生じ得る結果の重大性に応じて、個人に通知を行う。	
x. ダイレクト・マーケティング電子メールが「to」または「cc」の欄の受信者に送付され、それによって各受信者は他の受信者の電子メールアドレスを見ることができる。	必要。多くの個人が影響を受ける場合、センシティブ・データが明らかとになる場合（例：心理療法士のメーリングリスト）またはその他の要素が高いリスクを示す場合（例：電子メールが初期パスワードを含む）には、監督当局に対する通知が義務付けられる可能性がある。	必要。関係する個人データの範囲および種類ならびに生じ得る結果の重大性に応じて、個人に通知を行う。	センシティブ・データが明らかとならない場合で、かつ僅かな電子メールアドレスのみが明らかになる場合、通知は必要とはならないと考えられる。

11. データ保護影響評価の実施義務はないか？
データ保護影響評価（DPIA）とは？

- **ポイント：EDPBのデータ保護影響評価のガイドラインが公表されているため、当該ガイドラインを踏まえて対応を行う。**
- **データ保護影響評価**（Data Protection Impact Assessment: DPIA）**とは、データ処理の前に実施される個人データ保護に関する影響評価を意味し、データ処理（特に新しい技術を用いる処理）が個人の権利および自由対して高度のリスクをもたらす可能性がある場合に管理者が行うことが義務付けられるものである（第35条第1項）。**
- **データ保護影響評価は、以下の場合に特に必要となる（第35条第3項）。**
  - プロファイリングを含めた自動処理に基づいて自然人に関する個人的側面が体系的かつ広範囲に評価され、当該評価に基づいて自然人に関して法的効果を発生させまたは類似の重大な影響を及ぼす決定が行われる場合
  - 特別カテゴリの個人データまたは有罪判決および犯罪に関する個人データを大規模に処理する場合
  - 一般の人々がアクセス可能な空間において大規模な体系的監視を行う場合
- **監督当局は、データ保護影響評価が必要となる処理業務のリストおよびデータ保護影響評価が不要な処理業務のリストを作成し、EDPBに通知する。EDPBにより、データ保護影響評価に関するGDPRの一貫性のある適用が確保される。**
- **事前相談：管理者によるリスクを軽減する対策が講じられなければ処理が高度のリスクをもたらす可能性があることをデータ保護影響評価が示す場合、管理者は処理の前に監督当局と協議する必要がある（第36条）。**

11. データ保護影響評価の実施義務はないか？

どの処理業務に関してDPIAが必要となるか？

いつDPIAは義務的であるか？どのような場合に処理が「高度のリスクをもたらす可能性」があるか？

- ポイント：IoT装置による個人データ処理についてはDPIAの実施義務ありと判定されやすい基準となっている。DPIAは、実行後に当局への事前相談が必要となるケースがあり、IoTの新製品のローンチのタイミングに大きく影響を与える可能性がある。
- ポイント：EDPBのDPIAのガイドラインにおいて挙げられる下の9項目のうちの2項目に該当するにもかかわらず、「高度のリスクが生じる可能性」はないと考える場合、当該管理者はDPIAを実施しない理由を十分に書面化する必要がある。

1. 評価またはスコアリング
2. 法的効果または類似の重大な影響を伴う自動的な意思決定
3. 体系的な監視
4. センシティブなデータまたは非常に個人的な性質を有するデータ
5. 大規模なデータ処理
6. データのセットのマッチングまたは結合
7. 脆弱なデータ主体に関するデータ
8. 新しい技術的若しくは組織的な解決方法の革新的な利用または適用
9. 処理自体がデータ主体が権利を行使しまたはサービスを利用し若しくは契約を行うことを妨げること

- DPIAが必要な高いリスクのある処理行為については監督当局が続々とブラックリストを公表しているため、追加で、各国別のブラックリストに該当する処理行為についてもDPIAを行う必要がある。

11. データ保護影響評価の実施義務はないか？

「自然人の権利及び自由に対する高度のリスクをもたらす可能性」がある場合

1. 評価またはスコアリング

- データ主体の職場での実績、経済的状況、健康、個人的嗜好又は関心、信頼性又は行動、居場所又は移動に関する側面から特に行われるプロファイリング及び予測が含まれる。例えば、信用照会データベースまたはマネーロンダリング、テロリストによる資金調達に対する対策もしくは詐欺行為に関するデータベースで消費者を審査する金融機関、病気・健康リスクを評価及び予測するために消費者に対して遺伝子テストを直接提供するバイオテクノロジー企業が挙げられる。

2. 法的効果または類似の重大な影響を伴う自動的な意思決定

- 例えば、処理が個人の排除又は差別を生じさせる可能性がある場合が個人に与える影響として問題となり、僅かな影響を及ぼす又は全く影響がない処理は、この基準には該当しない。

3. 体系的な監視

- データ主体の観察、監視又は支配のために使用される処理であり、ネットワークまたは一般の人々がアクセス可能な空間に関する体系的な監視を通じて収集されたデータが含まれる。

11. データ保護影響評価の実施義務はないか？

「自然人の権利及び自由に対する高度のリスクをもたらす可能性」がある場合(2)

4. センシティブなデータまたは非常に個人的な性質を有するデータ

- 有罪判決又は犯罪に関連する個人データのみならず特別カテゴリの個人データ（例えば、人種または民族的素性に関するデータ、個人の政治的意見に関するデータ、医療データ等）が含まれる。また、家庭および私的な活動に関連する個人データも含まれる（例えば、個人的な文書、電子メール、日記、メモ帳機能を有する電子書籍リーダーにおけるメモ、ライフ記録のためのアプリケーションに含まれる非常に個人的な情報等が含まれる）。

5. 大規模なデータ処理

- 大規模であるか否かに関する明確な定義はないが、関係するデータ主体の数、処理されるデータの量・範囲、データ処理活動の期間、処理活動の地理的範囲等によって判断される。

6. データのセットのマッチングまたは結合

- 例えば、データ主体の合理的な期待を超える方法において、異なる目的及び/又は異なるデータ処理者によって行われる2つ又はそれ以上のデータ処理業務に起因するものが挙げられる。

11. データ保護影響評価の実施義務はないか？

「自然人の権利及び自由に対する高度のリスクをもたらす可能性」がある場合(3)

7. 脆弱なデータ主体に関するデータ

- 個人が自己のデータの処理に対して同意又は異議を述べることができない可能性があるという意味において、データ主体及びデータ処理者の間において力関係の不均衡が存在する場合が想定されている（例えば、子供や従業員）。また、例えば、老人、患者等のような人間社会におけるより脆弱なセグメントのデータ主体も該当する可能性がある。

8. 新しい技術的若しくは組織的な解決方法の革新的な利用または適用

- 例えば、アクセス制御のための指紋及び顔認証を組み合わせて使用すること、いわゆるInternet of Thingsに係る技術の適用が挙げられる。

9. 処理自体がデータ主体が権利を行使しまたはサービスを利用し若しくは契約を行うことを妨げること

- 例えば、消費者に対して融資を行うか否かを決定するために信用照会データベースにより消費者を審査する銀行が挙げられる。

11. データ保護影響評価の実施義務はないか？

DPIAの要否の判断に関する具体例

処理の具体例	関連する可能性のある基準	DPIAは必要か？
患者の遺伝子および健康データを処理する病院（病院の情報システム）	• センシティブデータまたは非常に個人的な性質を有するデータ • 脆弱なデータ主体に関するデータ • 大規模なデータ処理	必要
高速道路上の運転行動を監視するためのカメラシステムの使用。管理者は、情報処理機能のあるビデオ分析システムを車の特定および車のナンバープレートの自動識別を行うために使用することを想定している。	• 体系的なモニタリング • 技術的若しくは組織的な解決方法の革新的な利用または適用	
従業員のオフィス、インターネット上の操作等を含む従業員の活動の体系的な監視を行う企業	• 体系的なモニタリング • 脆弱なデータ主体に関するデータ	
プロフィールを作成するための公のソーシャルメディアのデータの収集	• 評価またはスコアリング • 大規模なデータ処理 • データのセットのマッチングまたは結合 • センシティブデータまたは非常に個人的な性質を有するデータ	
国レベルで与信評価または詐欺行為に関するデータベースを作成する機関	• 評価またはスコアリング • 法的効果または類似の重大な影響を伴う自動的な意思決定 • 処理自体がデータ主体が権利を行使しまたはサービスを利用し若しくは契約を行うことを妨げること • センシティブデータまたは非常に個人的な性質を有するデータ	
研究プロジェクトまたは臨床治験における脆弱なデータ主体に関する仮名化されたセンシティブな個人データのアーカイブ目的での保存	• センシティブデータ • 脆弱なデータ主体に関するデータ • 処理自体がデータ主体が権利を行使しまたはサービスを利用し若しくは契約を行うことを妨げること	
医師、その他の医療専門家または弁護士による患者または依頼者から提供を受けた個人データの処理（GDPR前文91項）	• センシティブデータまたは非常に個人的な性質を有するデータ • 脆弱なデータ主体に関するデータ	必要ない
購読者に対して一般的な日々のダイジェスト版を送付するためにメーリングリストを使用するオンライン雑誌	• 大規模なデータ処理	
ウェブサイトの特定の場所において閲覧または購入された商品に基づく限定的なプロファイリングを伴う古い型の自動車部品のための宣伝を表示するeコマースのウェブサイト	• 評価またはスコアリング	

12. データ保護責任者の選任義務はあるか？誰を選任するか？
データ保護責任者(DPO):意義、任務、選任、地位

- DPOの意義
  - DPOとは、GDPRの内部における遵守を監視するために、管理者または処理者を支援するために専任されるデータ保護法およびその実務に関する専門知識を有するものとして専任される者
- DPOの任務
  - 少なくとも第39条第1項に列挙されたタスク、例えば、GDPRおよびその他のEUおよび加盟国の条項に基づく義務について管理者・処理者および個人データを処理する従業員に対し情報と助言を提供すること、管理者・処理者の個人データ保護方針の遵守を監視すること等を行うこと
- DPOの選任
  - 専門家としての質、特にデータ保護法およびその実務の専門知識ならびに任務を遂行する技量に基づいて選任されるものとする(IAPP(国際プライバシー専門家協会)のCIPP/EはGDPRを含むEUデータ保護法の専門知識を有することを示すものであり国際的に認められている資格である)。管理者または処理者の従業員、または業務委託契約に基づいて任務を遂行するものでもよい。
- DPOの地位
  - 管理者・処理者は、DPOが個人データ保護に関する一切の事柄について適切、適時に取り組むことを確保。
  - 管理者・処理者はDPOが任務の遂行に係わる指示を一切受けないことを確実にしなければならない。DPOは当該任務の遂行について管理者・処理者から解雇または処罰を課されないものとする
  - DPOは、管理者または処理者の最高経営レベルに直接報告を行なうものとする。
  - DPOは、その他の任務や義務も遂行できるものとする。管理者または処理者は、そのような任務や義務が利益相反にならないよう確実にしなければならない。

12. データ保護責任者の選任義務はあるか？誰を選任するか？
選任義務の有無をチェックする

- 管理者および処理者は、次のいずれかの要件を満たす場合にはDPOの選任義務あり
  - 処理が公的機関または団体によって行われる場合（但し、司法権に基づく裁判所の行為を除く）
  - 管理者または処理者の中心的業務が、その性質、適用範囲および/または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする作業である場合
  - 管理者または処理者の中心的業務が、第9条で言及された特別カテゴリーの個人データまたは第10条で定める有罪判決および犯罪に関する個人データを大規模に処理する場合、または
  - EUまたは加盟国の法律(例:ドイツ)でDPOの選任が義務付けられている。
    - 2017年7月、GDPR施行のための新ドイツ連邦データ保護法が成立した。DPOの選任に関して、個人データの自動的処理に関して少なくとも10名の従業員を雇用する企業は、DPOを選任する義務を負う。管理者および処理者は、GDPR第35条に基づくデータ保護影響評価が必要な処理を行う場合、DPOを選任しなければならない。これは個人データが商業上のデータ移転またはマーケティングもしくは市場調査の目的で行われる場合にも当てはまる。
    - 欧州でビジネスを行う日本企業の欧州拠点の多くは、GDPR上のDPOの選任義務を負うことになる可能性が高い。

12. データ保護責任者の選任義務はあるか？誰を選任するか？
「中心的業務」(core activities)(第37条第1項(b)(c))

- EDPBのデータ保護責任者に関するガイドライン(WP243)6頁
- 「中心的業務」ー考慮要素
  - 管理者のまたは処理者の目的を達成するための重要な業務
- 「中心的業務」ー例
  - 患者の健康記録等の健康データの処理は病院の中心的業務の一つであると考えられ、病院はデータ保護責任者を選任する義務がある
  - 「組織の中心的業務または主要な事業のために必要なサポート機能」は通常「中心的業務」ではなく付随的機能と考えられる。
    - 従業員への支払いを行うことおよび標準的なITサポート業務を持つこと等のサポート業務は全ての組織が実行するものである。

12. データ保護責任者の選任義務はあるか？誰を選任するか？「大規模に」(large scale)(第37条第1項(b)(c))

- EDPBのデータ保護責任者に関するガイドライン(WP243)7頁
- 「大規模に」－考慮要素
  - 関係するデータ主体の数（個別の数または関連する人口の中の割合）
  - 処理されるデータの量および/または異なるデータの項目の範囲
  - データ処理活動の期間または永続性
  - 処理活動の地理的程度
- 「大規模に」－例
  - 病院による通常業務における患者データの処理
  - 街中の公共交通システムを使用する個人のトラベルデータの処理（トラベルカードを通じた追跡）
  - 保険会社または銀行による通常業務における顧客データの処理
  - 検索エンジンによる行動広告のための個人データの処理
  - 電話またはインターネットサービスプロバイダーによるデータ（コンテンツ、トラフィック、位置）の処理

12. データ保護責任者の選任義務はあるか？誰を選任するか？
「定期的かつ系統的な監視」(regular and systematic monitoring)（第37条第1項(b)）

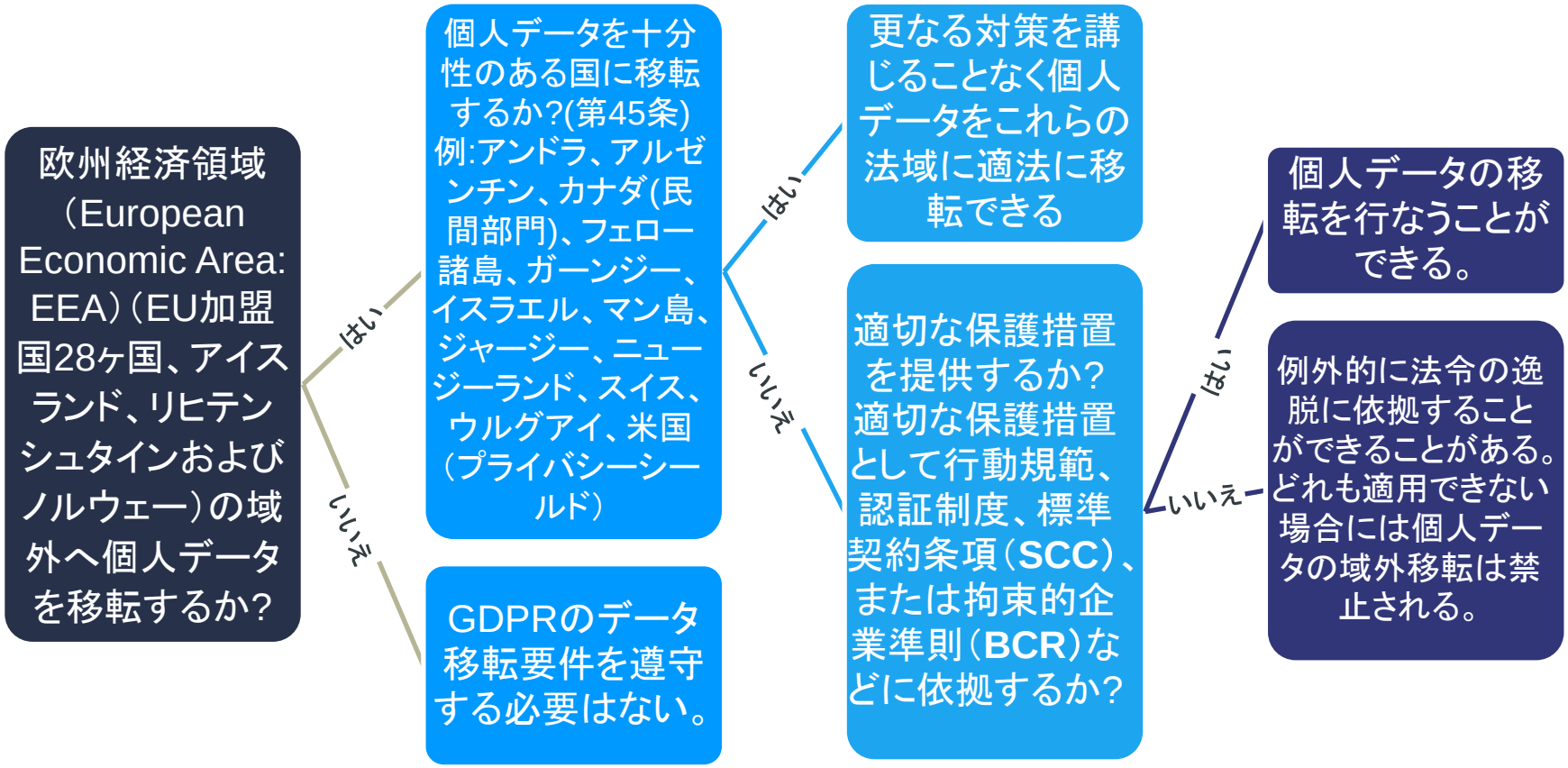
- EDPBのデータ保護責任者に関するガイドライン(WP243)8頁
- 行動広告を目的とするものを含む、インターネット上の追跡およびプロファイリングのあらゆる形式のものを含むが、「監視」はオンライン環境に限定されない
- 「定期的」とは以下のいずれか一つまたは複数を意味する
  - 現在進行中の、または特定期間に特定の間隔で生じること
  - 繰り返し起こるまたは定刻に繰り返された
  - 何度もまたは周期的に起こっている
- 「系統的」とは以下のいずれか一つまたは複数を意味する
  - システムによって生じる
  - 所定の、整理されたまたは秩序だった
  - データ収集の一般的な計画の一部として生じる
  - 戦略の一部として実行された
- 例：電気通信ネットワークの運営、電気通信サービスの提供、Eメールの再標的化、データドリブンマーケティング活動、リスク評価の目的でのプロファイリングおよび採点法（例えば、信用度採点、保険料の制定、詐欺防止、マネーロンダリングの検知の目的）、例えば携帯アプリによる位置追跡、ロイヤリティプログラム、行動広告、ウェアラブル端末によるウェルネス、フィットネスおよび健康データの監視、有線テレビ、スマートメーター、スマートカー、ホーム・オートメーション等の接続機器

12. データ保護責任者の選任義務はあるか？誰を選任するか？
どこの誰をDPOとして選任できるかを検討する

- DPOの選任の条件
  - DPOは効率的にデータ主体と連絡しおよび関係する監督当局と協力する立場にいなければならない。この連絡は、関係する監督当局およびデータ主体が使う言語によって行われなければならない。
  - EDPBのDPOのガイドラインによればDPOはEU内において設置することが望ましいとされているが、DPOのあまりにも強力な独立性と地位は、データ保護の論点に関するDPOの意見によってビジネスに無用な支障が生じることにつながりかねない。DPOの人選には慎重を期すことが望ましい。
  - 日本本社においてDPOを選任し、DPOのチームの一員としてのサポートチームを欧州内に設置することで、欧州のデータ保護監督当局やデータ主体へのアクセスの容易性を確保することが、GDPR適用開始から暫くの間は、DPOに起因するGDPRのリスクを最小化する上で有効な方策ではないかと考える。
- 利益相反
  - DPOは個人データの処理の目的や方法を決定する組織上の地位を有することはできない。組織毎に個別の組織構造であることから、この点はケースバイケースで検討されなければならない。
  - 利益相反のある地位は、シニアマネジメントの地位（例えば、CEO、COO、CFO、CMO (Chief Medical Officer)、マーケティング部門長、人事部長またはIT部門長）や他の組織構造上の下位の役割（上記地位や上記役割が処理の目的や手段を決定することにつながる場合）
- **欧州のデータ保護監督当局に対するDPOの連絡先の通知義務**
  - **当局毎に連絡先の通知フォームが異なるため、個別にチェックする必要がある。**

3. 個人データの移転の主なチェック項目

個人データ移転規制：概要



Bird & Bird

データ移転のツールの概要

- 産業界の取り組みとしては、GDPR対策として、SCCを利用することでGDPR上の個人データの域外移転規制対策を行っている。
- 産業界の課題は、GDPR適用開始までにSCCまたは／およびBCRを利用したGDPR対策を完了させることである。大企業においては対策は進みつつあるが、中小企業にはGDPRの順守には荷が重い状況
- EUのデータ保護の分野では、データ保護のアクティビストによって十分性認定の有効性がEU裁判所で争われることが珍しくなく、産業界としては十分性認定が無効となるリスクも念頭に置く必要がある。

法的根拠	説明
標準契約条項 SCC（Standard Contractual Clauses）	**欧州委員会が決定したデータ移転契約のひな型で、個人データの移転をGDPR上適法化するためのものである。日本の産業界の多くの企業は、GDPR上のデータ移転規制に、SCCを締結することにより対応を行っている。**
拘束的企業準則 BCR（Binding Corporate Rules）	**楽天株式会社がルクセンブルグの監督当局からBCR承認取得済み。株式会社インターネット・イニシアティブ（IIJ）は英国の監督当局に申請中。**
EU-米国プライバシー・シールド Privacy Shield	プライバシー・シールドは、EUから米国へのデータ移転のみに利用可能である。プライバシー・シールドの有効性についてEU裁判所で争われた。欧州議会は、2018年7月、米国がプライバシー・シールドに関して2018年9月1日までに改善を図らなければSuspendすることを発表した。
十分性認定の取得 Adequacy Decision	日本の十分性認定がなされてもEEA外であって十分性認定を受けていない国・地域へのEEAデータの域外移転については適切な保護措置の提供が必要である。例えば、日本企業のフランス子会社からインド子会社へのデータ移転は十分性認定によって適法化されない。 **また、日本の十分性認定後に、データ保護のアクティビストによって日本の十分性認定の有効性がEU裁判所で争われるリスクも念頭において、十分性認定の交渉に臨むことが望ましいと考えられる（実際にEU-米国セーフハーバー決定は2015年10月にEU司法裁判所で無効判決が下された）。**
認証 Certification	認証機関の枠組みがまだ決まっていない。現状、産業界において利用できる状況にない。
行動規範 Code of Conducts	行動規範の枠組みがまだ決まっていない。現状、産業界において利用できる状況にない。

個人データの移転規制の主なチェック項目

1. 標準契約条項（Standard Contractual Clauses: SCC）を締結しているか？締結するのに必要な情報は何か？
   - ① EEA域外への個人データの移転の目的は何か？
   - ② データ主体は？
   - ③ データの種類は？
   - ④ 受領者または受領者のカテゴリー
   - ⑤ センシティブデータの有無
   - ⑥ 個人データの処理行為を監督当局へ登録したか。
   - ⑦ 追加の有益な情報（保管期間の限定および他の関連情報）
2. 事業者グループのEEA内拠点からどこへの移転か？
   - ① 事業者グループ内のEEA外拠点
     - ① データ輸出者（事業者グループEEA内拠点）は管理者？処理者？
   - ② 事業者グループ外のEEA外拠点：データ輸入者（事業者グループ内外のEEA外拠点）は？

標準契約条項を締結しているか？
ANNEX B – 移転の詳細

- 2004年SCC（管理者–管理者）を締結するためには以下の情報を収集する必要がある。
  - データ主体 - 移転される個人データは、以下のカテゴリーのデータ主体に関するものである：
  - 移転の目的 – 移転は、以下の目的で行われる:
  - データのカテゴリー - 移転される個人データは、以下のカテゴリーのデータに関するものである：
  - 受領者 - 移転される個人データは、以下のカテゴリーの受領者に限り、開示することができる：
  - センシティブ・データ（該当する場合）- 移転される個人データは、以下のカテゴリーのセンシティブ・データに関するものである。
  - データ輸出者のデータ保護登録情報（該当する場合）
  - その他の参考情報（保管の上限及びその他関連情報）
  - データ保護に関する質問の担当窓口

事業者グループのEEA内拠点からどこへの移転か？
標準契約条項（SCC）

- SCCとは、欧州委員会によって決定された契約書の雛形であり、二当事者間でこの雛形を使ってデータ移転契約を締結することで適切な保護措置を提供し、適法なデータ移転を行うものである。現時点で利用可能なSCCは管理者−管理者SCCが2つ、管理者−処理者SCCが1つの計3つある。
- SCCは、単に署名をしさえすれば後は保管しておけば良いという性質のものではなく、SCC中のデータ輸出者とデータ輸入者の義務をそれぞれ履行できる体制を整えることが肝要である。
- 処理者−復処理者のSCCはまだ存在しない（EDPBが提案したSCC案のみ）

輸出者	輸入者	状況	現在のSCCのセット
管理者	管理者	個人データがEU内の管理者からEU外の管理者へ移転される場合	2セットのSCCがある ▪2001年SCC(EC Decision 2001/497/EC) ▪2004年SCC(EC Decision 2004/915/EC)
管理者	処理者	個人データがEU内の管理者からEU外の処理者へ移転される場合	▪ 2010年SCC(EC Decision 2001/87/EC)
処理者	復処理者	個人データが、まずEU内で管理者から処理者へ移転され、その後、その処理者からEU外にいる復処理者へ移転される場合	EDPBは2014年3月、処理者-復処理者SCC案を提案した(WP214)。しかし、欧州委員会はこれをまだ承認していない。

2004年管理者-管理者SCC

II. データ輸入者の義務

データ輸入者は、以下を保証し、約束する。

a) 個人データを偶発的又は違法な破壊、偶発的な喪失、変更、不正開示又はアクセスから保護するための適切な技術的対策及び組織的対策を講じ、処理及び処理されるデータの本質により生じるリスクを回避できるよう適切なレベルのセキュリティを提供すること。

b) データ輸出者が個人データへのアクセス権限を付与する第三者（処理者を含む。）が個人データの秘密及びセキュリティーを尊重及び保持できるような手続きを構築すること。データ輸入者の権限に基づき行為する者（データ処理者を含む。）は、もっぱら当該データ輸入者の指示に基づき個人データの処理を行う義務を負うものとする。ただし、本条項は、法律又は規則により、個人データへのアクセス権限を付与され、又は個人データへのアクセスが要求される者には適用されない。

c) 本契約条項を締結する時点で、本契約条項で定められた保証に実質的に悪影響を及ぼしうる地域法が存在すると信じる理由はないこと。また、かかる法律を認識するに至った場合は、データ輸出者に通知すること（データ輸出者は、要請に応じて当該通知を当局に伝える。）。

d) 付属書類 B に記載された目的のために個人データを処理すること。また、本契約条項に規定された保証を行う法的権限及び本契約条項に規定された義務を履行する法的権限を有すること。

e) 個人データの処理に関する質問に回答する権限を有するデータ輸入者の担当窓口を、データ輸出者に明らかにすること。また、かかる全ての質問に関し、合理的期間内に、データ輸出者、データ主体及び当局と誠実に協力すること。データ輸出者が解散した場合、又は両当事者が合意した場合、データ輸入者は、第 I 条(e)項の条項を遵守する責任を負う。

2004年管理者-管理者SCC

II. データ輸入者の義務

f) データ輸出者の要請に応じ、第III条に基づく責任を履行するのに必要な財源を有する証拠をデータ輸出者に提供すること（保険の保障内容を含みうる。）。

g) データ輸出者の合理的要請に応じ、本契約条項に規定されている保証及び義務の遵守を確認するため、データ輸出者（又は、データ輸出者が選定する独立したもしくは公平な検査機関もしくは監査人であり、データ輸入者から合理的な異議申し立てがされていない者）が合理的な通知をした上で、通常の営業時間内に実施する調査、監査及び／又は確認のために、処理に必要なデータ処理設備、データ・ファイル及びドキュメンテーションを提出すること。上記要請を行うには、データ輸入者の国内の規制当局又は監督当局から、同意又は承認を受ける必要がある場合はそれに従い、データ輸入者は、かかる同意又は承認を適時に取得するよう努める。

h) データ輸入者は、自身の選択により、以下のいずれかに従って個人データを処理すること。

i. データ輸出者が設立された国におけるデータ保護法令。又は、

ii. Directive 95/46/EC の第 25 条 6 項に基づく欧州委員会決定の関連条項（データ輸入者が、かかる認定又は決定の関連条項を遵守し、かかる認定又は決定に関係する国を拠点としているが、個人データの移転に関しては、かかる認定又は決定の対象に含まれていない場合2。）。

iii. 付属書類 A に規定されたデータ処理方針。

データ輸入者は、いずれの選択肢を選択するか示すこと：.....

データ輸入者のイニシャル：.....;

i) 欧州経済領域（European Economic Area（EEA））の外に拠点を置く第三者データ管理者に対し、個人データを開示又は移転しないこと。ただし、データ輸入者がデータ輸出者に対して当該移転に関する通知を行い、かつ、以下のいずれかに該当する事由が存在する場合を除く。

i. 当該第三者データ管理者が、第三国が十分な保護措置を講じているという欧州委員会の決定に従い、個人データを処理すること。

ii. 当該第三者データ管理者が、本契約条項又はその他のデータ移転契約（EU の管轄当局の承認を受けたもの）の署名者になること。

iii. データ主体が、当該移転の目的、受領者のカテゴリー及びデータの輸出先となる国に異なるデータ保護基準が存在する可能性があるという事実の通知を受けた上で、異議を述べる機会が付与されたこと。又は、

iv. センシティブ・データの転送に関して、データ主体が当該転送について、明確な同意を与えたこと。

2010年管理者-処理者SCC

第5条　データ輸入者の義務

データ輸入者は、以下に同意し、以下を保証する。

(a) 個人データの処理を、データ輸出者のためにのみ、データ輸出者の指示及び本契約条項に従って行うこと。何らかの理由により上記を遵守することができない場合、データ輸入者は、すみやかにデータ輸出者に通知することに同意する。この場合、データ輸出者は、データ移転を一時停止する権利及び／又は本契約を解除する権利を有する。

(b) データ輸入者に適用される法令により、データ輸出者からの指示の遂行及び本契約に基づく自身の義務の履行が妨げられると信じる理由は存在しないこと。また、本契約条項に規定された保証及び義務に実質的に悪影響を及ぼすおそれのある上記法令への変更が行われた場合、データ輸入者は、当該変更を認識した後すみやかに、データ輸出者に対して当該変更を通知すること。この場合、当該データ輸出者は、データ移転を一時停止する権利及び／又は本契約を解除する権利を有する。

(c) 移転された個人データの処理を行う前に、付属書類 2 で特定される技術的及び組織的セキュリティ対策を講じていること。

(d) 以下について、データ輸出者にすみやかに通知すること。

(i) 法執行機関から、法的拘束力を有する個人データの開示要請を受けた場合。ただし、通知を行うことが禁止されている場合（例えば、刑法に基づく法執行機関の捜査の秘密性を維持するための禁止）を
除く。

(ii) 偶発的又は不正アクセス。

(iii) データ主体から直接受けた要請（通知以前に（要請への）対応を行わない）。ただし、対応することが認められている場合を除く。

(e) 移転の対象である個人データの処理に関するデータ輸出者からの全ての質問を、迅速かつ適切に処理すること。また、移転されたデータの処理に関する監督当局からの助言に従うこと。

(f) データ輸出者の要請に応じ、データ輸出者又は検査機関（監督当局との合意により（該当する場合）、データ輸出者により選定された、独立性及び必要とされる専門的資格を有し、秘密保持義務に拘束されるメンバーにより構成される。）が実施する、本契約条項の対象となる処理活動の監査のためにデータ処理設備を提供すること。

(g) 要請に応じ、データ主体に対し、本契約条項又はデータの復処理に関する既存の契約書のコピー1 部を提供すること（ただし、本契約条項又は上記復処理契約に商業上の情報が含まれる場合は、当該商業上の情報を除外することができる）。ただし、付属書類 2 については、データ主体がそのコピーをデータ輸出者から入手できない場合は、セキュリティ対策の概要で代替するものとする。

(h) データの復処理が行われる場合、事前にデータ輸出者に通知し、事前の書面による同意を取得していること。

(i) 復処理者による処理サービスが、本契約条項の第 11 条に従い実施されること。

(j) 本契約条項に基づき締結されたデータの復処理契約書のコピー1部を、すみやかにデータ輸出者に送付すること。

2010年管理者-処理者SCC

第11条　復処理

1. データ輸入者は、データ輸出者の事前の書面による同意がある場合を除き、本契約条項に基づきデータ輸入者がデータ輸出者のために履行する処理業務を委託しないものとする。データ輸入者が、データ輸出者の同意を得て本契約条項に基づく自身の義務を委託する場合、データ輸入者は、本契約に基づきデータ輸入者に課されるものと同一の義務を復処理者に課す契約を書面で締結することによってのみ、かかる復処理の委託を行うものとする（脚注3：この要件は、本決定に基づきデータ輸出者とデータ輸入者との間で締結された契約に、復処理者が連署する方法でも満たすことができる。）。復処理者が、かかる書面による契約に基づくデータ保護義務の履行を怠った場合、データ輸入者は、当該契約に基づく復処理者の義務の履行について、データ輸出者に対し完全に責任を負うものとする。

2. データ輸出者又はデータ輸入者が事実上消滅し、もしくは法律上存在しなくなった場合、又はこれらの双方が支払不能に陥った場合で、かつ契約又は法律によりデータ輸出者又はデータ輸入者の法的義務を全て引き受ける承継人が存在しないため、データ主体が第6条1項に規定された損害賠償の請求をデータ輸出者又はデータ輸入者に対して行うことができない場合に備え、データ輸入者と復処理者との間の事前の書面による契約には、第3条に定められている第三受益者条項を規定するものとする。かかる復処理者の第三者に対する法的責任は、本契約条項に基づく自身の処理業務に限定されるものとする。

3. 第1項で言及される、契約に基づく復処理におけるデータ保護の観点に関する規定は、データ輸出者が設立されたEU加盟国、すなわち
……の法律に準拠するものとする。

4. データ輸出者は、本契約に基づき締結され、第5条(j)項に基づきデータ輸入者から通知された復処理契約のリストを保管するものとする。同リストは、少なくとも1年に1回の更新が行われるものとする。同リストは、データ輸出者のデータ保護監督当局も入手することできるものとする。

2010年管理者-処理者SCC

標準契約条項の付属書類1

- データ輸出者

データ輸出者は、（本件移転に関するデータ輸出者の活動を簡潔に記載してください。）

- データ輸入者

データ輸入者は、（本件移転に関するデータ輸出者の活動を簡潔に記載してください。）。

- データ主体

移転される個人情報は、以下のカテゴリーのデータ主体に関するものである（明記してください。）。

- データのカテゴリー

移転される個人データは、以下のデータカテゴリーに関するものである（明記してください。）。

- 特別カテゴリーのデータ（該当する場合）

移転される個人データは、以下のデータの特別カテゴリーに関するものである（明記してください。）。

- 処理業務

移転された個人情報は、以下の基本的な処理活動の対象となる（明記してください。）。

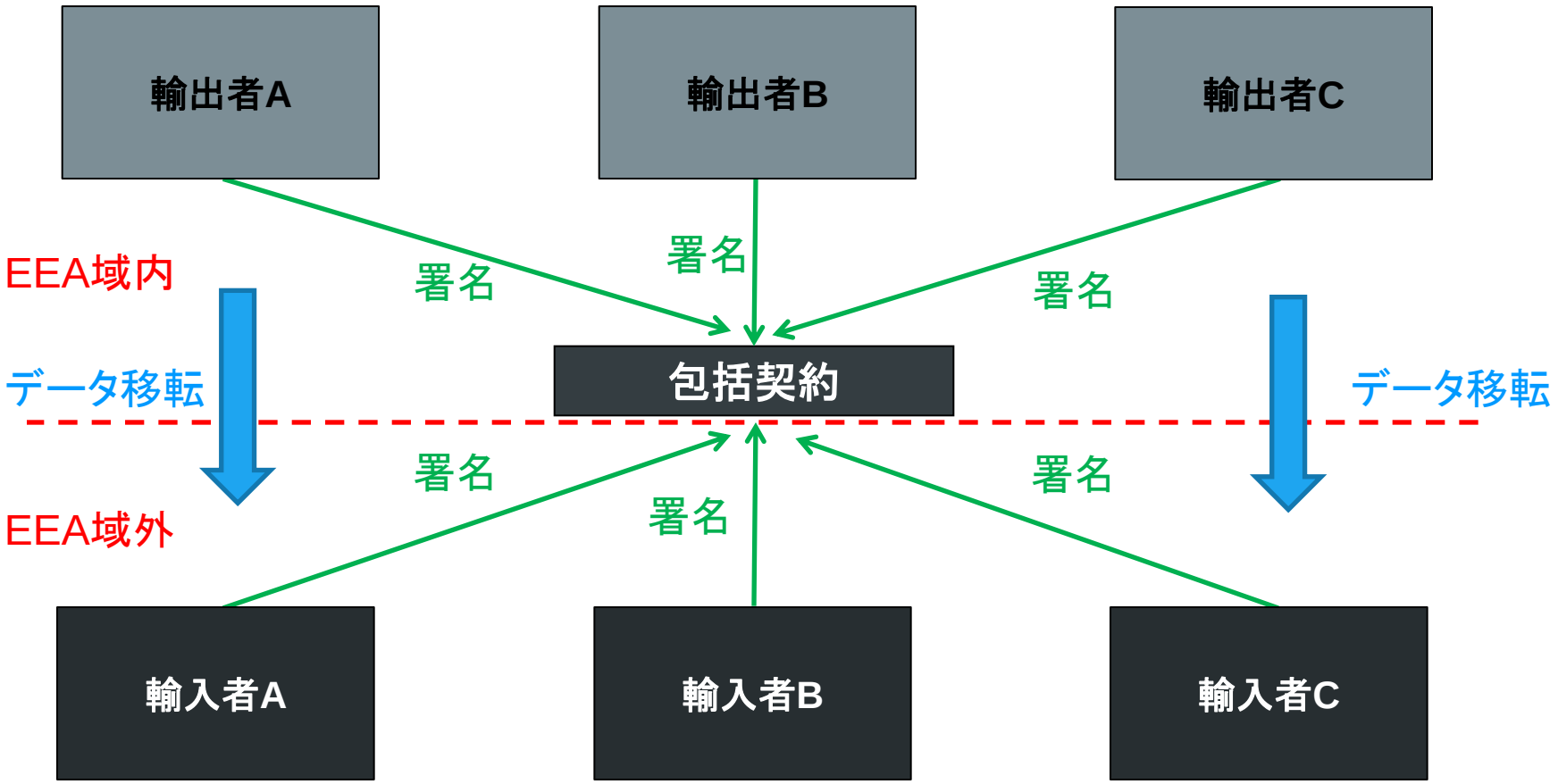
2010年管理者-処理者SCC

標準契約条項の付属書類２

- 本付属書類は、本契約条項の一部を構成する。両当事者は、本付属書類の全項目に必要事項を記入の上、これに署名しなければならない。
- 第 4 条(d)項及び第 5 条(c)項に従い、データ輸入者により講じられた技術的及び組織的セキュリティ対策の説明（又は文書／法律を添付）:

複数当事者間のデータ移転①

SCCを多数当事者間契約として締結する

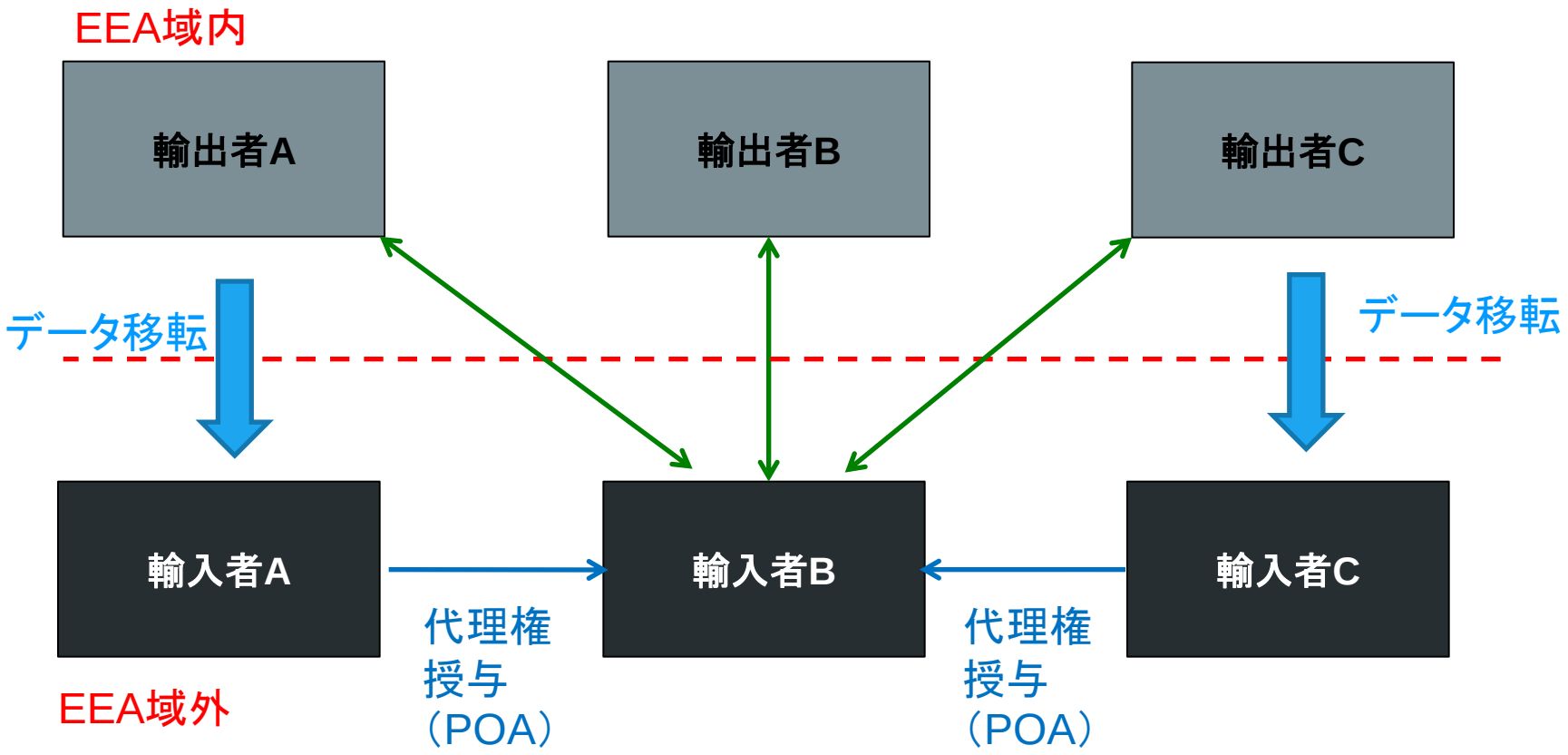


SCC中のデータ輸入者の義務を履行するべく社内体制の構築をEEA外を含む日本本社においても推進

Bird & Bird

複数当事者間のデータ移転②

EEA内は個別にSCCを締結、EEA外の拠点は代理権授与方式



SCC中のデータ輸入者の義務を履行するべく社内体制の構築をEEA外を含む日本本社においても推進

Bird & Bird

III. GDPR対応の具体的成果物

GDPR対応の具体的成果物

プライバシーポリシー

- **GDPR上、管理者がどのようにGDPRを守るのかについての方針を明らかにする、データ保護方針の一部として説明責任の一環として持つことが要求されると考えられる。**
  - GDPR上の管理者の義務に対応した項目を網羅する。
- **GDPR上、管理者は、データ主体に対して情報を提供しなければならない。「簡潔で、透明性があり、かつ容易にアクセス可能な形式」**
- **GDPRにおける強化された開示要件（GDPR第13条、第14条の情報通知義務に対応する）**
  - 誰が個人データに対して責任を負うか？
  - どのような個人データを収集するか。
  - 他の人々に関する情報
  - 個人データをどのように収集するか。
  - 個人データを提供し損ねた場合には。
  - 個人データを使って何をするか（処理の目的）
  - 個人データを処理する法的根拠は何か
  - 個人データをどこへ送るか／誰がその情報にアクセスを持つか
  - 個人データのセキュリティ
  - 個人の権利
  - 同意を撤回する権利
  - 個人データをどの程度の期間保持するか
  - DPOがいる場合にはその特定

GDPR対応の具体的成果物

個人データ侵害の通知のためのプロトコル（例）

I. 導入

- **プロトコルの対象の定義：本社およびグループ企業**
- **「個人データ侵害」の定義**

II. 範囲

- **全ての従業員は個人データの処理に関して特定された事故をプライバシーチームに報告する。**
- **プライバシーチームの定義**

III. 管理者の場合

- **「プライバシーチーム」の役割：ITセキュリティチームとの協働、データ保護責任者が通知および相談を受けることの確保**
- **プライバシーチームが、個人データ侵害が、データ主体の権利および自由に対してリスクを持つか、またそのリスクが高いかを、できるだけ速やかに評価する。**
  - リスクがある→データ保護監督当局へ報告
  - どのように、何を当局に報告すべきか（Schedule）
  - リスクが高い→影響を受けたデータ主体へ個別通知（Annex 1 – 個別通知のモデル）
  - 例外：データ主体への個別通知が不均衡な努力を伴う場合、個人データ侵害を公的に通知するか同等の方法により報告する（Annex 2 – 公的通知のモデル）
  - 個人データ侵害の記録を取らなければならない（Annex 3 – 個人データ登録フォーム）

IV. 処理者の場合

- 処理者として個人データ侵害を探知し発見した場合、管理者に対し不当な遅滞なく通知しなければならない（Annex 4 – 管理者に対する個人データ侵害通知）。

GDPR対応の具体的成果物

個人データ侵害の通知のためのプロトコル（例）別紙

Annex 1 – データ主体に対する個人データ侵害通知のテンプレート

- **個人データ侵害の性質**
- **影響を受ける個人データの種類の例、影響を受けた個人の概数**
- **当該個人データ侵害の主要な結末**
- **管理者が実行した個人データ侵害を解決し、その悪影響を緩和するために行った方策**
- **コンタクト先（プライバシーチーム）**
- **（DPOが選任されている法域においては次のDPOの連絡先詳細を含める）DPOの名称とEメールアドレス**

Annex 2 –個人データ侵害公的通知テンプレート

- **内容はAnnex 1と同じ**

Annex 3 - 個人データ侵害登録フォームテンプレート

- **個人データ侵害の報告者、個人データ侵害が報告された人または部署、個人データ侵害が発生した日時、個人データ侵害を発見した日時、個人データ侵害の説明、影響を受けたデータ主体の種類、影響を受けた個人データの概数、EUの内外の影響を受けた拠点、即時の影響、潜在的な結末、採られた方策、悪影響を緩和するための方策理者の場合**

Annex 4 – 管理者に対する個人データ侵害通知のテンプレート

- 個人データ侵害の性質、潜在的な結末、方策

Schedule – 管理者の法域におけるデータ保護監督当局

- データ保護監督当局の連絡先、連絡方法

GDPR対応の具体的成果物

データ保護影響評価（DPIA）実行のプロトコル

I. はじめに

II. 適用範囲

- **プライバシーチームの関与**

III. DPIA実行の必要性に関する分析

- **DPIAガイドラインの9つのリスク要因：そのうち2つ以上を満たす場合には高リスクの個人データ処理に該当し、DPIAの実行が必要となる。**
  - 当局が35条5項に基づきDPIAが不要な種類の個人データ処理行為を規定する力を行使しない限りDPIAの実行が必要
  - DPIAを実行しない場合には、プライバシーチームはDPIAの実行をする必要がないと考える理由を文書化する必要がある。
- **個人データの処理の実行前に、関連部署は、DPIAを実行する必要を分析するプライバシーチームに報せなければならない。**

IV. DPIAの実行

- **DPIAのレポートの含むべき内容**
- **DPIAのテンプレート（Annex 1）**
- **データ監督当局に対する事前相談のテンプレート（Annex 2）**

GDPR対応の具体的成果物

データ保護影響評価（DPIA）実行のプロトコル－別紙

Annex 1 – DPIAのテンプレート
I.はじめに
II.意図する処理の描写
III.データ主体の権利および自由へのリスク
IV.比例性の評価
V.リスクに対処するために予定されている方策
VI.結論

Annex 2 – 関連するデータ保護監督当局に対する事前相談のテンプレート
- **データ管理者としての責任**
- **（適切な場合）共同データ管理者の責任**
- **（適切な場合）データ処理者の責任**
- **処理の目的および手段**
- **提供された方策および安全管理措置**
- **プライバシーチームのメンバーの連絡先詳細**

GDPR対応の具体的成果物

データ保護影響評価（DPIA）実行のプロトコル－別紙

DPIAのテンプレート－詳細版

1.はじめに

a. プロジェクト・プレゼンテーション、b. ゲート質問

2. 処理の詳細

c. データ主体、

d. プロジェクトのために、収集され、使用され、開示され／移転され、保管される個人データ

i. 人事・従業員データ、 ii. 顧客関連

e. プロジェクトのためにデータが開示されおよび／または移転される受領者を選ぶ

iii. 受領者の一覧、iv. 供給業者の一覧

3.処理によって生じるリスクおよび害悪

f.個人に対する潜在的リスクまたは不利益

g.処理がプライバシー法に沿っているか

v. 通知 ・処理案はプライバシーポリシーでカバーされているか

vi. 処理の根拠、 vii. 互換性のある目的

viii. データ最小化、 ix. データ保持

x. セキュリティ、 xi. EEA外への移転

xii. 個人の権利

4. 労働評議会（ワークスカウンシル）の意見（関連する場合）

5. データ保護責任者の意見（もし選任された場合）

6. 結論（ビジネスリスクなのか、法的リスクなのか、リスクは緩和・低減可能か）

GDPR対応の具体的成果物

データ主体の権利に対処するためのプロトコル（例）

I. はじめに
II. 適用範囲
III. データ保護の権利の導入
IV. 権利の行使および権利への対処
V. アクションプロトコル
1~6 各権利毎にプロトコルを準備
1.1. 権利行使の適切性
1.2. 行使は適切でない
1.3. 行使は適切である

Annex 1-7について、管理者が請求者に関する個人データを保有する場合と保有しない場合とでOption 1と2とを場合分け。
Annex 1 アクセス権に対する回答のテンプレート
Annex 2 訂正権に対する回答のテンプレート
Annex 3 削除権に対する回答のテンプレート
Annex 4 処理の制限権に対する回答のテンプレート
Annex 5 データポータビリティ権に対する回答のテンプレート
Annex 6 異議権に対する回答のテンプレート
Annex 7 プロファイリングを含む自動化された個別意思決定への異議権に対する回答のテンプレート

GDPR対応の具体的成果物

データ保持ポリシー（例）－加盟国法に関する調査が必要

I. はじめに
II. 範囲
III. データ保持期間
- データ保持：適用法等に基づくオフィス毎の主要データ保持期間、適用保持期間経過後、個人データは電子および非電子システムから削除
- 追加遮断期間：主要データ保持期間経過後も、処理の帰結として生じ得る責任の消滅時効期間の残りの期間、公的機関、裁判所および裁判官に対し当該データを利用可能としておくことが許される。個人データを適法に遮断しておくことがデータの削除の例外である。例えば、従業員が退職した後は、時効期間との関係で従業員の記録を保持することが求められるが、その期間は遮断が要求される。
- 個人データの遮断の方法
- 個人データを非遮断にする時

IV. データの削除
- 電子データ、ビデオ監視の記録、バックアップ記録
- 破壊された文書の記録

V. データ保持チャート
- 例：主要データ保持期間が5年、追加遮断期間が7年の場合、保持期間は12年

VI. 質問
VII. バージョン管理

GDPR対応の具体的成果物

データ保持ポリシー（例）－データ保持チャート（国毎）

データ主体の種類	個人データが当初収集された目的	主要保持期間	追加遮断期間
候補者			
従業員			
顧客			
潜在顧客			
ウェブサイト使用者			
供給業者			

Eプライバシー指令に基づく加盟国法対応の成果物

クッキーポリシー（例）

- **クッキーとは何か？**
- **このウェブサイトは以下の種類のクッキーを使っている。**
  - 厳密に必要なクッキー（Strictly Necessary Cookies）：ウェブサイトのセキュアエリアにアクセスする等のウェブサイトを移動するのを可能にするために不可欠なクッキー
  - パフォーマンスクッキー（Performance Cookies）：ウェブサイトが動く方法を改善するのに使われる
  - 機能性クッキー（Functionality Cookies）：選択内容を覚えておき、より個人的な特色を使用できるようにする
  - ソーシャルメディアクッキー（Social Media Cookies）：LinkedInやツイッター等のソーシャルメディアにおいて何をやってきているかを共有するもの
  - グーグルアナリティクスクッキー（Google Analytics Cookies）：トラフィックレベル、検索ワードおよびウェブサイトへの訪問を監視するグーグルアナリティクスによって使われている
  - 電子マーケティングクッキー（E-Marketing Cookies）：Eメールでのマーケティング通信を送った際に、そのEメールでのクリックによりウェブサイトにとんだ場合には、Eマーケティングでの行動とウェブサイトでの行動を追加のクッキーを使って紐づける
- **クッキーに関する同意と選択**
  - **ウェブサイトへの訪問の際に、ポップアップでクッキーが使われている目的とオプトアウトの方法についてお知らせしている。クッキーの同意はいつでも撤回できる。**

IV. EDPBによるGDPRガイドラインの公表状況

EDPBによるGDPRガイドラインの公表状況

No.	GDPRに関する第29条作業部会ガイドラインのテーマ
WP 242 rev.01	データポータビリティの権利
WP 243 rev.01	データ保護責任者
WP 244 rev.01	管理者または処理者の主導監督当局の特定
WP 248 rev.01	GDPRにおけるデータ保護影響評価および「高リスクとなる可能性がある」処理かどうかの決定
WP 249	職場におけるデータ処理に関する意見書02/2017
WP 250 rev.01	GDPRの下での個人データ侵害通知
WP 251 rev.01	GDPRにおける自動化された個別の意思決定およびプロファイリング
WP 252	協調高度道路交通システム（C-ITS）に関連する個人データ処理に関する意見書03/2017
WP 253	GDPRにおける行政制裁金の適用および設定
WP 254 rev. 01	十分性の参照

EDPBによるGDPRガイドラインの公表状況

No.	GDPRに関する第29条作業部会ガイドラインのテーマ
WP 256 rev.01	拘束的企業準則における要素および原則の表の説明に関する作業文書
WP 257 rev.01	処理者拘束的企業準則における要素および原則の表の説明に関する作業文書
WP 259 rev.01	GDPRにおける同意
WP 260 rev.01	GDPRにおける透明性
WP 261	GDPRにおける認証機関の認定
WP 262	GDPR第49条
WP 263 rev.01	GDPRにおける管理者および処理者の「拘束的企業準則」の承認のための協力手続の説明に関する作業文書
WP 264	個人データの移転のための管理者拘束的企業準則の承認のための標準申請書に関する勧告
WP 265	個人データの移転のための処理者拘束的企業準則の承認のための標準申請書に関する勧告
	GDPR第30条第5項に基づく処理行為の記録維持義務の例外に関する方針説明書

GDPRに関するEDPBガイドラインとして公表される予定で未完成のもの

- 認証
- GDPRの地理的適用範囲（GDPR第3条）
- 行動規範（第40条および第41条）
- GDPR第6条第1項第b号に関するガイダンス（「無料」オンラインサービスの提供との関連を特にテーマとして）

V. 十分性決定と個人データの直接取得

移転に関する一般原則

- GDPR第44条は、第三国等に対する個人データの移転に関する第V章で規定される移転に関する規制を管理者または処理者が遵守しなければ、個人データの移転は認められない旨を規定している（**Any transfer** of personal data which are undergoing processing or are intended for processing after transfer **to a third country or to an international organisation** shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with **by the controller and processor**, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.）。
- 規定の文言を素直に読むと、EUから第三国への移転行為を規制するものであり、EU内の管理者または処理者による移転行為を規制すること想定していると考えられる（適切な保護措置がSCCやBCRがEU内の管理者または処理者から第三国への移転を想定した内容であることも上記解釈と整合的）。

十分性認定と個人データの直接取得（第3条）

- 第45条第1項：第三国または国際機関への個人データの移転は、当該第三国、第三国域内の領域または一つもしくは複数の特定された部門、または国際機関が保護に関して十分なレベルを保証していると欧州委員会が決定した場合に行うことができる。
- GDPRの域外移転の規制は、十分なレベルのデータ保護があると欧州委員会が認定していない国に対する個人データの移転は原則として禁止されており（第45条）、適切な保護措置（第46条）または法令上の例外（第49条）の要件を満たす場合には例外的に個人データの移転を認めている。
- 十分性決定は、第三国への個人データの移転を適法化するもの

十分性認定と個人データの直接取得（第3条）(2)

- GDPRの域外移転の規制の趣旨は、十分性認定のない第三国への個人データの移転について、適切な保護措置に基づきデータ輸入者側がGDPRと同等のレベルの個人データの保護に関する義務を負わせることによってその適切な保護措置に基づく枠組内のデータ移転を認め、または法令上の例外については限定的な状況について個人データの移転を認めるものである。
- そのため、GDPRがEEA外の企業に直接適用される場合にはEEA外の企業はGDPRに基づく義務に拘束されることになることから、GDPRの域外移転の規制の趣旨からは、適切な保護措置を講じる必要はないと考えられる。データを直接取得する行為については、域外移転の規制の対象にはならない。
- すなわち、欧州委員会が日本の十分性認定を行った場合、日本国内から行うEEAのデータ主体の個人データの直接取得のケースでは、GDPRが直接適用となる。

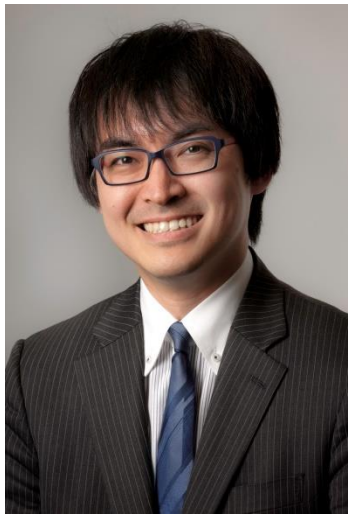
十分性認定と個人データの直接取得（第3条）(3)

- 欧州委員会が日本の十分性認定を行った場合であっても、以下のGDPRの直接適用は引き続き問題となると考えられる。
- EEA域内の管理者又は処理者の拠点の活動に関連してなされる個人データの処理に適用される（処理が域内で行われるか域外で行われるかを問わない）（3条1項）
  - A. 自社欧州子会社の従業員データ・顧客データを日本で保存する
  - B. クラウドサービス事業者が、顧客企業の従業員データを日本のサーバで保存する。
- EEA域内に拠点がない管理者又は処理者によるEEA域内のデータ主体の個人データの処理のうち、以下のいずれかの場合には適用される（3条2項）
  - A. EEA域内のデータ主体に対し、商品又はサービスを提供する場合
    - 1) 日本法人が、英語で、ポンドやユーロが支払通貨として利用できるようにして日本のサーバでECサイトを運営し、欧州に在住する顧客から、個人情報を取得する場合等（前文（23））
  - B. EEA域内のデータ主体の行動を監視する場合
    - 1) 欧州に在住する個人から、アプリ等で位置情報を取得したり、ウェブサイト上からクッキーで個人情報を取得する場合

VI. まとめ

まとめ

- いよいよGDPRの適用が開始されたが、GDPR適用開始初年度は、データ保護監督当局側も、様子を見ながらの慎重な執行を行うものと考えられる。
- GDPR適用開始初年度（2018年6月から2019年5月）の間に、EDPBによるGDPRガイドラインを踏まえた適切なGDPR対応を心掛けたい。加盟国法により従業員データの処理等の幾つかの論点について各国別の対応がなされる点もフォローしていく必要がある。
- 特に、処理のセキュリティのように、個人データ侵害が起こった場合に、高い確率でデータ保護監督当局から遵守状況のチェックがなされる項目については注意が必要である。ENISAやCNILのガイドラインによって処理のセキュリティに関するリスク判断の具体的な手法と、リスク判断の結果に基づいて具体的に取るべき施策が明らかとされた以上、企業にとってGDPRにより求められるセキュリティ対応のレベルは大きく上がったと考えられる。
- まもなく欧州委員会による日本の十分性決定が発効すると考えられるが、十分性決定によって対応を取らなくて済む項目の範囲を適切に理解したうえで対応することが望ましいと考えられる。



杉本 武重
Takeshige Sugimoto, CIPP/E

takeshige.sugimoto@twobirds.com
Direct +32 (0)2 282 6076
Mobile +32 (0)499 054619 (ベルギー)
Mobile +81 80 8051 4848(日本)

2006年	弁護士登録（59期）
同年	第一東京弁護士会所属
2013年	ニューヨーク州弁護士登録
同年	ニューヨーク州弁護士会所属
同年	ブリュッセル弁護士会登録（準会員） 同会所属

バード・アンド・バード法律事務所ブリュッセルオフィス
パートナー　弁護士　杉本　武重

経歴

2000年　駒場東邦高等学校卒業

2004年　慶應義塾大学法学部法律学科卒業

2006年　長島・大野・常松法律事務所入所

2012年　シカゴ大学ロースクール法学修士課程卒業(LL.M)

2013年　オックスフォード大学法学部法学修士課程卒業(Magister Juris)

同年　　ウィルマーヘイル法律事務所入所、同事務所ブリュッセルオフィス・アソシエイト

2015年　同オフィス・シニアアソシエイト

同年　　デュッセルドルフ日本商工会議所法務委員会専門委員就任

2016年-2017年　公正取引委員会競争政策研究センター客員研究員

2017年　ウィルマーヘイル法律事務所退所

同年　　ギブソン・ダン・クラッチャー法律事務所入所、同事務所ブリュッセルオフィス、オブ・カウンセル就任。

2018年5月　同事務所退所

2018年6月　バード・アンド・バード法律事務所ブリュッセルオフィス・パートナー就任、現在に至る。

主要な取扱分野

EUデータ保護法

EU競争法（EUカルテル規制、EU企業結合規制および標準必須特許問題を含むEU競争法全般）

EUサイバーセキュリティ法

最近の主要著作

▪日本貿易振興機構（ジェトロ）ブリュッセル事務所「『EU一般データ保護規則（GDPR）』に関わる実務ハンドブック（入門編）」（2016年11月）
https://www.jetro.go.jp/ext_images/_Reports/01/dcfcebc8265a8943/20160084.pdf
「EU一般データ保護規則（GDPR）」に関わる実務ハンドブック（実践編）」（2017年8月）
https://www.jetro.go.jp/world/reports/2017/01/76b450c94650862a.html

最近の主要講演

▪一般財団法人日本情報経済社会推進協会・第18回IoTデータ流通促進ワーキンググループ「国境を越えるデータ流通の促進」において「EU：一般データ保護規則、十分性認定等の動きを踏まえた産業界の取り組みと課題」と題する講演（東京・2017年12月7日）
▪在英国日本国大使館、在英日本商工会議所（JCCI）およびジェトロ・ロンドン「EUデータ保護法早わかりセミナー」講師（ロンドン・2017年11月30日）
▪日本貿易振興機構（ジェトロ）主催セミナー「EUデジタル単一市場の進捗と一般データ保護規則への対応」において「「一般データ保護規則（GDPR）」直前準備と最新動向～SCC、BCRのポイント～」と題する講演（東京・2017年10月5日）
▪日本経済団体連合会情報通信企画部会にて「EU一般データ保護規則が企業に与える影響」と題する講演（東京・2016年7月26日）

Bird & Bird

Thank you & Bird & Bird

twobirds.com