EU一般データ保護規則（GDPR）の適用開始前の直前対策

（2018年4月）

（ベルギー日本人会商工委員会ビジネスセミナー）

ギブソン・ダン・クラッチャー法律事務所
ブリュッセルオフィス
オブ・カウンセル
弁護士　杉本 武重
+32 2 554 7280 (Direct)
+32 499 05 46 19 (Mobile)
TSugimoto@gibsondunn.com

GIBSON DUNN

Beijing • Brussels • Century City • Dallas • Denver • Dubai • Frankfurt • Hong Kong • Houston • London • Los Angeles

Munich • New York • Orange County • Palo Alto • Paris • San Francisco • São Paulo • Singapore • Washington, D.C.

目次

第1　GDPRの基本概念　3

第2　GDPRに関して2018年5月25日までに最低限完了させておきたい事項　11

A. 制裁金決定を回避するための戦略的対応＜総論＞　12

B. 制裁金決定を回避するための戦略的対応＜各論＞　22

第3　まとめ　80

第1 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。
- 違反の場合の制裁金の上限額は2通り。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）（**作業部会**）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）。
▪作業部会は**欧州データ保護会議**(European Data Protection Board.「**EDPB**」)へと改組

GIBSON DUNN

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

GIBSON DUNN

特別カテゴリの個人データ

概念	説明	例
特別カテゴリの個人データ(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

GIBSON DUNN

GDPR違反の場合の制裁金の基準と違反行為の類型

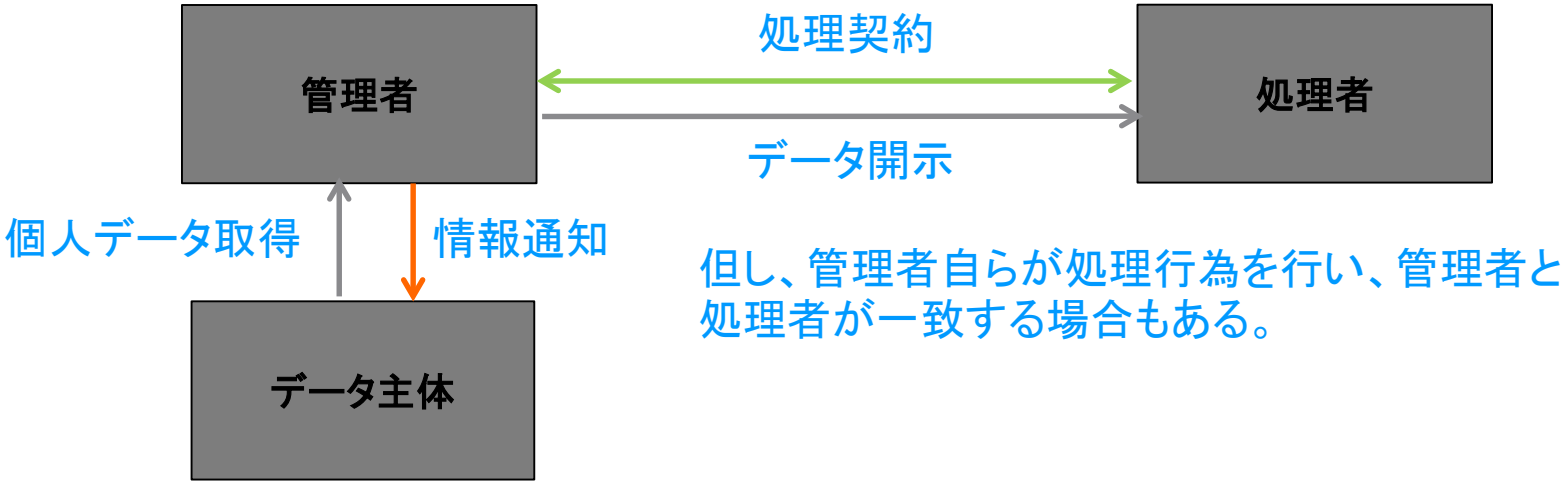
■ ポイント:「事業者の全世界年間売上高」とは、事業者グループの最終親会社に遡って、その最終親会社のグループをいう。例えば、日本企業の英国子会社によるGDPR違反の場合には日本本社のグループの全世界年間売上高となる。

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EEA代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。



但し、管理者自らが処理行為を行い、管理者と処理者が一致する場合もある。

GIBSON DUNN

GDPRの適用範囲(第3条)

ポイント：EEA域外での個人データの処理に対してGDPRが直接適用される範囲を定めた。

1. GDPRは、EEA内の管理者又は処理者の事業所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。
   - 日本本社がEEA域内の所在者からjob applicationを直接受け付ける。
   - 日本本社のウェブサイトにおいて複数の欧州言語で訪問者からのコメントを受け付ける。
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。
   - 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、個人データを取得する場合等

(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
   - 行動の監視：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
   - 監視はあらゆるカテゴリーのデータを参照することで起きうるかもしれない。
     - インターネットブラウジング（例. トラッカークッキー、個人のコンピュータの履歴保存）
     - 欧州に在住する個人から、ウェブサイト上からクッキーで個人データを取得する場合

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。 作業部会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

GIBSON DUNN

第2　GDPRに関して2018年5月25日までに最低限完了させておきたい事項

A. 制裁金決定を回避するための戦略的対応
＜総論＞

1. GDPR遵守のための現状把握—データマッピング

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（GDPRが直接適用される）
   - 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（SCCを締結しデータ輸入者の義務を負うため、SCCで移転させる個人データの処理・移転に関するデータ輸入者の義務の履行のために社内体制を構築する必要がある。または例外的にGDPRが直接適用される。）

1. GDPR遵守のための現状把握—データマッピング
データマッピングの過程

- データマッピングの開始から完了まで約2か月から3か月かかることが一般的だが、効率的・スピーディに進めることを目指す。

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
7. 回答内容に基づくGDPR上の評価と評価内容に基づくGDPR遵守のための各種文書の作成

1. GDPR遵守のための現状把握—データマッピング
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

1. GDPR遵守のための現状把握—データマッピング
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？

1. GDPR遵守のための現状把握—データマッピング
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？

2. 2018年5月25日までに対応を完了できる項目の作業完了データマッピングの結果を踏まえて早期に対応可能な項目

- 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
    1. 処理行為の適法性の確保・記録保持義務の履行
       - A) 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
       - B) 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
       - C) 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
       - D) 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
       - E) 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）
    2. 業務委託契約の見直しが必要となる第三者（処理者）を特定
    3. データ保護影響評価の実行義務の有無を判定
    4. 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→移転規制には、事業者グループ内での域外移転については、域外拠点からの再度の移転を除き、対応完了することは不可能ではない。
    - 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・締結

2. 2018年5月25日までに対応を完了できる項目の作業完了

GDPRに関連する社内規程類・マニュアルの作成・導入（データマッピングの結果の一部または全部を前提とせずとも推進できる）

- 以下の社内規程、外部向けポリシー、各種マニュアル・フォーマット等を英語で作成し、一通りGDPRの適用対象となるEEA内外の拠点に備えることで、監督当局からGDPRへの遵守の状況に関する説明を求められたときに、一通りの説明をできるようにしておく。各拠点毎の改訂作業やそれに基づく運用については5月25日以降に作業を行う。

1. 個人データ保護規程（社内規程）の作成
2. プライバシーポリシー（社外向け）の作成
3. 同意のフォーマットの作成
4. 情報通知のフォーマットの作成
5. 個人データ侵害通知の場合の72時間以内の監督当局への報告義務やデータ主体への個別の報告義務の履行のためのマニュアルの作成
6. データ主体の権利行使に対する対応マニュアルの作成
7. データ保護影響評価の実行義務の判断と同評価の実行に関するマニュアルの作成
8. 処理者との間で提供する処理契約の条項のフォーマットの作成
9. データ保護責任者の書面による選任と監督当局への連絡先の通知

3. 2018年5月25日までに対応を完了できない項目の洗い出しおよび対応完了に向けたロードマップの作成

- 2018年5月25日までに対応を完了できない項目の洗い出し→以下の事項は多くの企業が5月25日までに対応を完了させることが難しい項目になるため、できるだけ5月25日より前に完了させることが望ましいが、実際には、以下の事項を5月25日以降、いつの時点で対応完了させることができるかのロードマップを作って説明責任を果たせるよう備えておく必要があるものと考えられる。

1. 個人データの処理に関する外注契約に関する第三者との処理契約の締結
2. 個人データの域外移転に関するSCCの締結（グループ外の第三者とのSCCの締結）
3. 各種社内規程・外部向けポリシー・各種マニュアルに関する各拠点でのカスタマイズ
4. 同意のフォーマットや情報通知のフォーマットの各拠点におけるビジネスフローに応じたカスタマイズ
5. 各拠点におけるGDPRに関するトレーニング
6. 各拠点におけるセキュリティアセスメントと改善事項の洗い出し、改善策の立案と実行
7. 新しい処理行為に関するデータ保護影響評価の実行

4. まとめ

- 以上見てきた通り、GDPRに関して2018年5月25日までに最低限完了させておきたい事項としては、以下のものが考えられる。
  1. GDPR遵守のための現状把握—データマッピング
  2. 5月25日までに対応を完了できる項目の作業完了
     A) データマッピングの結果を踏まえて早期に対応可能な項目
     B) GDPRに関連する社内規程類・マニュアルの作成・導入（データマッピングの結果の一部または全部を前提とせずとも推進できる）
  3. 5月25日までに対応を完了できない項目の洗い出しおよび対応完了に向けたロードマップの作成
- 残り時間との関係で、適切に優先順位付けを行って作業することが、GDPRの制裁金決定を受けるリスクを最小限に抑えるための努力として、必要なことであると考える。
- 制裁金決定を避けるための戦略的対応を行う上で重要なのは、いかにして監督当局に対する説明責任を果たすかを考えながら、一つ一つのGDPR上の義務に対応した取組みを行うことであると考える。

B. 制裁金決定を回避するための戦略的対応
＜各論＞

B. 制裁金決定を回避するための戦略的対応＜各論＞

I.　データマッピングの質問票の構造

II.　データマッピングの質問票の質問事項の詳細

III.　2018年5月25日までに対応を完了できる項目の作業完了
データマッピングの結果を踏まえて早期に対応可能な項目

IV.　2018年5月25日までに対応を完了できる項目の作業完了
GDPRに関連する社内規程類・マニュアルの作成・導入（データマッピングの結果の一部または全部を前提とせずとも推進できる）

V.　2018年5月25日までに対応を完了できない項目の洗い出しおよび対応完了に向けたロードマップの作成

データマッピングの質問票の構造

質問票	質問事項
質問票シートA （個人データの処理に関する義務を遵守するために必要な情報を集める）	1. データ処理の目的 (GDPR 5条(1)(b)) 2. データを処理されるファイリングシステム（Filing system）(GDPR 2条(1) and 4条(6)) 3. 個人データのカテゴリー(GDPR 4条(1), 5条(1), 9条(1)) 4. データ主体(GDPR 4条(1), 5条) 5. データの保持(GDPR 5条(1)(e)) 6. 法的根拠 (GDPR 6条) 7. 個人データの流入（In-flows） (GDPR 14条(1)(f), 24条 ff.) 8. データ主体への情報提供(GDPR 12～14条) 9. 管理者／処理者としての役割(GDPR 24～28条) 10. 可能性のある受領者のカテゴリ(GDPR 28条) 11. 高リスクのデータ処理(GDPR 35条)
質問票シートB （事業者グループ内での個人データ移転を標準契約条項（SCC）を締結してカバーするために必要な情報を集める）	1. 個人データが移転される国 (GDPR 44条) 2. 適切な保護措置の対象となる移転 (GDPR 46条) 3. SCCsを完成させるために必要な情報(GDPR 46(2)(c)条) 4. データ主体に関する情報(GDPR 13条及び14条) 5. その他の規制に基づく義務
質問票シートC （事業者グループ外での個人データ移転）	（シートBに同じ）
質問票シートD	1. 処理の遵守とセキュリティ(GDPR32条) 2. データが処理されるファイルリングシステム(GDPR2条1項および4条6項) 3. 行動規範と認証(GDPR40条)
用語集	

GIBSON DUNN

用語集

	用語	定義
1	個人データ	自然人（データ主体）を特定できる、あるいは特定しうることにつながるあらゆる情報のこと。特定しうる自然人とは直接的あるいは間接的に特定しうるということであり、特に氏名やID番号、位置情報、オンライン識別子、あるいは自然人の1つあるいは2つ以上の物理的、生理学的、遺伝的、精神的、経済的、文化的あるいは社会的な特定の要素を参照することによって特定しうるということである。 例： - 姓名、- 役職、- 自宅住所、- ID番号(顧客番号など)、- 位置情報、- 電子メールアドレス（自宅/会社)、- 電話番号（自宅/会社) - オンライン識別子（IPアドレス、クッキー識別子） - 物理的、生理学的、遺伝的、精神的、経済的、文化的、社会的アイデンティティ、犯罪履歴 - クレジットカード/銀行口座情報、- 患者の身体的および医療情報（例. 生年月日、年齢、性別、身体的特徴、病歴、家族の病歴、手術の履歴等) - 患者の処方箋情報（例　処方箋番号、薬の名前、薬の強度、製造者、販売価格、新規あるいは詰め替え、利用目的等） - 録音された顧客からの電話、- ビデオ監視 （監視カメラの情報） - 従業員のパフォーマンス評価結果、 - 採用情報（例. CV, 資格、既婚/未婚、生年月日、リファレンスレター等） 個人データには特別カテゴリーの個人データが含まれる。それは、人種や民族、政治信条、宗教あるいは哲学的信念、組合員たる地位を明らかにするデータや自然人を特定する目的で行われる遺伝的、生体的データの処理、健康に関するデータあるいは性生活または性的指向に関するデータのことである。 例：治験の結果、健康診断の結果、指紋、網膜パターン、顔の構造、声、掌形認証、静脈パターン 回答中に迷われたときはすべて個人データとして取り扱ってください。
2	処理	個人データあるいはそのセットに対して行われる処理あるいは一連の処理であり、自動処理か否かを問わない。これは個人データの収集、記録、組織化、構造化、保管、適用、改変、検索、調査、使用、移転、広告その他の手段による開示、整列、組合せ、制限、消去、破壊を言う。 例：クレジットカード情報の保管、電子メールアドレスの収集、顧客コンタクト情報の修正、顧客名の開示、従業員評価結果に対するスーパーバイザーによる閲覧、データ主体のオンライン識別子の削除、全従業員の氏名、タスク、オフィス住所、写真のリスト作成
3	処理者	処理者とは、管理者の代わりに個人データを処理する会社のことである。 例：ホスティングサービスベンダー、会計サービス提供ベンダー
4	管理者	管理者とは、単独あるいは他者と共同で、個人データの処理の目的と手段を決定する会社のことである。 例：直接的あるいは間接的にデータを収集し、どのようにそれを使うかを決めている会社

用語集(2)

	言葉	定義
5	データ主体	"直接的あるいは間接的に個人データを参照されることで識別されたあるいは識別可能な自然人のことである。例：従業員、最終顧客/ユーザー、ビジネスパートナーのコンタクト先、子ども"
6	移転あるいはアクセス（閲覧）	GDPR上は特定の定義は提供されていない。第三者が個人データを利用可能になる措置のことであり、データの転送（電子メール、CD/DVD、FTPサーバ等)あるいは他社からアクセス可能なシステムにデータを入力すること（例 ソフトウェア、オンラインシステム、ネットワーク、共有サーバ、グループ間ドキュメント管理システム等）を含んでいる。 例：他社によってアクセス可能なネットワークにアップロード、他社にメールやその他の手段で送付、他社が運用するシステムやソフトウェアにデータをアップロード
7	EEA	EU加盟国＋アイスランド、リヒテンシュタイン、ノルウェイ EU加盟国：オーストリア、イタリア、ドイツ、ラトビア、ブルガリア、リトアニア、クロアチア、ルクセンブルグ、キプロス、マルタ、チェコ、オランダ、デンマーク、ポーランド、エストニア、ポルトガル、フィンランド、ルーマニア、フランス、スロバキア、ドイツ、スロベニア、ギリシア、スペイン、ハンガリー、スウェーデン、アイルランド、英国の28か国）
8	SCC	標準契約条項(Standard Contractual Clauses)。欧州委員会によって採択された契約のテンプレート。EUが個人データの"十分な保護"がなされていないとする国への個人データの移転を適法化する保護措置の1つ。 *「十分な保護」とは欧州委員会によってなされる宣言（決定 Decision）であり、EEA外の第三国がデータ保護を十分なレベルであることを保証することを確認したものである。十分性認定のない国へのデータ移転は原則違法であり、適切な保護策（SCCなど）がとられた場合に例外的に適法となりうる。
9	データ保護監督当局	EU加盟各国のデータ保護法制の適用を監視することに責任を持つ公的な執行機関
10	評価/スコアリング	データ主体の個人的側面の評価（仕事の成果、経済状況、健康、個人の嗜好や興味、信頼性や行動、位置や動き等）
11	自動的意思決定	データ主体に法的効果をもたらすデータ主体に対する意思決定を目的とした自動的データ処理（データ主体間での差別を生む恐れもある。）個人にほとんど、あるいはまったく影響がない処理はこの条件を満たさない。 例： - 保険料/補償範囲を提供するための自動スコアリング - 子どもの学校/クラスを決定するための自動評価

用語集(3)

	言葉	定義
12	体系的監視	(i)データ主体を観察、監視、あるいは制御するために、(ii)体系的に、行われるデータ処理 監視はあらゆるカテゴリーのデータに関して起こり得る - 個人のインターネットブラウジング（例. トラッカークッキー、個人のコンピュータの履歴の保存） - 個人の位置情報(例. GPD あるいは 位置トラッキングデバイス) 「体系的」とは、次のいずれもあてはまる - システムに関連して行われる - 事前にアレンジされ、組織化され、秩序正しいものである - データ収集の一般的な計画の一環として行われる - 一般的な戦略の一部として実行される
13	組合せ	貴社が収集した個人データを、第三者によって収集された、及び/又はデータ主体の観点からは予期していない異なる目的において、他の個人データと組み合わせること
14	ファイリングシステム	データを保管し、処理する1つあるいは複数の手段。紙のキャビネットから電子的なシステムまでありえる。後者はデータベースや登録ソフトウェア(SAPなど)、電子メール処理ツール(Outlookなど)、データ処理ツール(Excelなど)、自動データログ(Webサイトのアクセス記録、登録や入室に関するログなど）やその他のデータを含む。
15	ワークスカウンシル（労働評議会）	従業員または労働組合の団体であり、労働者代表の集まりが会社の全従業員を代表し、会社の雇主とともに、これらの従業員の権利と利益を声にするもの。フランスにおける「comité d'entreprise」、スペインにおける「comité de empresa」、又はドイツにおける「Betriebsrats」、「Betriebs」をいう。

データマッピングの質問票シートAの質問事項の詳細
1.データ処理の目的 (GDPR 5条(1)(b))

- なぜ、EEA (7*)に関連した個人データ(*1)が処理 (*2)されているのか説明してください（データ処理 (*2)の目的）

- 各目的を、はっきりと特定し、詳細に規定するとともに、個別に説明してください。例えば、従業員データも、異なる目的のために処理されているかと思います（例：給与の処理のため、建物への入退室管理のため、業績評価のため、費用清算のため).

- 例：ドイツの[会社]　毎月の従業員の給与処理

データマッピングの質問票シートAの質問事項の詳細

2. データを処理されるファイリングシステム（Filing system）(GDPR 2条(1) and 4条(6))

- 当該EEA (7*) 内の個人データ(1*)が処理(2*)される登録システム（14*）/サポート/プログラム/データベース/フォーマット/媒体について説明してください。（例：紙ファイル、Eメール、エクセル、CRMシステム、SAPシステム）

- 例：
- - エクセル（トラッキングシート）
- - 人事マネジメントソフト

GIBSON DUNN

データマッピングの質問票シートAの質問事項の詳細

3. 個人データのカテゴリー(GDPR 4条(1), 5条(1), 9条(1))

- 当該目的のために収集される個人データ (1*) の種類を挙げてください。 （例：名前、住所、電話番号、職業、クレジットカード番号、顧客番号）

- 例：
- - 従業員の氏名
- - 住所
- - ソーシャルセキュリティ/財務番号
- - 給与
- - 銀行口座

GIBSON DUNN

データマッピングの質問票シートAの質問事項の詳細
4.データ主体(GDPR 4条(1), 5条)

- 誰の個人データ(1*)が処理 (2*)されているか説明してください。

- A)個々の「データ主体」(5*)を挙げてください。（例：従業員、顧客/エンドユーザー、ビジネスパートナーの担当者、子供）
- B) 各データ主体(5*)の種類ごとに、データ処理の対象となる個人の概数を教えてください。

- 例：
- - ドイツの[会社名]の従業員 - 47名

データマッピングの質問票シートAの質問事項の詳細
5. データの保持(GDPR 5条(1)(e))

- 5.1 あなたのチーム／事業部隊においてデータ処理(2*)を行う必要のある期間を教えてください。当該処理(2*)期間が、法定要件と関連する者かどうかについて、記載してください。（例：租税法）
- 例：個人データは、要求があった後最大5年間は保管が必要である（適用のある商法、税法、国税法）

- 5.2 実際に当該個人データ (1*) が保管されている期間を教えてください。（実際に保管されてすぐに引き出せるか、アーカイブされているかを含む。）
- 例: 個人データは、要求があった後最大5年間は保管が必要である（適用のある商法、税法、国税法）
- 例: 全てのデータ: 永久に.

データマッピングの質問票シートAの質問事項の詳細
6. 法的根拠(GDPR 6条)

- 6.1 個人データ (1*)の処理 (2*)については、データ主体 (5*)から事前に同意が取得されていますか？ （例：同意書フォーム、オンラインのチェックボックス等）当該同意が要求され、又は取得される際に使用されるフォーマットを提出してください。
- 例:いいえ
- 6.2 個人データ (1*) の処理 (2*) は特別の法律に基づく義務によるものですか。（例：不正防止法、税法）当該データの処理を義務付けている法律を特定してください。
- 例：はい、雇用法に基づいている。
- 6.3 個人データ (1*) の処理 (2*) は、その他の理由に基づくものですか。（例：事業を行うため等） 理由を説明するに当たっては、可能な限り正確に記載をしてください。
- 例: はい（従業員に対して給与を支払うために必要）

データマッピングの質問票シートAの質問事項の詳細

7. 個人データの流入（In-flows） (GDPR 14条(1)(f), 24条 ff.)

- 個人データ (1*) をどこから入手したのか説明してください。入手経路を説明してください。（例：従業員から、直接の顧客から、ウェブサイト上で)
- 他の法人からEEA個人データを入手している場合には、当該法人の名前と所在国を教えてください。
- 例: 従業員
- 7.1 個人データ (1*) をデータ主体 (5*)から直接取得している場合、当該個人データ (1*)の処理 (2*) に関する情報をデータ主体に提供していますか。（例：情報通知、パンフレット）もし回答が「はい」の場合、かかる書類のサンプルを提供してください。
- 例：ない、雇用契約において。（義務履行のためのデータ処理に関する一般的なディスクレーマを記載）
- 7.2 個人データ (1*) をデータ主体 (5*)から直接取得していない場合、データ主体(5*)が、貴社における当該個人データ (1*)の処理 (2*)について認識しているかどうかわかりますか。（例：第三者による情報通知等）
- もし回答が「はい」の場合、かかる書類のサンプルを提供してください。
- 例：該当なし

GIBSON DUNN

データマッピングの質問票シートAの質問事項の詳細
8. 管理者／処理者としての役割(GDPR 24～28条)

- 8.1 貴社でのデータの処理(*2)は貴社が処理者 (*3)として、他社に対するデータ処理(*2)サービスの一環で行っていますか。（例：他社、すなわち管理者(*4)のためにデータ処理(*2)を行っている。）
- 例：処理者として行動していません；ドイツの[会社名]は管理者として行動しています。
- 8.2 貴社が処理者 (*3)として行動している場合には、貴社がデータ処理を提供している会社を教えてください。（管理者 (*4)名、貴社が提供しているサービスの内容、及び当事者間の合意書ないし書式のサンプルを提供してください。）
- 例：該当なし（[会社名]は管理者として行動しています。）
- 8.3 貴社が管理者（4*）として行動している場合、プライバシーポリシー、内部データ保護規程その他の書類／ガイダンス等を作っているか教えてください。そのような書類のサンプルを提出してください。
- 例：いいえ。

データマッピングの質問票シートAの質問事項の詳細
9. 可能性のある受領者のカテゴリ(GDPR 28条)

- 9.1 個人データ(1*)が、他の法人に対して移転され、又は他の法人からアクセス可能な(6*)状況にあるか、教えてください。（例：他のグループ会社、ベンダー、サービス業者、顧客）もし回答が「はい」の場合、以下の二つを教えてください。
- i)グループ会社（例：HQ、子会社、関連会社）
- ii)第三者（例：ベンダー、パートナー、サービス業者）
- 例: はい:
- 1. X社 (データを保存し処理しているサーバーを所有している。)
- 2. Y社 (サイバーセキュリティに関するアドバイザーであり、データのサンプルに時々アクセスする)
- 3. Z社 (給与支払サービス業者)

- 9.2 各法人について、当該個人データ(1*)の移転(6*)に適用されるデータ処理に関する合意書、条項、又はポリシー等があるか教えてください。もしそのような合意書、条項又はポリシーがあれば、そのサンプル／写しを提供してください。
- 例:
- 1. X社：はい、サーバー業務を提供している会社とのサービス提供合意書。
- 2. Y社 ：いいえ
- 3. Z社 ：はい

GIBSON DUNN

データマッピングの質問票シートAの質問事項の詳細
10. 高リスクのデータ処理(GDPR 35条)

- 10.1 データ主体（5*）の評価（10*）を行うために当該個人データ（1*）の処理（2*）を行っているか教えてください。詳細について説明してください。
- 例：いいえ
- 10.2 データ主体（1*）に関する自動的な決定（*11）のために、当該個人データ（1*）の処理（2*）が行われているか、教えてください。詳細について説明してください。
- 例：いいえ
- 10.3 データ主体（1*）の体系的監視（12*）のために当該個人データ（1*）の処理（2*）が行われているか教えてください。詳細について説明してください。
- 例：いいえ
- 10.4 他のデータベース／データセット／システム等と組み合わせて（*13）当該個人データ（1*）の処理（2*）を行っているか、教えてください。詳細に説明してください。
- 例：はい。マネジメントや取締役の給与情報が評価目的の他の情報と組み合わせられています。

データマッピングの質問票シートB/Cの質問事項の詳細
1. 個人データが移転される国 (GDPR 44条)

- シートB: 個人データ(1*)の移転／アクセス可能（6*）先となる、EEA域(*7)外のグループ会社がどこか、説明してください。各法人について、当該法人が事業を営み、個人データの移転／アクセス可能となる（推定）先の国を特定してください。
- 回答例 1 - EEA域内子会社におけるマネジメント及び役員の人事評価: 日本HQ　[会社名] - 日本

- 個人データが移転されるあるいはそこからアクセスするEEA域外(日本を含みます。以下、質問票Cでは全て同様)の会社を記述してください。

- シートC: 以下双方をリストアップしてください。
- i) グループ会社（例：本社、子会社、兄弟会社）
- ii) グループ会社以外（例：ベンダー、パートナー、サービスプロバイダー）
- 各会社について、当該会社が事業を行い、おそらく個人データが移転されたり、そこからアクセスが行われる国（日本を含みます。以下、質問票Cでは全て同様）を記述してください。
- 回答例1 - 賃金の人事処理

データマッピングの質問票シートB/Cの質問事項の詳細
2. 適切な保護措置の対象となる移転(GDPR 46条)

- 2.1 個人データ（1*）の移転（6*）が、貴社及び個人データ（1*）の移転（6*）先企業間で締結されるSCC（8*）によってカバーされているかどうか教えてください。締結済みのSCCの写し又はサンプルを提出してください。
- 例：いいえ
- 2.2 個人データ（1*）の移転（6*）がデータ保護当局（9*）により承認された契約条項によりカバーされているか否か教えてください。当局から取得した承認と共に、締結済みの契約条項の写し又はサンプルを提出してください。
- 例：いいえ

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.1 なぜEEA（7*）域外に個人データ（1*）の移転（6*）をするのか説明してください。各目的について、個別に、かつ、詳細に、明確に特定・定義してください。当該移転の理由を説明するために必要があれば、個人データの移転先の会社の事業内容を説明してください。
- シートB
- 例: マネージャー及び役員のデータは、従業員のパフォーマンス評価のため、日本のHQである[会社名]に移転されている。
- シートC
- X社は当社グループに対するストレージおよびサーバサービスプロバイダーである。理由：管理目的による従業員データの保管

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.2 誰の個人データが移転されているのかを記述してください。（例. 従業員、消費者/ユーザー、ビジネスパートナーのコンタクト先、子ども等の社会的弱者）
- シートB
- 例: ドイツにある[会社名]のマネージャー
- シートC
- 例：従業員

データマッピングの質問票シートB/Cの質問事項の詳細
3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.3 この特定の目的に対して移転される個人データのカテゴリーをリストアップしてください。（例. 氏名、住所、電話番号、職業、クレジットカード番号、顧客番号等）
- シートB
- 例:
- - 姓、名
- - 住所
- - 電話番号
- - メールアドレス
- - 評価及びパフォーマンスに関するコメント
- - EEA域内の子会社である[会社名]、又はそれらが管理する部署に関する財務データ（給与データ）
- シートC
- 例：
- - 姓名
- - 住所
- - 電話番号
- - 電子メールアドレス
- - 評価とパフォーマンスコメント
- - 当社が管理するEEA子会社あるいは組織に関する財務データ（給与データ）

GIBSON DUNN

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.4 もしわかれば、移転後に、当該個人データにさらにアクセス可能になるであろう人、部署、法人等を教えてください。（例：データを受領する会社の特定の部署、子会社）
- シートB
- 例:
- - 日本のHQである[会社名]の会社管理部門（役会）
- - 日本のHQである[会社名]人事部及びIT部門
- シートC
- 例:
- - X社は当社グループに対するストレージ及びサーバサービスプロバイザーである。他の会社はアクセスを有しない。

GIBSON DUNN

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.5 おわかりになれば、移転後に移転先の会社においてどのようにデータの処理がなされるかを記述してください。（例. 移転先におけるサポート/プログラム/データベース/システム、処理業務内容等）
- シートB
- 例:
- - メール（データ及びコミュニケーションの移転）
- - Excel (トラッキングシート).
- - Word (メモランダム).
- - 紙ファイル (プリントアウト)
- シートC
- 例:
- - 電子メール
- - サーバフォルダ(Excel(トラッキングシート), Word(メモ))

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.6 もしわかれば、データ移転先の法人において、実際に当該個人データが保管される期間を教えてください。（実際にすぐ取り出せる形で保管されるのか、アーカイブ保存かを含む。）
- シートB
- 例:
- - メール (データ及びコミュニケーションの移転) - 日本のHQである[会社名]では、10年間のデータ保存ポリシーが適用される。
- - Excel (トラッキングシート) - サーバーに当該エクセルが保管される期間
- - Word (メモランダム) -サーバーに当該ワードが保管される期間
- - プリントアウト - 適宜シュレッドされる。
- シートC
- 例:
- - 永久保管

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.7 当該移転に関して行われる安全管理措置について、移転（6*）先の会社から説明を受けましたか。 詳細に説明するとともに、関連書類と情報を提出してください。
- シートB
- 例: いいえ
- シートC
- 例: ISO27001の承認を受けたセキュリティ手段を実装していることを参照したサービス契約書

データマッピングの質問票シートB/Cの質問事項の詳細

3. SCCを完成させるために必要な情報(GDPR 46(2)(c)条)

- 3.8 当該処理（2*）ないし移転（6*）について、管轄しているデータ保護当局（9*）に対して以前の書式が提出されているか否かわかりますか。もし回答が「はい」の場合、詳細と証拠を提出してください。
- シートB
- 例: いいえ
- シートC
- 例: いいえ

GIBSON DUNN

データマッピングの質問票シートB/Cの質問事項の詳細
4.データ主体に関する情報(GDPR 13条及び14条)

- データ主体（5*）には、当該個人データの移転に関して事前に知らせていますか。
- もし回答が「はい」の場合、使用している情報通知のサンプルを提出してください。例：ウェブサイト上のプライバシーポリシー該当箇所、従業員に回付されている「情報通知」、[会社]のユーザのための「プライバシーポリシー」
- シートB
- 例: いいえ
- シートC
- 例: いいえ

データマッピングの質問票シートB/Cの質問事項の詳細
5.その他の規制に基づく義務

- データ主体（5*）が貴社従業員である場合、彼らの個人データ（1*）の移転は、当該従業員／貴社労働評議会に対して通知されていますか。もし回答が「はい」の場合、かかる情報通知または合意書のサンプルを提出してください。
- シートB
- 例: はい。2002年の労働評議会との合意。
- シートC
- 例: はい。2002年の労働評議会との合意。

データマッピングの質問票シートDの質問事項の詳細
1. 処理の遵守とセキュリティ(GDPR32条)

- 1.1 処理に関する技術的、組織的なセキュリティに対する決まり事を行っていますか？以下のように説明ください。
- 1. 個人データの仮名化と暗号化を行っている。
- 2. 個人データ処理システムとサービスの機密性、完全性、可用性と復元性を保証する能力を有する（例. ファイアウォール）
- 3. 物理的あるいは技術的事故時にすみやかに個人データにアクセスできるように復元する能力を有する（例. バックアップ、アーカイブ）
- 4. 処理のセキュリティを保証する技術的、組織的手段の有効性に関する定期的なテスト、査定、評価プロセスを有する。
- 「はい」の場合は、それらの決まりごとを記載した文書を記載し、ご提示ください。それらの文書のサンプルまたはコピーをご提供ください。
- 注意: ITとセキュリティシステムに関するGDPR遵守性の査定に際しては提供して頂く情報をレビューするとともに、ITベンダーあるいはコンサルタントの支援が必要となります。
- 回答例 - EEAの子会社におけるマネジメント及び役員の人事評価
- はい。ドイツ拠点はISO27001認証を取得しており、承認されたセキュリティ手段をとっている。
- 1.2 貴社のIT部門は、IT及びセキュリティのシステムがGDPRに適合していることを確認するための内部/外部評価を計画済みあるいは計画していますか？
- 例: いいえ:　IT部門はGDPR評価を実施する予定はありません。ISO27001によりリスクに対して適切なレベルが確保されていると確信しています。

データマッピングの質問票シートDの質問事項の詳細

2.データが処理されるファイルリングシステム(GDPR2条1項および4条6項)

- 各ファイリングシステム(例. 紙ファイル、電子メール、Excel, CRMシステム, SAPシステム等)について、自社運用されているか外部委託されているかを記述してください。もし外部委託されている場合、お分かりになればその委託先企業を記述してください。
- 回答例 - EEAの子会社におけるマネジメント及び役員の人事評価
- - WordとExcel：ローカル保存とX社のサーバに保管
- - 電子メール：X社のサーバに保管
- - 紙ファイル：ローカルに保管

データマッピングの質問票シートDの質問事項の詳細

3.行動規範と認証(GDPR40条)

- 貴社は(GDPRで定義され、欧州委員会に承認された)行動規範を遵守している、あるいは、データ保護とセキュリティ義務に関するなんらかの組織に承認(GDPRで定義された承認)をうけていますか？

- 例: いいえ

III.　2018年5月25日までに対応を完了できる項目の作業完了
データマッピングの結果を踏まえて早期に対応可能な項目

1. 処理行為の適法性の確保・記録保持義務の履行
A)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

- 処理行為の目的ごとに、個人データの処理行為を洗い出す。
  - 個人データの処理行為を、業務ごとに列挙するだけでは足りない。
  - 処理の目的は、十分に特定的でなければならない。
  - 同じ種類の個人データを処理する場合でも、処理の目的によって適法性の有無が変わってくる。

1. 処理行為の適法性の確保・記録保持義務の履行
B)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

- 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作業部会の意見書(WP217)参照
- ポイント：特別カテゴリーの個人データ(センシティブデータ)（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）は、明示的な同意をはじめとするより追加の法的根拠のいずれかを満たさなければ、適法に処理することができない（第9条）。

1. 処理行為の適法性の確保・記録保持義務の履行
C)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

- 同意という法的根拠は、それ以外の法的根拠が使えない場合に初めて使う。
- 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。
- 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))

1. 処理行為の適法性の確保・記録保持義務の履行
D) 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

- 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

1. 処理行為の適法性の確保・記録保持義務の履行
E) 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）

- 管理者の義務：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
- ポイント：処理者にも処理行為の記録を残す義務がある。

2. 業務委託契約の見直しが必要となる第三者(処理者)を特定

- **ポイント：個人データ処理を伴う業務を委託する場合には、委託先である第三者（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委託している場合には、委託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。

3. データ保護影響評価の実行義務の有無を判定

データ保護影響評価（DPIA）とは？

- ポイント：作業部会のデータ保護影響評価のガイドラインは完成版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、欧州データ保護会議に通知する。欧州データ保護会議により、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）。

3. データ保護影響評価の実行義務の有無を判定(2)

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装置や内部通報制度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：作業部会の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

3. データ保護影響評価の実行義務の有無を判定(3)

「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。

3. データ保護影響評価の実行義務の有無を判定(4)

「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。

3. データ保護影響評価の実行義務の有無を判定(5)

「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。

3. データ保護影響評価の実行義務の有無を判定(6)

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	

GIBSON DUNN

4. データ保護責任者の選任義務の有無を判定

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。

4. データ保護責任者の選任義務の有無を判定(2)
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。

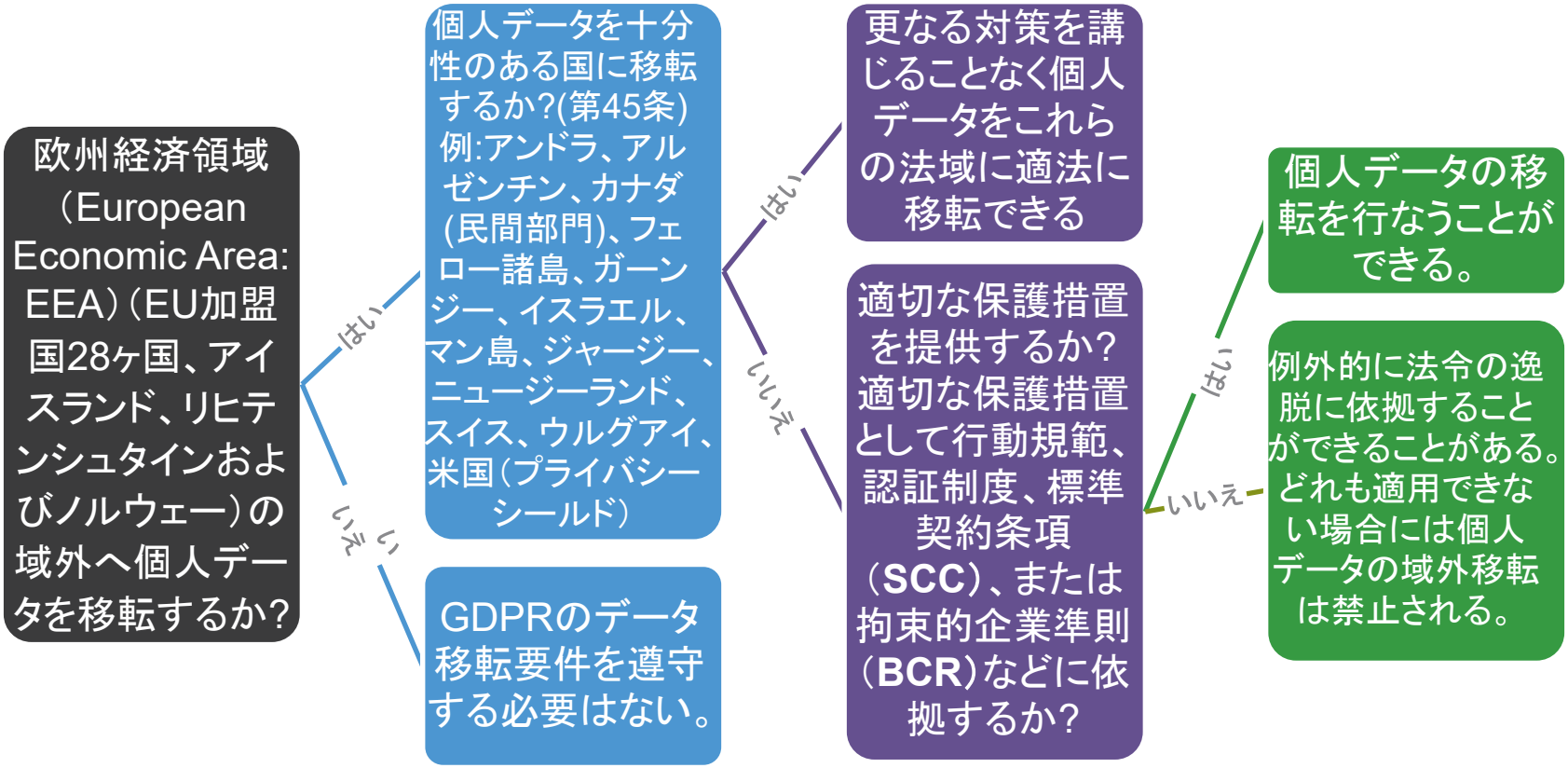
4. データ保護責任者の選任義務の有無を判定(3)
どこの誰をDPOとして選任できるかを検討する

- 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。
  - 第29条作業部会の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）

個人データの移転

- 移転規制には、事業者グループ内での域外移転については、域外拠点からの再度の移転を除き、対応完了することは不可能ではない。
  - 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・締結

個人データ移転規制：概要



GIBSON DUNN

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。また、BCRを利用する企業の数も順調に増加している。
- 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。産業界では2018年3月初め時点で少なくとも数社のBCR申請が完了。**
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。
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。

GIBSON DUNN

標準契約条項を締結しているか？
ANNEX B - DESCRIPTION OF THE TRANSFER

- 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。
  - Data subjects - The personal data transferred concern the following categories of data subjects:
  - Purposes of the transfer(s) - The transfer is made for the following purposes:
  - Categories of data - The personal data transferred concern the following categories of data:
  - Recipients - The personal data transferred may be disclosed only to the following recipients or categories of recipients:
  - Sensitive data (if appropriate) - The personal data transferred concern the following categories of sensitive data:
  - Data protection registration information of data exporter (where applicable)
  - Additional useful information (storage limits and other relevant information)
  - Contact points for data protection enquiries

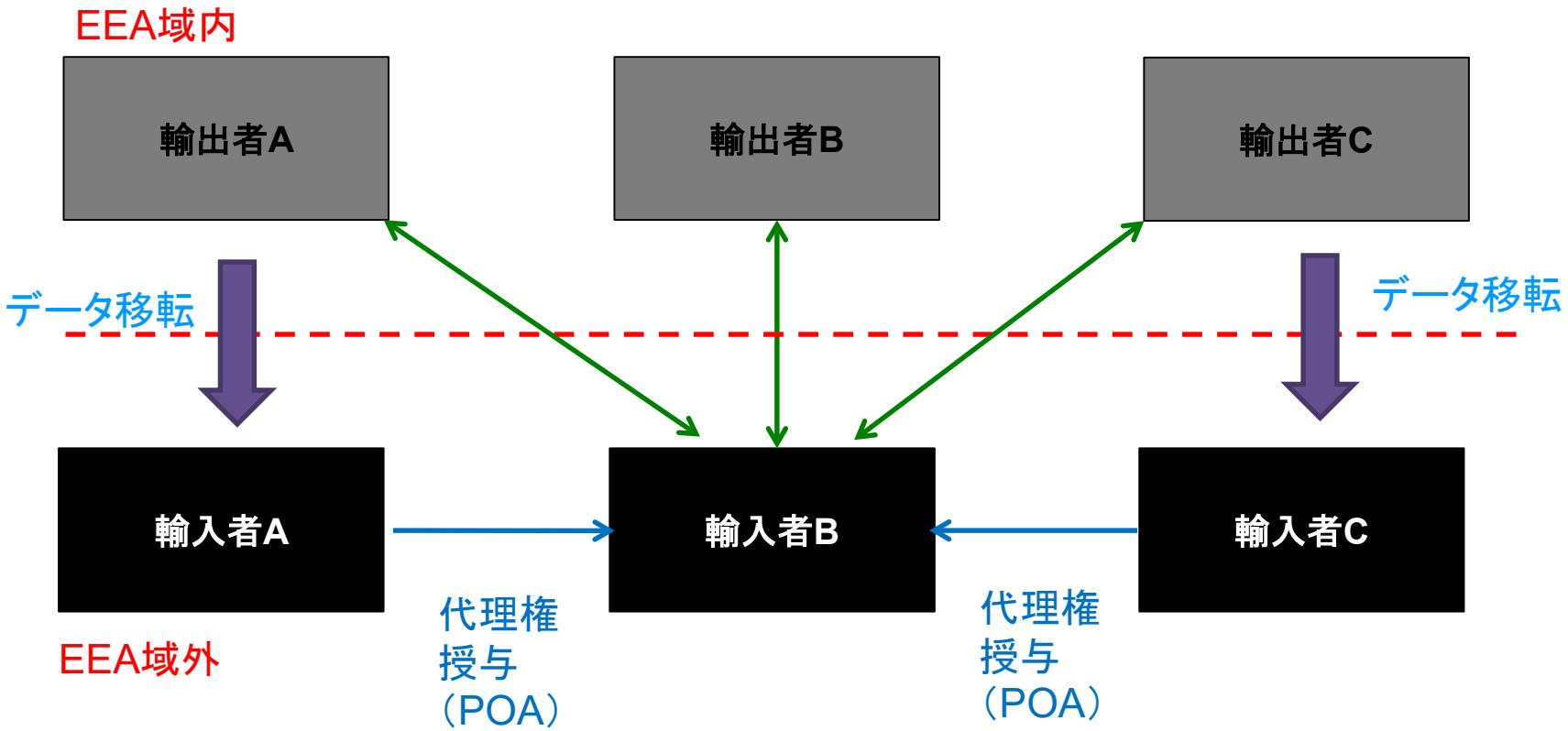
事業者グループのEEA内拠点からどこへの移転か？
標準契約条項（SCC）

- 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（作業部会が提案した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	作業部会は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。

複数当事者間のデータ移転①

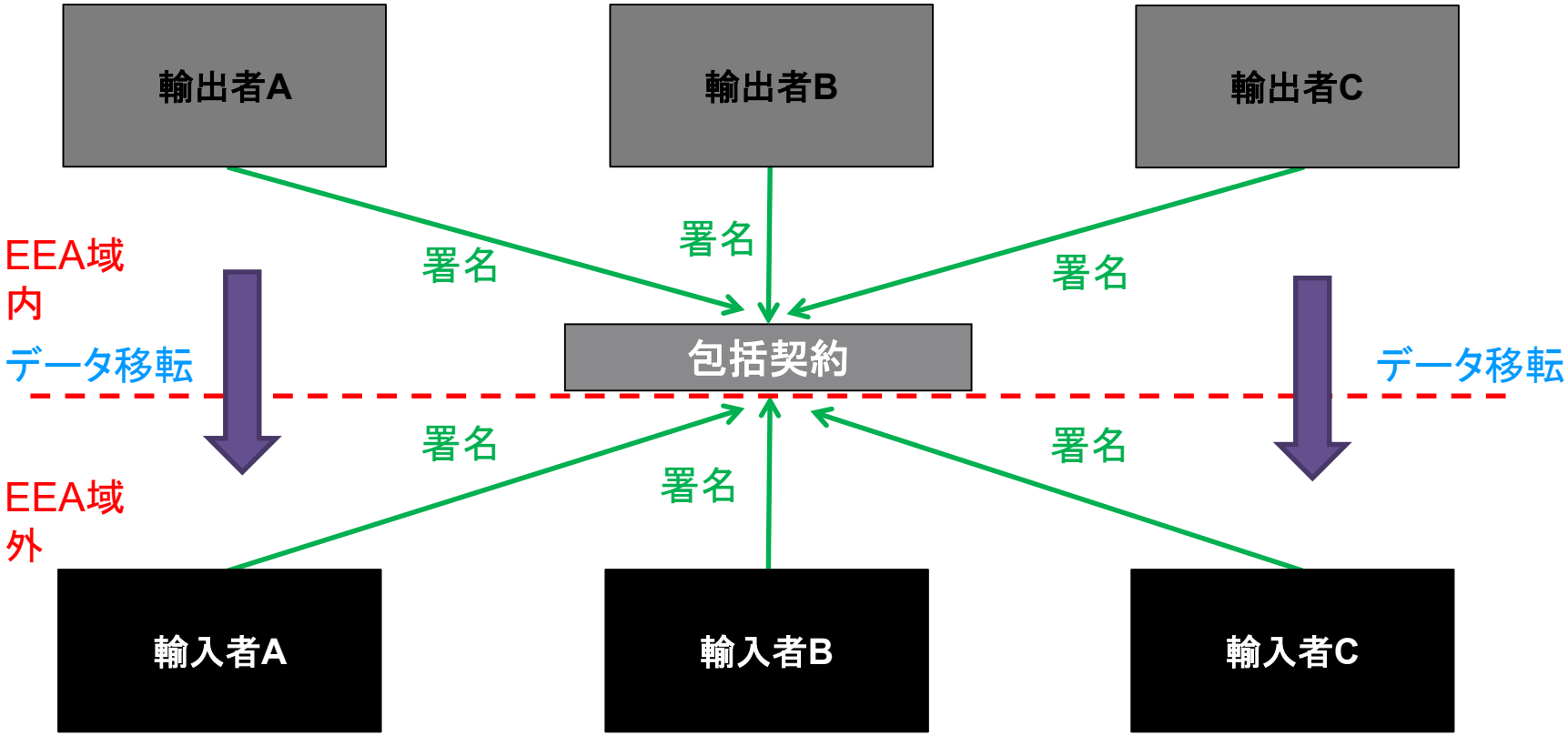
EEA内は個別にSCCを締結、EEA外の拠点は代理権授与方式



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

GIBSON DUNN

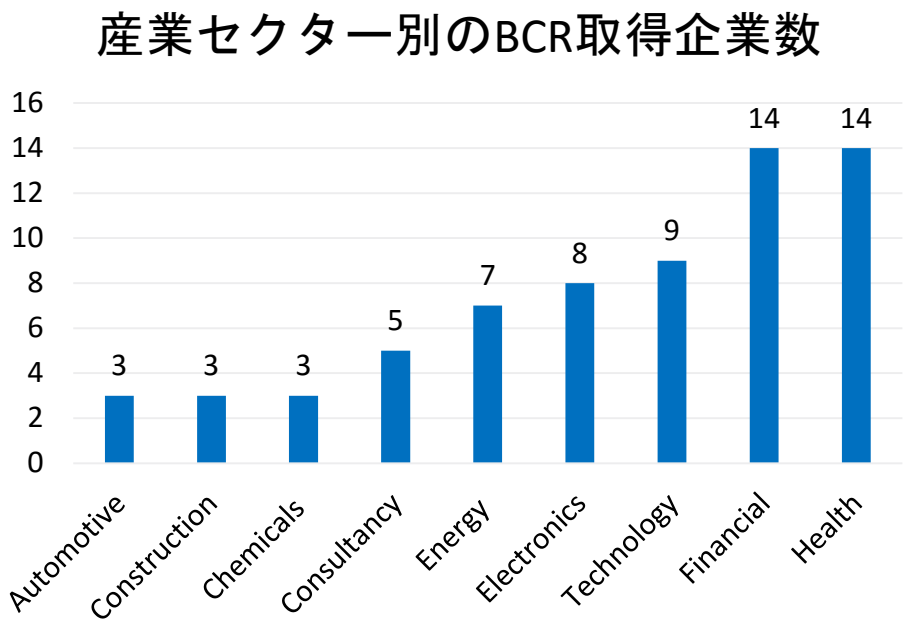
複数当事者間のデータ移転②
SCCを多数当事者間契約として締結する

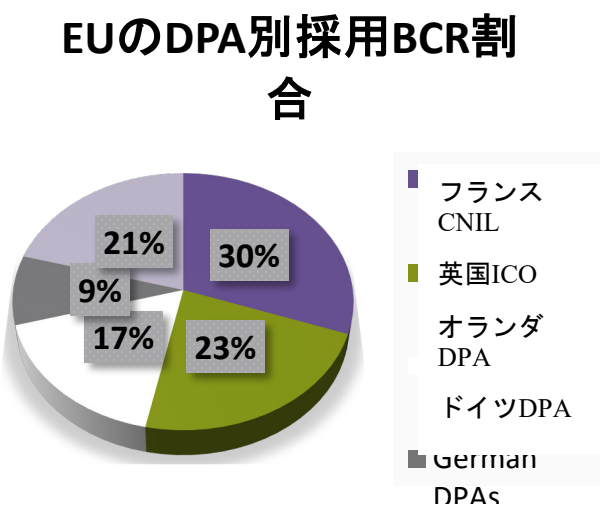


SCC中のデータ輸入者の義務を履行するべく社内体制の構築をEEA外を含む日本本社においても推進

拘束的企業準則（BCR）

- BCRは、企業グループ内部の個人データの移転および処理を対象として企業グループによって採択されるGDPRにおいて承認されたデータ保護に関する内部方針である。BCRはデータ保護監督当局による審査・承認を受ける必要がある
- 日本の産業界におけるBCRの申請状況：少なくとも日本企業数社がBCR承認申請中。世界で計87社が欧州データ保護監督当局からBCR承認を取得済み。





GIBSON DUNN

同意によって従業員データを移転させる

- 多くの会社は従業員の同意に基づきEEA外へ従業員の個人データを移転させることを求める
  - データ主体の同意は自由に与えられ、個別の、情報に基づく、不明瞭ではないものであり、さらに明示的である必要がある
  - 同意は個別になされなければならない。長く複雑な就業規則において個人データの移転に対する従業員の同意を得ることは同意の要件を満たさない可能性が高い
  - 従業員の同意の取得にあたっては、区別された別個のフォームを使うことが薦められる
  - グローバルタレントマネジメントシステムの導入において従業員の同意で行うことは執行リスクの観点からお薦めできない。SCCを使うべきである
  - 同意は非常に制限的である
    - データ主体がいつでも同意を撤回できる。
    - 企業は関係する全ての人から同意を取得する必要がある
    - 繰り返し行なわれ、大量で、かつ構造的であると認められる可能性がある個人データの移転は、可能であればSCCやBCRのような適切な保護措置の下で行なわれるべきである(WP114. p.9参照)

IV. 2018年5月25日までに対応を完了できる項目の作業完了

GDPRに関連する社内規程類・マニュアルの作成・導入（データマッピングの結果の一部または全部を前提とせずとも推進できる）

- 以下の社内規程、外部向けポリシー、各種マニュアル・フォーマット等を英語で作成し、一通りGDPRの適用対象となるEEA内外の拠点に備えることで、監督当局からGDPRへの遵守の状況に関する説明を求められたときに、一通りの説明をできるようにしておく。各拠点毎の改訂作業やそれに基づく運用については5月25日以降に作業を行う。

1. 個人データ保護規程（社内規程）の作成－社内で誰が法的根拠を判断するのかのメカニズムの構築がポイント
2. プライバシーポリシー（社外向け）の作成
3. 同意のフォーマットの作成
4. 情報通知のフォーマットの作成
5. 個人データ侵害通知の場合の72時間以内の監督当局への報告義務やデータ主体への個別の報告義務の履行のためのマニュアルの作成－誰が報告義務の有無を判断するかがポイント
6. データ主体の権利行使に対する対応マニュアルの作成
7. データ保護影響評価の実行義務の判断と同評価の実行に関するマニュアルの作成
8. 処理者との間で提供する処理契約の条項のフォーマットの作成
9. データ保護責任者の書面による選任と監督当局への連絡先（氏名は必要的ではない）の通知

V. 2018年5月25日までに対応を完了できない項目の洗い出しおよび対応完了に向けたロードマップの作成

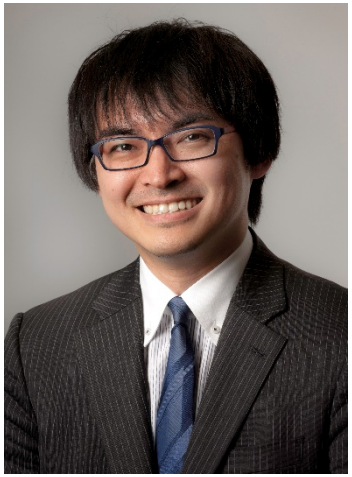
- 2018年5月25日までに対応を完了できない項目の洗い出し→以下の事項は多くの企業が5月25日までに対応を完了させることが難しい項目になるため、できるだけ5月25日より前に完了させることが望ましいが、実際には、以下の事項を5月25日以降、いつの時点で対応完了させることができるかのロードマップを作って説明責任を果たせるよう備えておく必要があるものと考えられる。

1. 個人データの処理に関する業務委託契約に関する第三者との処理契約の締結
2. 個人データの域外移転に関するSCCの締結（グループ外の第三者とのSCCの締結）
3. 各種社内規程・外部向けポリシー・各種マニュアルに関する各拠点でのカスタマイズ
4. 同意のフォーマットや情報通知のフォーマットの各拠点におけるビジネスフローに応じたカスタマイズ
5. 各拠点におけるGDPRに関するトレーニング
6. 各拠点におけるセキュリティアセスメントと改善事項の洗い出し、改善策の立案と実行
7. 新しい処理行為に関するデータ保護影響評価の実行
   - 誰が新しい処理行為について法的根拠を判断しデータ保護影響評価の実行義務を判断するかのメカニズムがポイント

第3 まとめ

まとめ―適切なGDPR対応を行うためのポイント

- 適切なGDPR対応を行うためのポイント
  - 欧州のデータ保護監督当局の執行の視点
    - 当局者による仕事の評価（内部評定）は、立件した件数と立件した案件の重大性が基礎となる。案件の重大性は、制裁金決定における制裁金金額が大きいことが分かりやすい。
    - 当局者は人的なリソース不足にあえいでいる。次年度に数多くの職員を採用するためには、当局が執行において結果を残すことが重要である。
  - 欧州における個人データ保護に対する考え方・文化が、日本におけるそれとは違うという相違点の受容
    - 一般的に、日本企業にとって執行リスクが低いのにも関わらず個人データ保護の問題によってビジネスを止めてしまうことはありえないが、欧州では個人データ保護の問題によってビジネスを止めることは許されるという風潮はたしかにある。
    - 日本企業が欧州のデータ保護法のコンプライアンスの実務で苦戦するのは、GDPRという法規に対する対応そのものでは実はなく、欧州との個人データ保護に対する考え方・文化の相違点から生起する論点である。
    - 欧州の考え方・文化に対する深い敬意を払い、真摯に向き合いつつも、日本企業・組織として、毅然とした態度で、適切なリスク評価に基づいて、大胆にGDPR対応を進めていくことが重要である。



杉本 武重
Takeshige Sugimoto, CIPP/E

tsugimoto@gibsondunn.com
Direct　+32 2 554 7280
Mobile +32 499 05 46 19(ドイツ)
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）
同年	同会所属

ギブソン・ダン・クラッチャー法律事務所ブリュッセルオフィス
オブ・カウンセル　弁護士　杉本　武重

経歴

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、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
- 国際的な腐敗行為防止法コンプライアンス

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）

Our Offices

Beijing
Unit 1301, Tower 1
China Central Place
No. 81 Jianguo Road
Chaoyang District
Beijing 100025, P.R.C.
+86 10 6502 8500

Brussels
Avenue Louise 480
1050 Brussels
Belgium
+32 (0)2 554 70 00

Century City
2029 Century Park East
Los Angeles, CA 90067-3026
+1 310.552.8500

Dallas
2100 McKinney Avenue
Suite 1100
Dallas, TX 75201-6912
+1 214.698.3100

Denver
1801 California Street
Suite 4200
Denver, CO 80202-2642
+1 303.298.5700

Dubai
Building 5, Level 4
Dubai International Finance Centre
P.O. Box 506654
Dubai, United Arab Emirates
+971 (0)4 318 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt
Germany
+49 69 247 411 500

Hong Kong
32/F Gloucester Tower, The Landmark
15 Queen's Road Central
Hong Kong
+852 2214 3700

Houston
1221 McKinney Street, Suite 3700
Houston, Texas 77010-2046
+1 346.718.6600

London
Telephone House
2-4 Temple Avenue
London EC4Y 0HB
England
+44 (0) 20 7071 4000

Los Angeles
333 South Grand Avenue
Los Angeles, CA 90071-3197
+1 213.229.7000

Munich
Hofgarten Palais
Marstallstrasse 11
80539 Munich
Germany
+49 89 189 33-0

New York
200 Park Avenue
New York, NY 10166-0193
+1 212.351.4000

Orange County
3161 Michelson Drive
Irvine, CA 92612-4412
+1 949.451.3800

Palo Alto
1881 Page Mill Road
Palo Alto, CA 94304-1125
+1 650.849.5300

Paris
166, rue du faubourg Saint Honoré
75008 Paris
France
+33 (0)1 56 43 13 00

San Francisco
555 Mission Street
San Francisco, CA 94105-0921
+1 415.393.8200

São Paulo
Rua Funchal, 418, 35°andar
Sao Paulo 04551-060
Brazil
+55 (11)3521.7160

Singapore
One Raffles Quay
Level #37-01, North Tower
Singapore 048583
+65.6507.3600

Washington, D.C.
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-5306
+1 202.955.8500