「欧州における個人情報保護法制の特徴～GDPRの概要と対応策 – 当局のガイドラインを踏まえて～」
（個人情報の域外移転セミナー～グローバル・ビジネスにおける域外移転対策の具体的なアプローチ～）
（2018年3月）

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 72 80 (直通)
+ 32 499 05 46 19 (携帯)
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

I. GDPRの基本概念

GIBSON DUNN

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

▪罰和を増大させる。

▪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。

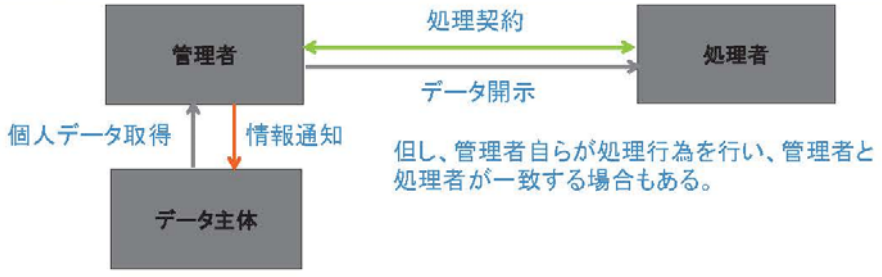
制裁金の基準	違反行為の類型
管理者または処理者が、右記に当てはまる場合、1000万ユーロ以下、または事業者の場合には、事業者の全世界年間売上高の2%以下のいずれか高い方	▪ 16歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者による同意または許可が必要という条件に従わなかった場合(第8条) ▪ GDPR要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合(第25条、第28条) ▪ 義務があるのにEEA代理人を選任しない場合(第27条) ▪ 責任に基づいて処理行為の記録を保持しない場合(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))

GIBSON DUNN

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。



GIBSON DUNN

GDPRの適用範囲(第3条)

- ポイント：GDPRはEEA外の拠点（日本本社等）が行う個人データの処理に対して直接適用されることがある。例えば、日本本社のウェブサイトにおいてEEA所在者からの質問等の連絡を受け付けている場合は、EEA所在者の個人データを、EEA内の管理者（英国子会社等）の事業所の活動に関連して処理すると評価され、GDPRの直接適用がありうる。
- ポイント：GDPRの適用範囲は非常に広範である。

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
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。** 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

II. 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-制裁金決定を回避するための戦略的思考

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思考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。

III. GDPR上の個人データの処理

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（説明責任）。

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
- ポイント：処理者にも処理行為の記録を残す義務がある。

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）。

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。
- 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) – 特別カテゴリの個人データの処理の適法性(第9条)

- 特別カテゴリの個人データは、要保護性が高いため、監督当局による制裁金賦課やデータ主体による損害賠償請求を受けないようにするため、特に処理の適法性に留意する必要がある。特別カテゴリ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？(2)
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

GIBSON DUNN

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？(3)
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。

GIBSON DUNN

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委託する場合または既に委託している場合には、委託先である第三者（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？

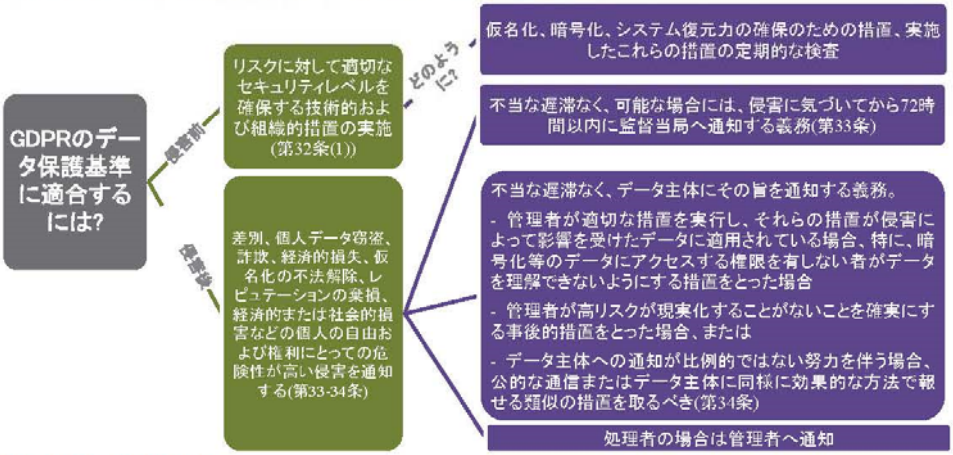
- **ポイント：個人データ処理を伴う業務を委託する場合には、委託先である第三者（処理者）との間で締結する業務委託契約のひな型に下の条項が網羅されていることを確認する。既に個人データ処理を伴う業務を委託している場合には、委託先である第三者との業務委託契約の見直しを行う。**
- 管理者から処理者への処理行為の委託は契約もしくはEU法または加盟国法（管理者に関する処理者を拘束し、処理の対象事項および期間、処理の性質および目的、個人データの種類およびデータ主体の種類ならびに管理者の義務および権利を定める法）に基づく法律行為に基づかなければならない（第28条第3項）。
  - 処理者が従うべきEU法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。

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

- 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。
- ポイント：事業者グループのEEA拠点における個人データ処理のセキュリティの状況について自社のセキュリティチームまたは外部のセキュリティの専門家を使い、まず現状把握を行う。
- GDPRとの関係でセキュリティ対策は取ったか？取っていないとして、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、制裁金賦課のリスクはない程度の対応を行ったといえるか？
- リスクに対して適切なセキュリティレベルを確保するため、適切な技術的・組織的対策の実施の方法を検討
  - 検討される選択肢
    - 仮名化
    - 暗号化
    - システムの復元力を確保する方法
    - ISO 27000
  - 実施する方法のテストを頻繁に行う

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

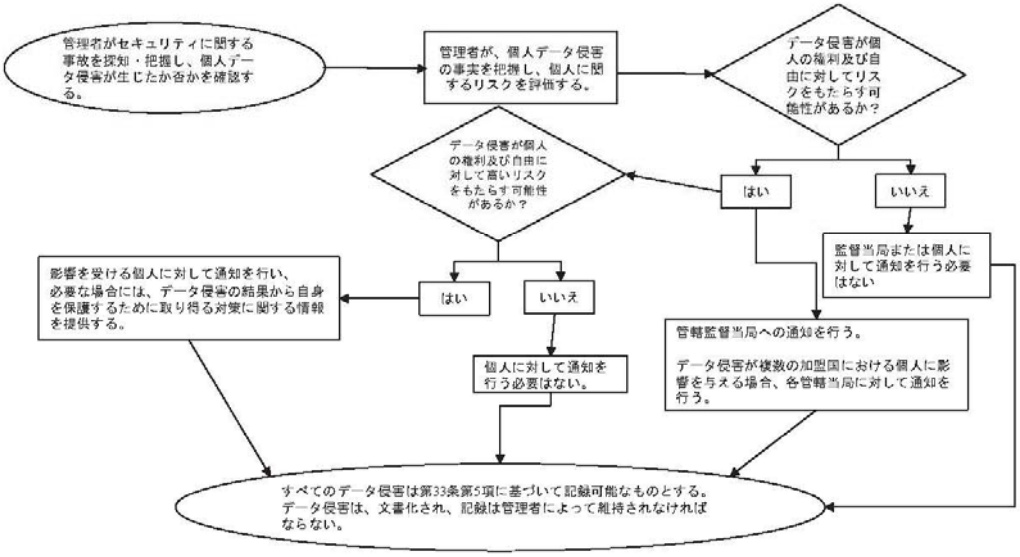
- ポイント：仮にサイバーアタックに遭い、個人データが漏えいした場合に、制限時間内に監督当局やデータ主体に通知できるように、個人データ侵害通知のマニュアルを作成し、トレーニングを行う。



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作業部会のガイドラインのドラフトが公表されており、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



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：作業部会の個人データ侵害通知のガイドラインのドラフトに記載されている具体例は本頁以降のスライドの表で網羅されている。

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第29条作業部会は推奨する。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：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）。

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

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。

GIBSON DUNN

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	

GIBSON DUNN

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/EI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

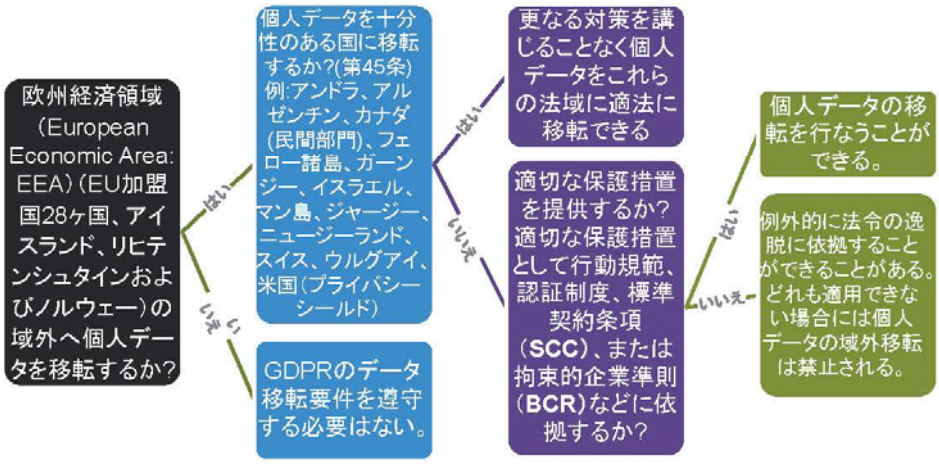
- 管理者および処理者は、次のいずれかの要件を満たす場合にはDPOの選任義務あり
  - 処理が公的機関または団体によって行われる場合（但し、司法権に基づく裁判所の行為を除く）
  - 管理者または処理者の中心的業務が、その性質、適用範囲および/または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする作業である場合
  - 管理者または処理者の中心的業務が、第9条で言及された特別カテゴリーの個人データまたは第10条で定める有罪判決および犯罪に関する個人データを大規模に処理する場合、または
  - EUまたは加盟国の法律(例：ドイツ)でDPOの選任が義務付けられている。
    - 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？
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）

IV. GDPR上の個人データの移転

個人データ移転規制：概要



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。

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

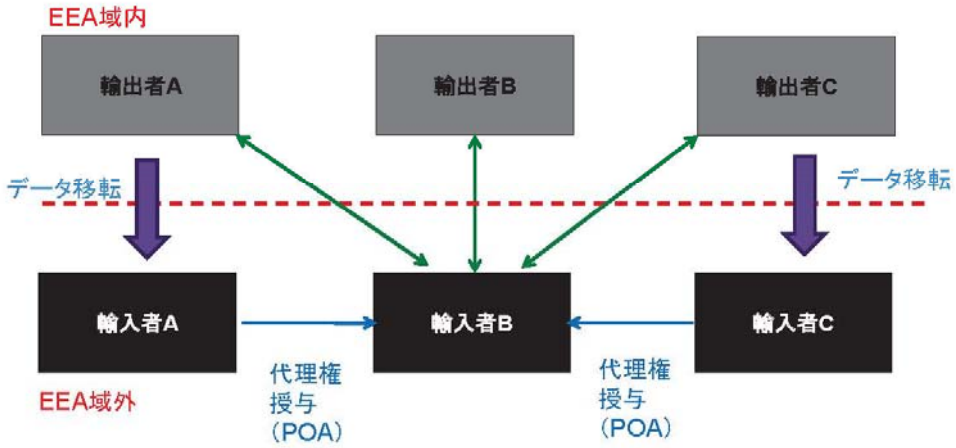
事業者グループのEEA内拠点からどこへの移転か？
標準契約条項（SCC）

- 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

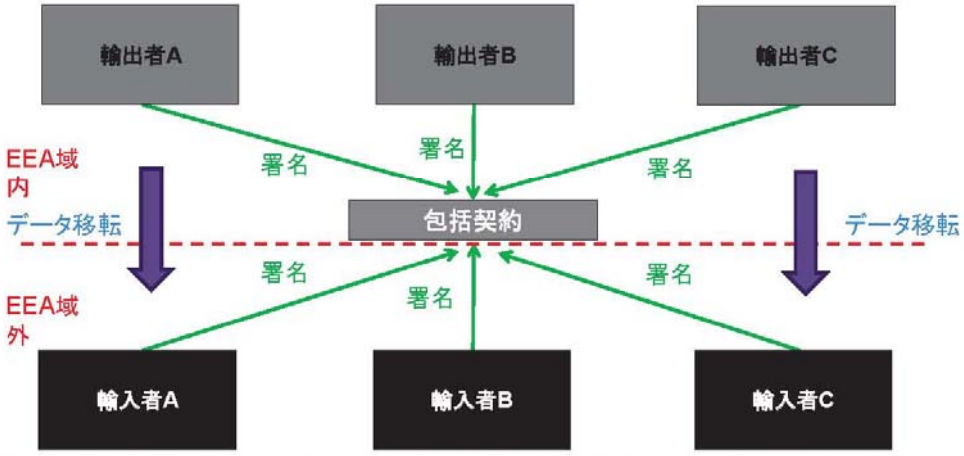
EEA内は個別にSCCを締結、EEA外の拠点は代理権授与方式



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

複数当事者間のデータ移転②

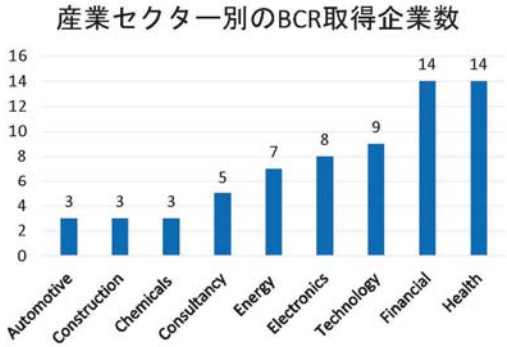
SCCを多数当事者間契約として締結する

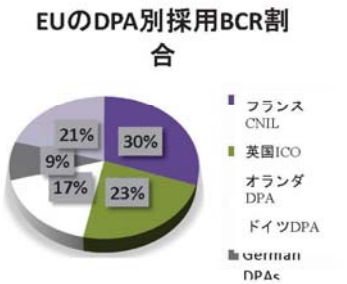


SCC中のデータ輸入者の義務を履行するべく社内体制の構築をEEA外を含む日本本社においても推進

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。





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)

V. 同意に関するガイドライン（WP259）（第29条作業部会2017年11月28日付採択）

1.はじめに

- 同意に関しては、同意の定義に関する意見書（WP187）が存在する。本ガイドラインは、既存の意見書を発展させ、完成させるためのものである。
- 電子プライバシー規則における同意の概念は、GDPRにおける同意の概念と関連する。

2.GDPR第4条(11)の同意

- 第4条第11号：同意とは、自由に与えられ、特定的に、情報提供を受けたうえでかつ曖昧でないデータ主体の意思表示を意味する。その意思は、当該データ主体が、陳述または明らかな積極的行為によって、自己に係る個人データの処理に関する合意（agreement）を表示するものである

3.有効な同意の要素

- 第4条第11号からは、以下の要素が導かれる。
  - 自由に与えられたこと
  - 同意の範囲が特定されていること
  - 同意に関する事前の情報提供が十分であること
  - 曖昧でないデータ主体の意思表示であること
  - 陳述または明確な積極的行為によること

3.1.自由に与えられた

- 以下の場合、自由に与えられたとはいえない。
  - データ主体に真正な選択の余地がない場合
  - 同意を強制されたとデータ主体が感じる場合
  - 同意しない場合、不利益な結果をデータ主体が受忍しなければならない場合
- 同意が交渉の余地がない取引条件に組み込まれた場合、自由に与えられた同意ではないと推定される。
  - 例：写真編集のためのモバイル・アプリは、ユーザーに対してサービスの利用に関してGPS位置情報のアクティベートを要求する。アプリは、収集されたデータは行動分析型広告のために利用するとしている。位置データおよびオンライン上の行動型広告は写真編集サービスの提供に必要ないものであり、提供される中心的なサービスの範囲を超えている。ユーザーは、これらの利用目的について同意しない場合にはアプリを利用できないことから、同意は自由に与えられたとは考えられない。

3.1.自由に与えられた
3.1.1.力関係の不均等

- 前文43項に明記のとおり、管理者とデータ主体との間に力関係の明らかな不均衡がある場合、同意は有効な法的根拠とすべきではない。典型的には管理者が公的機関、雇用主である場合。
- ただし、以下のようなケースでは、同意が法的根拠として認められる。
  - 市役所が道路工事による通行止など道路情報をメールで提供することを目的に、メールアドレスを利用することの同意を求めた。同意しなくても市役所のサービスを受けることや市民としての権利行使には影響しないので、市民は自由に同意は拒否することができる。すべての道路情報は市役所のwebサイトにも掲出される。
  - 土地所有者が(建築目的などで)複数の公的機関(州、市)の許可を必要としている。両自治体はデータベースを相互接続しておらず、別々の許可申請が必要。両自治体は重複申請をしなくてすむよう、土地所有者の個人データを含むデータベースのマージについて同意を求めた。同意は任意であり、同意しなくても従前どおり別々に許可手続をとることはできる。
  - 公立学校が生徒の写真を校内誌の記事に掲載することについて同意を求める。同意は任意であり、同意しなくても、受けられる教育サービスに影響をおよぼすことはない。
- 雇用主と従業員の力関係を考慮すると、職場におけるカメラ監視、人事評価シート記入などの個人データ処理に対する同意要求に従業員が圧力を感じないで自由に応じられる可能性は低い。第29条作業部会は、職場における個人データ処理の従業員の同意は任意性を欠く可能性が高いとして問題視している。

3.1.自由に与えられた
3.1.1.力関係の不均等(2)

- もっとも、雇用主が処理の法的根拠として同意に常に依拠できないわけではない。同意が実際に自由に与えられていることを雇用者が実証することが可能な状況もあり得る。雇用者と従業員の間の力の不均衡を考えると、従業員は例外的な状況においてのみ同意の有無によって不利益を受けないといえる (See also Opinion 2/2017 on data processing at work (WP249), paragraph 6.2.) 。
  - 例：映画クルーが、オフィスの特定の部分で撮影を行うことを予定している。 雇用主は、映像の背景に表示される可能性があるため、その場所に座っているすべての従業員に対し、撮影に関する同意を求める。撮影されたくない従業員は、罰を受けることなく、撮影中は建物内の別の場所で同等の執務デスクが与えられる。
- 力関係の不均衡は、公的機関や雇用者に限定されず、他の状況でも起こり得る。

3.1.自由に与えられた
3.1.2.条件

- 第7条第4項：同意が自由になされているかについて判断する際、サービス約款を含む契約の履行が、当該契約の履行に必要のない個人データの処理に対する同意を条件としているか否かについて、最大限の考慮がなされなければならない。
- 前文43項：個別に同意することが適切であるにもかかわらず、異なる個人データ処理業務毎に個別の同意をすることができない場合、また、契約の履行に同意は必要ないにもかかわらず、サービスの提供を含む契約の履行が同意に依存している場合、当該同意は自発的に行なわれなかったものと推定される。

3.1.自由に与えられた
3.1.2.条件(2)

- 取引条件との抱き合わせまたは契約の履行やサービスの提供に必要ではない個人データ処理との紐つけは非常に望ましくない。
- このような同意は任意ではないと推定される（前文43項）。
- 同意が求められている個人データの処理が直接的または間接的に相手方の契約の履行になってはならない。個人データの処理の法的根拠である同意および契約の履行は、統合されたり、境界が曖昧になってはならない。
- 契約履行に不必要な個人データの処理は、契約履行またはサービス提供の義務的な対価にはなり得ないという強い推定が働く。
- 契約の履行に必要な個人データ処理であるかどうかは、厳格に解釈すべきである。配送のための住所、支払いのためのクレジットカード情報、給与振込のための給与情報、銀行口座情報など、契約履行の目的と個人データ処理との間に直接的かつ客観的な関連性がある必要がある。しかし、このような場合、適切な法的根拠は「契約の履行のための必要性」となる可能性が高い。

3.1.自由に与えられた
3.1.2.条件(3)

- 管理者が実際に契約の履行に必要な個人データを処理しようとする場合、適切な法的根拠は第6条第1項(b)の契約である可能性が高い。この場合、同意など他の法的根拠を用いる必要はなく、第7条第4項は適用されない。契約履行の必要性は特別カテゴリーの個人データを処理するための法的根拠ではない（第9条第2項参照）。
- 第7条第4項の「最大限の考慮」という文言は、絶対的に否定する趣旨ではないと考えられる。もっとも、「推定する」との文言は、極めて限られた場合においてのみ、同意を条件とすることが許されることを明確に示している。
- 推定を反証する立証責任は管理者側にある。

3.1.自由に与えられた
3.1.2.条件(4)

- 管理者は、追加的な目的のための個人データの使用に関する同意を伴うサービスと追加的な目的のための個人データの使用を伴わない同等のサービスの間において選択ができる場合、組織がデータ主体に対して実質的な選択を提供していると主張できる可能性がある。他のまたは追加のデータ使用に同意することなく、管理者により契約が履行されまたは契約したサービスが提供される可能性がある限り、条件付サービスではないといえる。しかし、両方のサービスは、追加的なコストがかからないことを含め、真に同等な内容である必要がある。
- 同意が自由に与えられているかどうかを評価する際には、第7条第4項に規定されている契約またはサービスの提供と同意を紐づける特定の状況のみを考慮すべきではない。
- 第7条第4項は、非限定的な規定であり、本規定が適用される一定のその他の状況が存在する可能性がある。一般論として、データ主体の自由意思の行使を妨げるデータ主体に対する不適切な圧力または影響といった要素（多くの異なる方法で示される可能性がある）がある場合、同意は無効となる。

3.1.自由に与えられた
3.1.3.粒度

- あるサービスが複数の個人データ処理を伴う場合、データ主体はそれぞれの個人データ処理に対する同意と拒否を自由に選択できなければならない。各データ処理について別々に同意を与えることを認められない場合、そのような同意は自由に与えられていないと推定される（前文43項）。
  - 例：同じ同意の要請において、小売業者が顧客に対して、マーケティング目的の電子メールを送信することおよび顧客の個人データを他のグループ会社と共有することについて同意を求めた。2つの目的について別々に同意が存在しないことから、適切な粒度を欠き、有効な同意ではない。

3.1.自由に与えられた
3.1.4.不利益

- 管理者は、不利益を伴うことなく同意を拒否または撤回することが可能であることを証明する必要がある（前文42項）。例えば、管理者は、同意の撤回がデータ主体に何らのコストをもたらさず、同意を撤回した者に明確な不利益をもたらさないことを証明する必要がある。

3.2.特定性

- 同意は、一つの又は複数の特定された個人データ処理の目的について与えられなければならない。(第6条1項(a))
- それぞれの目的ごとに、同意するか拒否するかを選択できなければならない。
- 個人データ処理の目的限定の原則(第５条第1項(b))との関係
  - 個人データは、特定され、明確で、適法な目的のために取得しなければならず、これらの目的と適合しない方法で処理してはならない。
  - 同意が有効であるには、同意取得に先立って、意図した個人データ処理について、特定され、明確で、適法な目的が決定されていなければならない。
  - 同意の対象範囲の特定の要請およびデータ処理の目的限定の原則は、データ処理の目的がなし崩し的に拡大し、曖昧になることに対する保護措置として機能する。

3.2.特定性(2)

- 同意取得の際に説明した目的とは別の新たな目的のために個人データを処理しようとする場合には、管理者は、新たな目的について新たに同意を取得しなければならない。
  - 例：ケーブルTV運営会社は、視聴履歴に応じて視聴者ごとに番組を宣伝することを目的に個人データを処理している。同社が第三者によるターゲティング広告のために視聴履歴を利用するには、視聴者から新たな同意を取得しなければならない。
- 適切な粒度で同意を取得することは、同意の任意性の要求を満たすために必要であるだけではなく、同意の特定性の要求を満たすためにも必要である。したがって管理者が複数の目的のために同意を求めようとするときには、それぞれの目的毎に別のオプトインの意思表示手段を提供しなければならない。
- 複数の目的のために同意を求めようとするときには、それぞれの同意要求毎に別々の情報提供を行い、各同意毎にデータ主体がどのような影響を受けるかについて理解できるようにしなければならない。

3.3.情報が与えられた

- GDPRは、同意について情報が与えられていることという要件を強化する。第5条に基づき、透明性の要件は、公正性および適法性の原則に密接に関連する基本原則の1つである。 同意を得る前にデータ主体に情報を提供することは、情報に基づいた決定を行い、同意の対象を理解し、同意を撤回する権利を行使するために不可欠である。

3.3.情報が与えられた
3.3.1.情報が与えられた同意といえるための最低限の条件

- 第29条作業部会は、同意取得の前に、最低限、以下の情報提供が必要であるとする。
  - 管理者の識別情報
  - 同意取得の対象となる各個人データ処理の目的
  - 取得・処理するデータの種類
  - 同意を撤回する権利があること
  - プロファイリングを含む自動処理のみに基づく決定のために個人データが利用されるかどうか（第22条第2項）
  - 十分性認定を受けていない第三国への適切な保護措置がない個人データ移転を伴う場合、想定されるリスク（第49条第1項(a)）
- 複数の管理者もしくは共同管理者が同意を求める場合または別の管理者への個人データ移転を想定している場合、すべての管理者の名前が示されなければならない。
- 処理者の特定は、同意取得に関する情報提供においては必要ではない。ただし、第13条または第14条に基づき、受領者または受領者の種類（処理者も含む）に関する情報を提供する必要がある。

3.3.情報が与えられた
3.3.2.情報提供の方法

- 形式
  - 同意取得の前に行う情報提供の形式について、GDPRは特別に規定していない。
  - 書面、口頭、音声またはビデオメッセージ等、様々な形式が可能である。
- 明確かつ平易な言葉
  - 情報提供は、明確かつ平易な言葉でなければならない。平均的な一般人にとって容易に理解できるものでなければならない。
  - 管理者は、法律の専門用語が多く含まれた長くて読みにくいプライバシー・ポリシーまたはステートメントを使用することはできない。同意は、他の事項と明確に区別でき、理解しやすく、容易にアクセスできる形式で提供されなければならない。当該要件は、本質的には、基本的には、同意するか否かに関する意思決定に関連する情報は一般的な条件に隠れてはならないことを意味する。
- 電子的手段による同意の取得
  - 電子的手段で同意を取得する場合、明確かつ簡潔に同意取得の要請を行う必要がある。簡潔かつ完全な情報提供を行う観点からは、階層化し、粒度の高い情報提供を行うことが適切である。
- 管理者は、情報提供を受ける者の種類にも配慮する必要がある。例えば、未成年者を対象とする場合、情報が未成年者にとって理解可能であることを確保する必要がある。

3.3.情報が与えられた
3.3.2.情報提供の方法(2)

- 第7条第2項は、他の事項に関連する事前に作成された同意に関する宣誓について規定する。同意書が紙による契約の一部として要求された場合、同意の要請は他の事項と明確に区別されるべきである。契約書に個人データの使用に関する同意の問題と関連しない多くの事項が含まれている場合、同意の問題は明確に目立つ方法または別の文書によって同意が行われる必要がある。
- 同様に、電子的手段によって同意が要求された場合、同意要求は別途区別して行われなければならず、単に契約条項内の規定の一部であってはならない。小さなスクリーンまたは情報のための限られたスペースに対応するため、 適切であれば、ユーザー体験または製品設計に関する過度の妨害を避けるために、階層化された情報提供の方法も考えられる。

3.3.情報が与えられた
3.3.2.情報提供の方法(3)

- データ主体の同意に依拠する管理者は、第13条および第14条に定める個別の情報通知も行わなければならない。実際には、情報通知義務および同意に関する情報提供の要件の遵守は、統合されたアプローチによって行われる可能性がある。しかし、同意を得る際に、第13条および第14条のすべての要素について情報提供されていないとしても、有効な同意は存在し得る。
- 具体例：

  企業は同意に基づいてデータ処理を行う。同社は、同意要求を含む階層化されたプライバシー通知を使用している。同社は管理者の基本的な情報と想定されるデータ処理活動をすべて開示している。
  - 管理者の情報または処理の目的が階層化されたプライバシー通知における第一段階の階層から明らかではない場合、管理者がデータ主体が同意を行う前にデータ主体が情報にアクセスしたことを示すことができない限り、データ主体が同意に関して情報提供を受けたことを立証することは困難であると考えられる。

  もっとも、会社は、データ保護責任者にどのように連絡することが可能かについてプライバシー通知に記載していない。第6条における有効な法的根拠を備えることとの関係では、第13条および第14条に基づきデータ保護責任者の連絡先がプライバシー通知の第一階層において連絡されていないとしても、管理者は情報が与えられた有効な同意を得ている。

3.4.明確な意思表示

- 同意は、データ主体の明確な積極的行為によらなければならないと規定する（第4条第11号）。
- 明確な積極的行為は、データ主体が特定の処理行為に対して同意を行う意図的な行為を行っていなければならないことを意味する。
- 書面または口頭による陳述によることが可能（電子的手段を含む）
  - データ主体が同意の対象事項について説明したレターまたは電子メールを作成することが書面による陳述として最も正確な方法である。もっとも、これが現実的ではないことは多い。書面による陳述は様々な形態および規模で行われる可能性がある。
  - 口述の録音。ただし、同意の表示前にデータ主体に提供された情報が適切に記録されていなければならない。事前にチェックされたオプトインボックスの使用は無効である。沈黙、不作為およびサービスを単に進める行為は、積極的な表示とは考えられない。
- 契約締結またはサービスの一般的な契約条件の受諾と同じ行為を通じて得られ同意を取得することはできない。事前にチェックされたボックスまたはオプトアウト型の同意は無効である。

3.4.明確な意思表示
3.4.1.電子的手段を通じた同意

- 物理的な動作も、明確な積極的行為として認められる。
  - 例：明確な情報が提供されており、動作が特定の要求に対する同意を示すことが明らかである限り、以下の動作は同意を示すものといえる。
    - スマートデバイスのスクリーンをスワイプすること
    - スマートカメラの前で手をふること
    - スマートデバイスを時計回りに回転させること
    - スマートデバイスのスクリーンに指で8の字を書くこと
- 同意の宣言を含むサービスの提供条件をスクロールダウン又はスワイプすることは、明確な積極的行為とはいえない。大量の文字を手早くスクロールした場合に警告文を見落とす可能性があり、行為が十分に明確な内容であるといえない。

3.4.明確な意思表示
3.4.1.電子的手段を通じた同意(2)

- オンライン上では、例えば、ブラウザの設定を使用してインターネットユーザーの同意を得ることがよく行われる。そのような設定は、GDPRにおける有効な同意の条件に沿って開発されなければならない。例えば、同意は想定される目的ごとに細分化され、提供される情報は管理者の名前を含むべきである。
- GDPRは、第4条第11号において、処理活動の前に同意を与えなければならないことを明記していないが、これは明確に暗示されている。 第6条第1項の見出しと第6条第1項(a)の「与えられた(has given)」という文言は、この解釈を支持する。処理行為を開始する前に有効な法的根拠が存在しなければならないことは、第6条および第40条から論理的に明らかである。

4.明示的同意の取得

- 通常の同意の有効要件に加え明示的であることが求められる場合
  - 特別カテゴリーの個人データの処理に対する同意(第9条第2項)
  - 十分性決定を受けていない第三国への個人データの移転に対する同意(第49条第1項(a))
  - プロファイリングを含む自動化された意思決定のみに基づき、データ主体に法律的効果又は同様の影響を及ぼす意思決定を行うことに対する同意(第22条第2項(c))
- 明示的な意思表示と認められるためには、通常の同意有効要件である明確で積極的な意思表示に加え、何が求められるか。
  - 書面により、署名された同意
  - webフォームへの記入、電子メール送信
  - スキャンされた署名入り書面のアップロード
  - 電子署名された文書の送信
- 口頭による意思表示も明示的であると認められる可能性はあるが、有効な明示的同意に関するすべての条件が満たされていることを証明することは困難である場合がある。

4.明示的同意の取得

- 同意の二段階の検証は、明示的同意が有効であることを確認する方法にもなり得る。 例えば、データ主体は、医療データを含む記録を処理する管理者の意図を知らせる電子メールを受信する。管理者は、電子メールで、特定の目的のために特定の情報の使用について同意を求めることを説明する。データ主体がこのデータの使用に同意すると、管理者は「同意する」という陳述を含む電子メールの返信を要求する。返信が送信された後、データ主体は、クリックする必要がある確認リンクまたは確認コード付きのSMSメッセージを受け取り、同意を確認する。

5.有効な同意を取得するための追加的条件
5.1. 同意の証明

- 管理者はデータ主体が同意したことを証明することができなければならない(第7条第1項)。
- 同意の証明方法は管理者の自由な裁量に委ねられ、管理者は日常業務にフィットする方法を開発すればよい。同時に、有効な同意が管理者によって得られたことを証明する義務は、それ自体が過剰な量の追加的なデータ処理をもたらすべきではない。これは、管理者が処理との関連性を示すのに十分なデータを持つべきであるが（同意が得られたことを示すため）、必要以上の情報を収集すべきではない。
- 同意の証明義務は、同意に係る個人データ処理が終了するまで続く。処理行為が終了した後、法的義務または法的主張の立証、行使または防御のために厳密に必要な限度を超えて保有されるべきではない。
- 例えば、以下を証明するために、受領した同意の意思表示の記録を保有することが考えられる。
  - どのような方法で同意を取得したか
  - いつ同意を取得したか
  - データ主体にどのような情報が提供されたか
- 例えば、オンライン上で、管理者は、同意が表示された場面に関する情報と、その時点における同意のワークフローに関する文書、その時点においてデータ主体に対して提供された情報の写しを保有することがあり得る。単に各ウェブサイトに関する正しい設定を参照するだけでは不十分である。

5.1. 同意の証明(2)

- 同意が継続する期間に関して、GDPRには特定の期限はない。同意が継続する期間は、文脈、当初の同意の範囲、およびデータ主体の期待に依拠する。処理業務が大幅に変更または発展した場合、当初の同意はもはや有効ではない。この場合、新たな同意を得る必要がある。
- 第29条作業部会は、適切な間隔で同意を更新することをベストプラクティスとして推奨している。すべての情報を再度提供することは、データの主体がデータの使用方法や権利行使の方法について十分な情報を提供できるようにするために有益である。

5.2. 同意の撤回

- 管理者は、以下を確保しなければならない(第7条第3項)
  - 同意を与える場合と同程度に容易な方法で同意が撤回できること
  - 同意はいつでも撤回できること
- マウスクリック、スワイプ、キーストロークなどの操作で同意を取得する場合、それと同程度に容易な方法で同意を撤回することができなければならない。
- 同意を与える方法と同意を撤回する方法が同じ行為でなければならないわけではない。もっとも、例えば、webサイト、アプリ、ログオンアカウント、IoTデバイスのインターフェース、電子メールなどのサービス固有のユーザー・インターフェースを経由して同意を取得した場合、同じ電子的なインタフェースで同意を撤回することができなければならない。
  - 例：4時間利用可能なwebサイトでマーケティング目的の個人データ処理について同意を取得した場合、同意を撤回するためにコールセンターに午前8時から午後5時までの間に電話をしなければならないとすることは、第7条第3項に反する。

5.2. 同意の撤回(2)

- データ主体が不利益を受けることなく同意を撤回することが可能であるべきである。同意の撤回は、無償またはサービスのレベルを落とすことなく行うことが可能である必要がある。
- 同意をいつでも撤回できることは、同意取得の前に説明しなければならず、同意撤回の方法は、第13条の情報通知の一部として説明しなければならない。
- 個人データ処理の法的根拠が複数にわたる場合がある。たとえば、契約履行のために必要であることを法的根拠とする個人データ取得と併せて、マーケティング目的のための個人データ取得について同意を得る場合。そのような場合、後日、同意が撤回されても契約履行のために必要な個人データ処理は依然として適法である。そのような場合に備え、取得する個人データ項目それぞれについて法的根拠を明確に整理しておく必要がある。
- 同意が撤回された後も他の法的根拠(例ば管理者の正当な利益の追求)に基づいて、個人データ処理を継続しようとする場合、管理者はデータ主体に対して、第13条および透明性の原則に基づき、改めて情報提供(プライバシー・ノーティス)を行う必要がある。

5.2. 同意の撤回(3)

- 原則として、同意が撤回された場合、同意に基づいて行われ、同意撤回の前に行われたGDPRに従ったすべてのデータ処理行為は適法であるが、管理者は関係する処理行為を停止しなければならない。データの処理（例えば、追加の保存）を正当化する他の法的根拠がない場合、それらは管理者によって削除または匿名化されるべきである（第17条第1項(b)、第3項）。
- データが実際に処理される目的とデータの収集前に依拠した法的根拠について管理者が評価を行うことは非常に重要である。企業が複数の目的のために個人データを必要とし、処理が複数の法的根拠に基づいていることがある（顧客データが、契約および同意に基づいている場合がある）。同意の撤回は、データ主体との契約の履行に基づく目的のために処理されたデータを管理者が消去しなければならないことを意味しない。したがって、管理者は、データの各要素にどのような目的で適用され、どの法的根拠が信頼されているかについて、当初から明確にすべきである。
- 同意が撤回された後に同意に基づいて処理されたデータを削除する管理者の義務に加えて、個々のデータ主体は管理者がまだ保有するデータ主体に関する他のデータの消去を要求する機会を有する。この場合、データ主体は、第17条第1項(b)および前文65項に規定されているように、データを消去する権利を行使すべきである。第29条作業部会は、データ主体による削除要求がない場合においても、データの継続的な処理行為が適切であるか否かについて評価することを推奨する。
- データ主体が同意を撤回し、管理者が他の法的根拠に基づいて個人データの処理を継続することを希望する場合、撤回された同意から他の法的根拠に黙って移行することはできない。さらに、処理に関する法的根拠の変更は、第13条および第14条の情報通知義務に従ってデータ主体に通知されなければならない。

6. GDPR第6条における同意およびその他の法的根拠の関係性

- 原則として、ある一つの目的のための個人データ処理業務は複数の法的根拠に基づくことができない。
- しかし、個人データ処理が複数の目的のために行われる場合、各目的毎に別の法的根拠によることができる。
- これらの処理目的と法的根拠との関係は処理を開始する前に特定しておかなければならない。処理の途中で法的根拠を変更することはできない。つまり、ある個人データ処理について、同意の有効性に疑義が生じた場合でも、その処理を適法であると正当化するために遡って別の法的根拠を援用することは許されない。

7. GDPRにおいて関係する特定の分野
7.1 子供(第8条)

- 情報社会サービスの子供への直接的な提供に関して同意が適用される場合、子供の個人データの処理は、子供が少なくとも16歳である場合には適法である（第8条第1項）。子供が16歳未満の場合、そのような処理は、子供に対する保護責任者が同意を与えたかまたは承認した場合に限り、適法となる。
- GDPRの有効な同意に関する年齢制限について、加盟国はより低い年齢を規定することが可能であるが、13歳未満にすることはできない。

7.1 子供(第8条)
7.1.1.情報社会サービス

- 第29条作業部会は、この定義の範囲を評価する際に、ECJの判例法を参照する。
- ECJは、情報社会サービスは、オンラインで締結または送信される契約やその他のサービスをカバーすると主張した。サービスに2つの経済的に独立した要素があり、1つはオンラインの構成要素であり、契約の締結やマーケティング活動を含む製品やサービスに関する情報の提供や受諾など、この構成要素は情報社会サービスとして定義されているが、物品の物理的な配達または配布である他の構成要素は、情報社会サービスの概念によってカバーされていない。
- サービスのオンライン配信は、第8条の情報社会サービスの範囲に該当すると考えられる。

7.1 子供(第8条)
7.1.2.子供への直接的な提供

- 情報社会サービスの提供者が潜在的なユーザーに対して、18歳以上の人にのみサービスを提供していることを明らかにしており、このことが他の証拠によって損なわれない場合（サイトまたはマーケティング計画の内容など）、このサービスは「子供に直接提供される」とはみなされず、第8条は適用されない。

7.1 子供(第8条)
7.1.3.年齢

- 加盟国は、13歳未満とならないことを条件として、同意に関するより低い年齢を規定することも可能である。管理者は、サービスの対象となる一般人を考慮して、異なる国の法律を認識しなければならない。特に、越境的なサービスを提供する管理者は、その主要な拠点を有する加盟国の法律のみを遵守することに常に依拠することはできず、情報社会サービスを提供する各加盟国の国内法を遵守する必要がある。これは、加盟国がその国の法律またはデータ主体の居住地における基準点として管理者の主たる拠点を使用するかどうかによって決まる。まず第一に、加盟国は選択の際に子どもの最善の利益を考慮する。作業部会は、加盟国に対し、この問題に関して調和の取れた解決策を模索することを奨励する。
- 同意に基づいて子供に情報社会サービスを提供する場合、管理者は、ユーザーが同意制限の年齢を超えていることを確認するための合理的な努力を行うことが期待され、これらの対策は処理活動の性質とリスクに比例する必要がある。
- ユーザーが年齢制限を超えていると述べた場合、管理者は陳述が正しいことを確認するための適切なチェックを実行することができる。GDPRでは年齢を確認する必要性は明白ではないが、子供が有効な同意を行うのに十分な年齢ではない間に同意を行う場合、データ処理は違法となるため、黙示的に要求されている。

7.1 子供(第8条)
7.1.3.年齢(2)

- ユーザーが制限年齢未満であると述べた場合、管理者はそれ以上の確認を行わずに陳述を受け入れることが可能であるが、保護責任者の承認を取得し、同意書を提出した者が保護責任者であることを確認する必要がある。
- 年齢確認によって過剰なデータ処理が行われるべきではない。データ主体の年齢を検証するために選択された仕組みは、提案された処理のリスクの評価を伴う。リスクが低い状況では、サービスの新しい加入者に誕生年の開示を求めるか、または未成年者である（未成年者ではない）旨を述べるフォームを記入することが適切であると考えられる。疑義が生じた場合、管理者は年齢認証メカニズムを見直し、代替チェックが必要かどうかを検討する必要がある。

7.1 子供(第8条)
7.1.4.子供の同意および保護者の責任

- 保護責任者の承認に関して、GDPRは、親の同意を集めたり、特定の者が当該措置を講じる資格があることを立証するための実務的な方法を規定していない。第29条作業部会は、第8条第2項および第5条第1項(c)に従って、比例的なアプローチを採択することを推奨する。比例的なアプローチは、親または保護者の連絡先の詳細等、限られた量の情報を取得することに焦点を当てることが考えられる。
- ユーザーが同意を行うのに十分な年齢であることを確認すること、および子供のために同意を提供する者が保護責任者であることを確認することに関して、合理的であるかどうかは、処理に内在するリスクおよび利用可能な技術による。リスクの低いケースでは、電子メールによる親の責任の確認で十分である。反対に、リスクが高い場合には、管理者が第7条第1項に従って情報を検証して保有できるように、より多くの証明を求めることが適切であると考えられる。信頼できる第三者検証サービスは、管理者が処理する必要のある個人データの量を最小化する解決策を提示するものといえる。

7.1 子供(第8条)
7.1.4.子供の同意および保護者の責任(2)

- 第8条第2項は、特に、「管理者は、利用可能な技術を考慮して、子どもに対する保護責任者によって同意が与えられたまたは許可されたという状況を証明するために合理的な努力を行わなければならない」と付け加えている。
- 特定の場合にどのような対策が適切かの判断は管理者に委ねられる。原則として、管理者は、それ自体が過度の個人データの収集を伴う認証方法を避けるべきである。
- 第29条作業部会は、認証が困難である場合があることを認識している（例えば、自らの同意を得ている子どもたちがまだ「身分証明書」を設定していない場合や、親の責任が容易に確認できない場合など）。 このことはどのような努力が合理的であるかを判断する際に考慮されるが、管理者は処理と利用可能な技術を常に見直しておくことが期待される。

7.1 子供(第8条)
7.1.4.子供の同意および保護者の責任(3)

- 個人データの処理に同意し、処理を完全に支配するデータ主体の自律性に関して、保護責任者による同意、保護責任者によって承認された同意は、子供が年齢制限に係る年齢に到達したら、期限切れになる。その日以降、管理者はデータ主体から有効な同意を得る必要がある。実際には、子供の同意が16歳になると期限切れとなり、同意につき本人による再確認が必要であることをリマインドするために、ユーザーからの同意を得ている管理者が定期的にユーザーにメッセージを送信する必要があると考えられる。
- 前文38項によれば、親または保護者の同意は、子供に直接提供される予防またはカウンセリングサービスの文脈では必要ではない。例えば、オンラインチャットサービスによって子供にオンラインで提供される児童保護サービスの提供は、事前の親の許可を必要としない。
- 最後に、GDPRは、未成年者に対する親の認可要件に関する規則は、「子どもとの契約の有効性、成立または効果に関する規則等の加盟国の一般契約法」に介入するものではないと述べる。

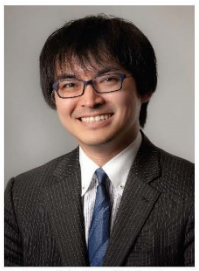
8.指令95/46/ECにおいて取得した同意

- 旧データ保護指令下で取得した同意は、管理者はGDPRの適用開始前に、取得済みの同意がGDPRの基準を満たすかどうかを確認すべきである。
- GDPRが新たに加えた同意の有効要件を満たさない場合の例
  - 同意取得を証明できない場合
  - 陳述または明確な積極的行為によりも、データ主体による黙示的な行為に基づいていた同意（例：チェックの入ったオプトインBoxを無視すること）
- 第13条に基づく情報通知との関係
  - 同意に先立つ情報提供として、第13条の情報提供がすべて必要なわけではないので、これらの情報提供が行われていないことを理由としてすでに取得した同意が無効となるわけではない。
- 旧指令に基づく同意がGDPRの基準を満たさない場合、管理者は他の法的根拠を援用することができる。ただしこれはGDPRへの移行に伴う1回限りの状況であり、GDPRのもとでは、ある目的のための個人データ処理について、法的根拠を変更することはできない。

VI. 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(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

GIBSON DUNN

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2004)5721

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

.....(name)

.....(address and country of establishment)

hereinafter "data exporter"

and

.....(name)

.....(address and country of establishment)

hereinafter "data importer"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a) "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b) "the data exporter" shall mean the controller who transfers the personal data;

c) "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d) "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I. Obligations of the data exporter

The data exporter warrants and undertakes that:

a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e) It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h) It will process the personal data, at its option, in accordance with:

i. the data protection laws of the country in which the data exporter is established, or

ii. the relevant provisions [1] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[2], or

iii. the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: .....

Initials of data importer: ..... ;

i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

i. the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

ii. the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii. data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv. with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III. Liability and third party rights

a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or

[1] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[2] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

a) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b) In the event that:

i. the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii. compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii. the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Dated: .....

FOR DATA IMPORTER	FOR DATA EXPORTER
.....	.....
.....	.....

ANNEX A

DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2. Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4. Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6. Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7. Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8. Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

   a) i. such decisions are made by the data importer in entering into or performing a contract with the data subject, and
      ii. the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties.

   or

   b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

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

Data importer	**Data exporter**
……	……
……	……
……	……

ILLUSTRATIVE COMMERCIAL CLAUSES (OPTIONAL)

Indemnification between the data exporter and data importer:

"The parties will indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of these clauses. Indemnification hereunder is contingent upon (a) the party(ies) to be indemnified (the "indemnified party(ies)") promptly notifying the other party(ies) (the "indemnifying party(ies)") of a claim, (b) the indemnifying party(ies) having sole control of the defence and settlement of any such claim, and (c) the indemnified party(ies) providing reasonable cooperation and assistance to the indemnifying party(ies) in defence of such claim.".

Dispute resolution between the data exporter and data importer (the parties may of course substitute any other alternative dispute resolution or jurisdictional clause):

"In the event of a dispute between the data importer and the data exporter concerning any alleged breach of any provision of these clauses, such dispute shall be finally settled under the rules of arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said rules. The place of arbitration shall be [ ]. The number of arbitrators shall be [ ]."

Allocation of costs:

"Each party shall perform its obligations under these clauses at its own cost."

Extra termination clause:

"In the event of termination of these clauses, the data importer must return all personal data and all copies of the personal data subject to these clauses to the data exporter forthwith or, at the data exporter's choice, will destroy all copies of the same and certify to the data exporter that it has done so, unless the data importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The data importer agrees that, if so requested by the data exporter, it will allow the data exporter, or an inspection agent selected by the data exporter and not reasonably objected to by the data importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours."

EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE

Directorate C: Fundamental rights and Union citizenship
Unit C.3: Data protection

Commission Decision C(2010)593
Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:.....

Address: .....

Tel.:.....; fax: .....; e-mail:.....

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: .....

Address: .....

Tel.:..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

.....
(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) *'the data exporter'* means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

---

1 Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely……..

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses [3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely .....
.....
.....

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……..

(stamp of organisation)

On behalf of the data importer:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature……..

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):
……
……

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
……
……

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):
……
……

Categories of data
The personal data transferred concern the following categories of data (please specify):
……
……

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):
……
……

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):
……
……

DATA EXPORTER

Name:……

Authorised Signature ……

DATA IMPORTER

Name:……

Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

.....
.....
.....
.....
.....

ILLUSTRATIVE INDEMNIFICATION CLAUSE (OPTIONAL)

Liability

The parties agree that if one party is held liable for a violation of the clauses committed by the other party, the latter will, to the extent to which it is liable, indemnify the first party for any cost, charge, damages, expenses or loss it has incurred.

Indemnification is contingent upon:

(a) the data exporter promptly notifying the data importer of a claim; and

(b) the data importer being given the possibility to cooperate with the data exporter in the defence and settlement of the claim[4].

[4] Paragraph on liabilities is optional.

International Association of Privacy Professionals

www.iapp.org

Takeshige Sugimoto, Gibson, Dunn & Crutcher, Brussels
March 2018

iapp

The growth of an industry

- Businesses and society are experiencing benefits from data generation and use
- Easy access to information results in new insights
- Companies must balance potential privacy risks

iapp

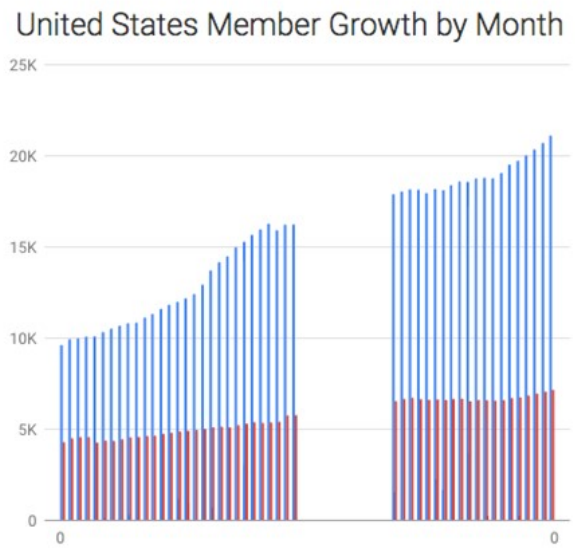
How the IAPP fits in

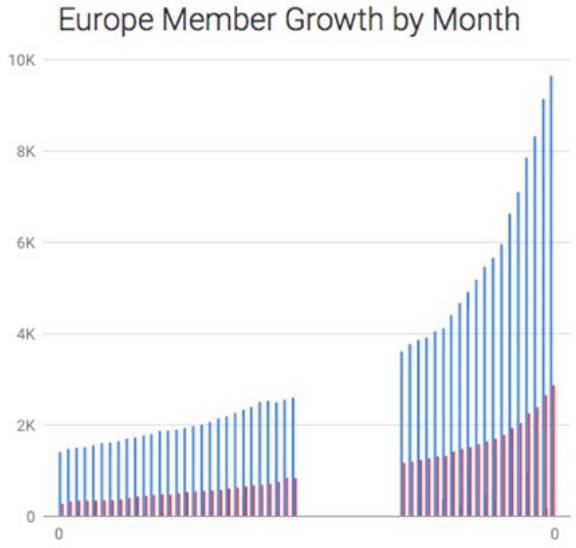
- Founded in 2000
- Largest privacy association in the world
- More than 38,000 members in 103 countries
- Massive warehouse of resources for practitioners



iapp

Member growth – 2013-2018





Total: 14,500 → 38,000

iapp

Member growth – 2013-2018

Total Asia: 375 → 1,700

The growth of the profession

- Privacy professionals gap in organizations
- Certified professionals make $10k more than average
- Privacy staffing will increase in half of all organizations in 2018

Setting the industry standard

IAPP certification is the global standard for privacy and data protection professionals.

- CIPP (privacy professionals) training, launched in 2004, demonstrates an understanding of the laws, regulations, frameworks and standards around privacy
- CIPM (privacy managers), launched in 2013, demonstrates how to embed privacy into an organization through management processes
- CIPT (privacy technologist) Launched in 2014, the CIPT training demonstrates how to manage and build privacy requirements and controls in technology

Certified Information Privacy Professional CIPP iapp

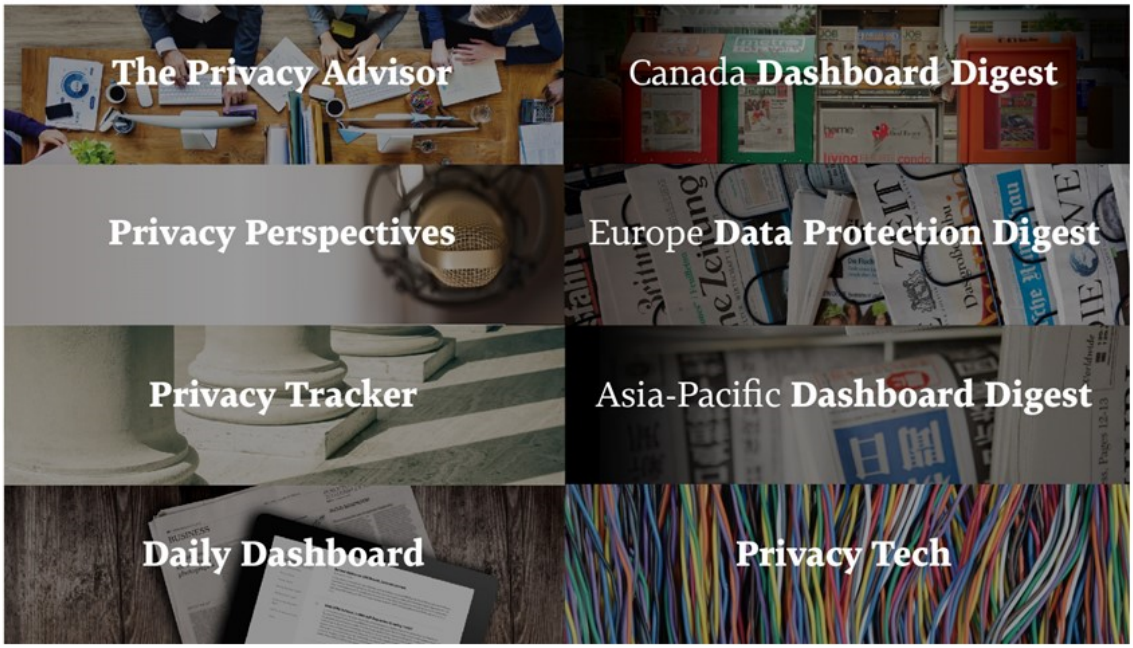
Certified Information Privacy Manager CIPM iapp

Certified Information Privacy Technologist CIPT iapp

iapp

News

IAPP publications keep members up to date on the latest privacy and data protection news worldwide.



Online resources

- ✓ IAPP Privacy List
- ✓ Web Conferences
- ✓ @PrivacyPros, @DailyDashboard
- ✓ 20k LinkedIn members

Resource Center

- Samples, Tools and Templates
- Privacy Research
- Career Center
- IAPP Articles and Presentations
- Privacy Discussions
- Privacy Glossary
- FTC Casebook
- Westin Center
- Data Protection Authorities

iapp

Conferences

More than a professional association, the IAPP provides a home for privacy professionals around the world to share experiences—working to promote career readiness and improve job effectiveness

IAPP Global Privacy Summit
The world's top privacy conference! Whether you work in the public or private sector, anywhere in the world, Summit is the place to be.

IAPP Canada Privacy Symposium
The Symposium gathers regulators and thought-leaders for intensive education and discussion on Canadian privacy challenges.

Privacy. Security. Risk. (P.S.R.)
P.S.R. brings together the best of the best in privacy and cloud security, with innovative cross-education and stellar networking.

IAPP Europe Data Protection Intensive
Held annually in London, the Intensive digs deep into operational privacy and practical strategies you can put straight to use.

IAPP Asia Privacy Forum
The Forum delivers world-class discussion and education on the top privacy issues in Asia Pacific and around the globe.

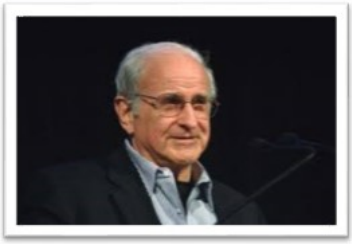
IAPP Europe Data Protection Congress
The Congress is the source for European policy debate, thought leadership and strategic thinking with data protection pros.

iapp

Research & education

The IAPP Westin Research Center was created in 2013 to encourage, enable and produce practical, applicable research and scholarship in privacy.

IAPP
WESTIN RESEARCH
CENTER



Notable Research:

- The **FTC Privacy Casebook**
- The **Top 10 Operational Impacts of the GDPR**
- The **IAPP-EY Privacy Governance Report**

iapp

Understanding and Assessing Professional Credentials and Training

There is a wide variety of data protection credentials in the marketplace, with differing requirements and features. These credentials may also be subject to varying levels of third-party oversight and validation (accreditation). Understanding these differences will help organizations and individuals choose the right credential for the task at hand.

This chart, based on a survey of the global marketplace*, provides a quick reference to the different types of credentials and their component parts.

▼ REQUIREMENT	TRAINING CERTIFICATE OF ATTENDANCE	CERTIFICATE PROGRAM	PROFESSIONAL CERTIFICATION	DEGREE	LICENSE	Factors to consider when assessing an organization offering credentials:
TRAINING	YES	YES	SOMETIMES	YES	SOMETIMES	• Does the training simply teach you how to take the test?
ASSESSMENT: An exam with a set score for passing or failing	NO	YES	YES	YES	SOMETIMES	• Does the exam assess experience and competence, or merely retention of knowledge?
ACCREDITATION: An assessment by a third party of the quality and integrity of the credential (i.e., ISO 17024)	SOMETIMES	SOMETIMES	SOMETIMES	YES	YES	• Does the credential have independent accreditation from a third party?
CONTINUING EDUCATION: An ongoing education requirement, after the initial training and assessment	NO	NO	YES	NO	YES	• Does the credential require ongoing education?
JOB TASK ANALYSIS: A study of the skills and knowledge used by actual practitioners of the credentialed field	NO	NO	YES	NO	YES	• Is the credential based on real-world job requirements or simply a test of knowledge?

*Sources:
International Certification and Reciprocity Consortium
Institute for Credentialing Excellence
U.S. Federal Trade Commission
U.S. Department of Labor
EU Commission's Employment, Social Affairs & Inclusion

WHAT OTHER CONSIDERATIONS ARE IMPORTANT?

- Is the credentialing body for profit or not-for-profit?
- Is the credential local, regional, or global in scope? How broadly is it recognized and understood?
- Does the credentialing body offer continuing education for the credential?
- Does the credentialing body offer connection to a broader professional community?

WHY IS ACCREDITATION IMPORTANT?

An independent accreditation of a credential provides a high degree of assurance as to the substance and integrity of a certification program.

WHAT IS A "JOB TASK ANALYSIS" (JTA)?

A formal process to determine what professionals in a particular field do, under what conditions, and with what levels of knowledge and skill. A "JTA" is a requirement for accreditation under ISO 17024.