

欧州一般データ保護 規則（GDPR）施行に 向けた最新状況

弁護士・ひかり総合法律事務所

国立研究開発法人理化学研究所

革新知能統合研究センター客員主管研究員

板倉陽一郎

自己紹介

- 2002年慶應義塾大学総合政策学部卒，2004年京都大学大学院情報学研究科社会情報学専攻修士課程修了，2007年慶應義塾大学法務研究科（法科大学院）修了。2008年弁護士（ひかり総合法律事務所）。2016年4月よりパートナー弁護士。
- 2010年4月より2012年12月まで消費者庁に出向（消費者制度課個人情報保護推進室（現・個人情報保護委員会事務局）政策企画専門官）。2017年4月より国立研究開発法人理化学研究所革新知能統合研究センター社会における人工知能研究グループ客員主管研究員。
- 総務省・AIネットワーク社会推進会議環境整備分科会及び影響評価分科会構成員，IoT推進コンソーシアム・データ流通促進WG及びカメラ画像利活用SWG委員等。

参考文献

- 条文（訳文）
 - 「個人データの取扱いに係る自然人の保護及び当該データの自由な移転に関する欧州議会及び欧州理事会規則（一般データ保護規則）（仮日本語訳）」（JIPDEC, 2016年8月）
 - 「EUデータ保護一般規則前文私訳の公開」（夏井高人・KDDI総研, 2016年11月1日）
- 解説
 - 夏井高人「個人データの処理と関連する自然人の保護及び個人データの自由な移転並びに指令95/46/ECの廃止に関する欧州議会及び理事会の2016年4月27日の規則（EU）2016/679（一般データ保護規則）[参考訳]」法と情報雑誌1巻3号1-186頁（2016年9月）[夏井]
 - 堀部政男「EU一般データ保護規則と日本」ビジネス法務17巻8号12-13頁（2017年8月）[堀部]
 - 宮下紘「規則の特徴と対応」同14-18頁[宮下]
 - 杉本武重「EU域内における義務強化—データ管理者・処理者の新たな責任」同19-26頁[杉本]
 - 加藤隆之「個人データに関する『新たな権利』」同27-30頁[加藤]
 - 石井夏生利「域外適用の対象と違反時の制裁」同31-35頁[石井]
 - 板倉陽一郎「越境データ移転—事業者が選択可能な方法と実務対応」同36-40頁[板倉]
 - 佐藤真紀「適用対象の拡大とCookie規制の緩和 eプライバシー規則案」同41-45頁[佐藤]
 - 市川芳治「個人データ保護規則と競争政策—日本でも議論進む・今後の展開は」同46-49頁[市川]
 - 柳池剛「プライバシーコンプライアンスの『世界標準』」同50-54頁[柳池]

アジェンダ

- 1 欧州一般データ保護規則（GDPR）の概要
 - 1.1 GDPRとは何か
 - 1.2 GDPRはいつから適用されるのか
 - 1.3 GDPRは誰に適用されるのか
 - 1.4 GDPRは誰が執行するのか
- 2 GDPR上の権利・義務
 - 2.1 GDPRにおける個人データ取扱いの原則
 - 2.2 GDPRにおけるデータ主体の権利
 - 2.3 GDPRにおけるデータ管理者・データ処理者の義務
- 3 EUによる日本の十分性認定
 - 3.1 GDPRにおける越境移転制限
 - 3.2 GDPRにおける十分性認定
 - 3.3 例外事由

- 4 「個人情報保護に関する法律についてのガイドライン（EU域内から十分性認定により移転を受けた個人データの取扱い編）」（案）
 - 4.1 経緯
 - 4.2 ガイドラインの位置付け
 - 4.3 ガイドラインの内容
 - 4.4 今後の展望
- 5 日本によるEUの同等性認定
 - 5.1 個人情報保護法24条
 - 5.2 「個人情報の保護に関する法律施行規則の一部を改正する規則」
 - 5.3 パブリックコメントにおける意見等
- 6 関連する話題
 - 6.1 BREXITのGDPRへの影響
 - 6.2 e-プライバシー規則
- 7 まとめ

1 欧州一般データ保護規則 (GDPR) の概要

1.1 GDPRとは何か

- 前提知識：EU法の種類（国立国会図書館リサーチ・ナビ「EU法について」より）
- 一次法（Primary Legislation）
 - EUの基本条約。現行の基本条約は、2009年12月に発効したリスボン条約により改正されたEU条約及びEU機能条約。基本条約と「同一の法的価値」を持つとされるEU基本権憲章、EU司法裁判所が依拠する法の一般原則などを含むこともあり。
- 二次法（Secondary Legislation）
 - 規則（Regulation），指令（Directive），決定（Decision），勧告（Recommendation），意見（Opinion）
- 判例（Case-Law）
 - EU司法裁判所（司法裁判所・総合裁判所・専門裁判所）の判例。但し先例拘束性はないとされる

前提知識：二次法（Secondary Legislation）の種類

- 規則（Regulation）

- 加盟国の国内法に優先して、加盟国の政府や企業、個人に直接適用される。加盟国の国内立法は不要。加盟国の政府等に対して直接的な法的拘束力を及ぼす。

- 指令（Directive）

- 加盟国の政府に対して直接的な法的拘束力を及ぼす。指令には政策目標と実施期限が定められ、指令が採択されると、各加盟国は、期限内に政策目標を達成するために国内立法等の措置を取ることが求められる。ただし、どのような措置を取るかは各加盟国に委ねられる。なお、企業や個人には直接適用されない。

- 決定（Decision）

- 特定の加盟国の政府や企業、個人に対して直接適用され、対象となる加盟国の政府等に対して直接的な法的拘束力を及ぼす。

- 勧告（Recommendation）

- 加盟国の政府や企業、個人などに一定の行為や措置を取ることを期待する旨、欧州委員会が表明するもの。原則として法的拘束力なし。

- 意見（Opinion）

- 特定のテーマについて欧州委員会の意思を表明するもの。勧告と同様、原則として法的拘束力なし。

データ保護改革パッケージ (data protection reform package)

規則

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
欧州一般データ保護規則 (GDPR)

指令

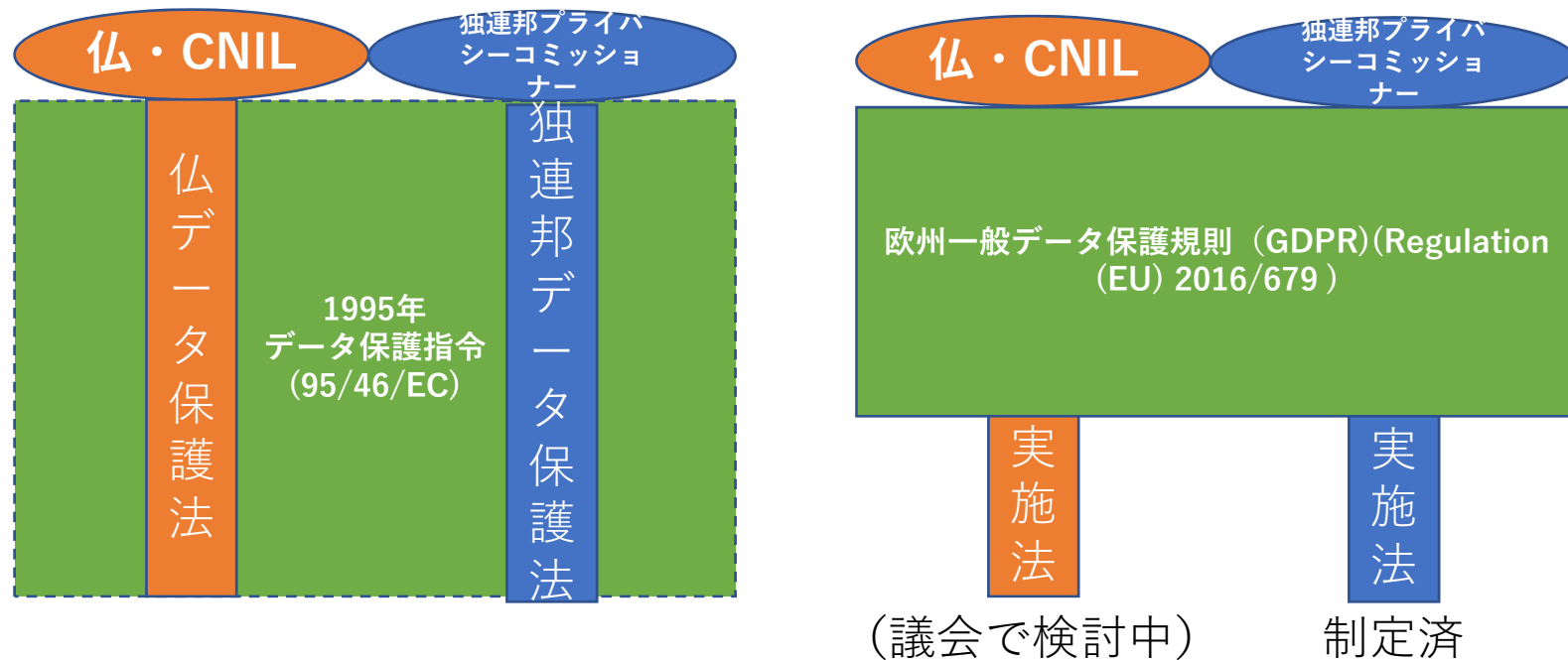
DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
1995年データ保護指令

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA
刑事データ保護指令

決定

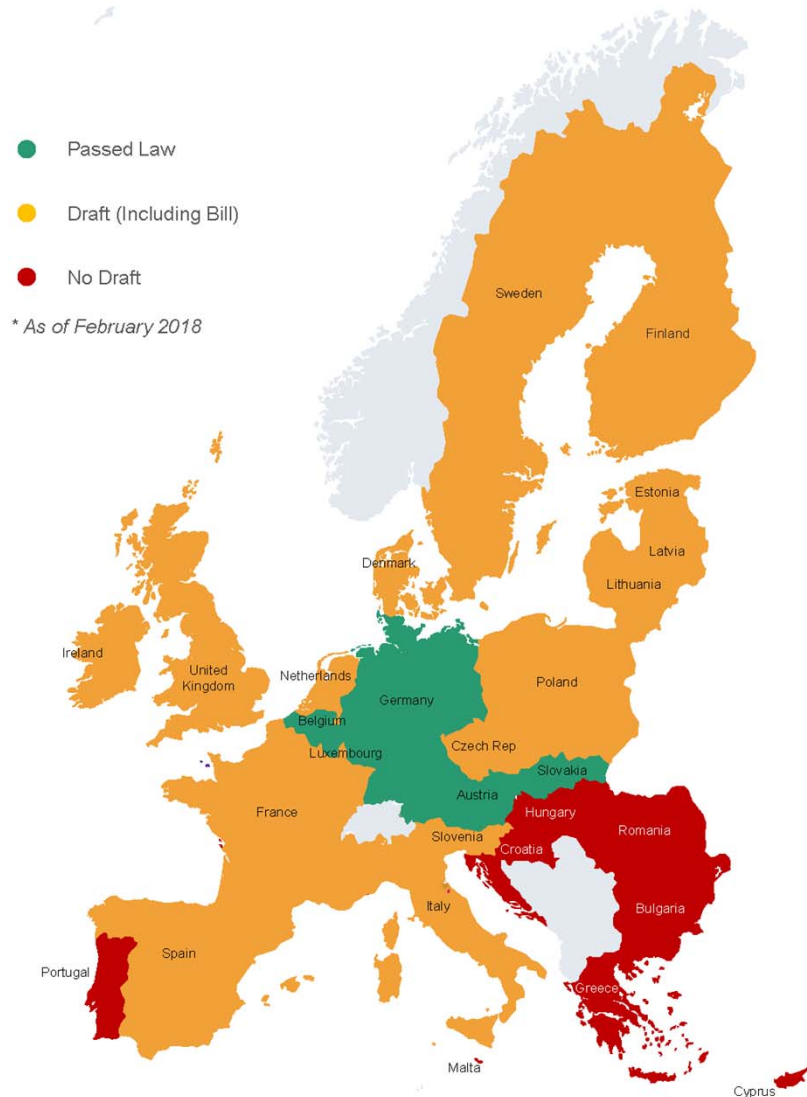
COUNCIL FRAMEWORK DECISION 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters
刑事データ保護枠組み決定

データ保護指令から一般データ保護規則へ



独・仏の例

各国実施法の成立状況



レイサムワトキンス法律事務所作成

- 成立したのは極僅か
 - ドイツ, オーストリア, スロバキア, ベルギー (組織法)
- 実施法 (案) が英語で検討できる国
 - ドイツ, 英国, アイルランド

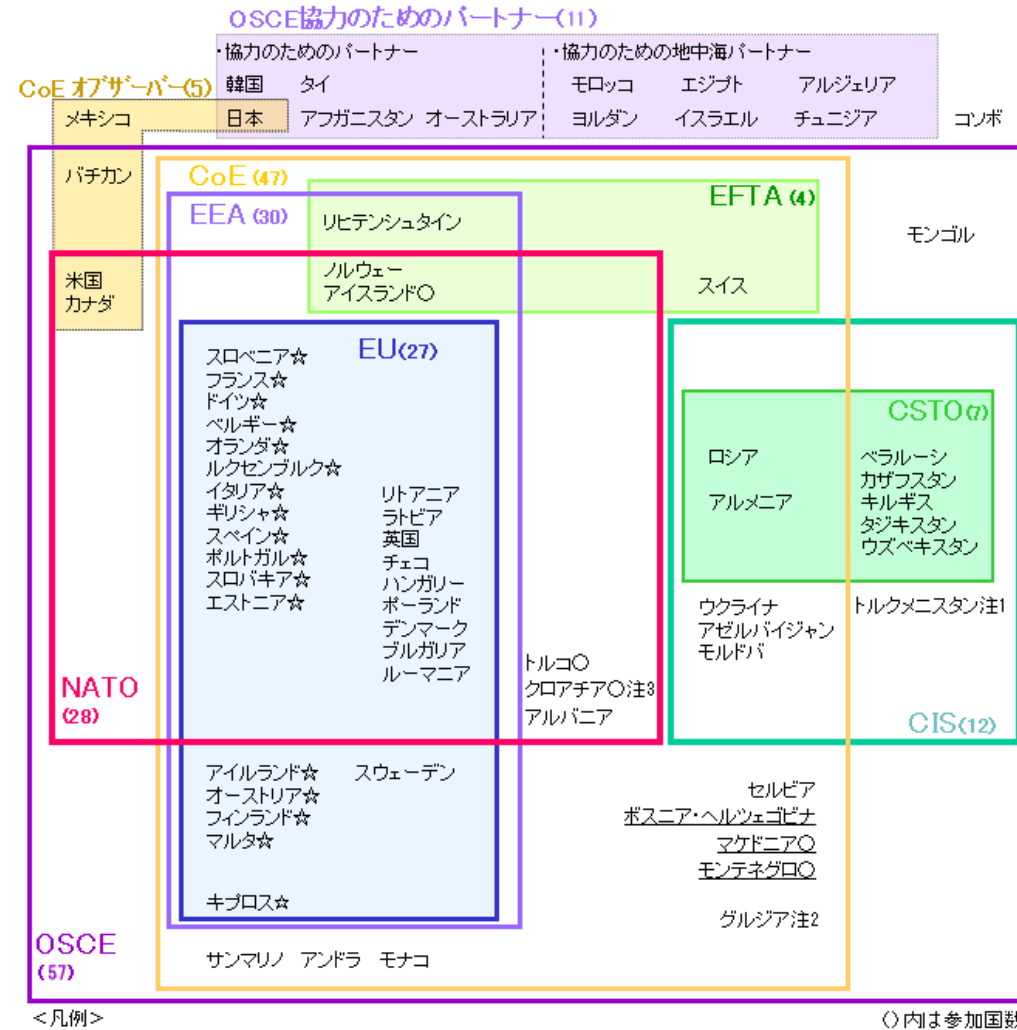
例：板倉・寺田「欧州一般データ保護規則
(GDPR)における各国実施法の学術研究除外に
ついての動向」 (EIP80予告)

- GDPR89条2項は、「科学的又は歴史的・研究目的又は統計目的」についてデータ主体の権利の除外を定めることを規定
 - 全てのデータ主体の権利を例外とすることを許しているものではなく、「第15条、第16条、第18条及び第21条で定める権利」を挙げているに過ぎない。具体的には、アクセス権（開示請求権）（15条）、訂正請求権（16条）、処理の制限を得る権利（18条）、異議申立権（21条）のみ
- ドイツ（安全管理措置を義務付け）
- イギリス（承認プロセス）
- アイルランド（データ最小化）

1.2 GDPRはいつから適用されるのか

- 2016年4月8日理事会採択
- 2016年4月14日欧州議会採択
- 2016年5月24日施行
- **2018年5月25日から適用**
- 参考：刑事データ保護指令
 - 2016年4月8日理事会採択
 - 2016年4月14日欧州議会採択
 - 2016年5月5日施行
 - 2018年5月6日までに国内法化義務

1.3 GDPRは誰に適用されるのか



<凡例>

○: EU加盟候補国(5)

☆: ユーロ参加国(17)

—: NATO加盟のための行動計画(MAP)参加国 (2)

(注1) トルクメニスタンは2005年よりCIS準加盟国。

(注2) グルジアは、2008年8月18日にCISからの脱退を表明。09年8月18日に正式に脱退。

(注3) クロアチアは、2013年7月1日からEUへ加盟の予定。

外務省ウェブサイト

http://www.mofa.go.jp/mofaj/area/osce/s_kikou.html より

第2条 実体的範囲

Article 2 Material scope

- 1. 本規則は、全部又は一部が自動的な手段による個人データの取扱いに適用される。ファイリングシステムの一部である、又はファイリングシステムの一部にすることが意図された個人データの自動的な手段以外の取扱いにも適用される。
- 1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.
- 2. 本規則は、次に掲げる個人データの取扱いには適用されない。
- 2. This Regulation does not apply to the processing of personal data:
 - (a) EU 法の適用を受けない活動における個人データの取扱い。
 - (a) in the course of an activity which falls outside the scope of Union law;
 - (b) (略)
 - (c) 全面的に個人的な又は家庭内の活動における自然人による個人データの取扱い。
 - (c) by a natural person in the course of a purely personal or household activity;
 - (d) (略)
- 3.-4. (略)

ファイリングシステムによる 限定

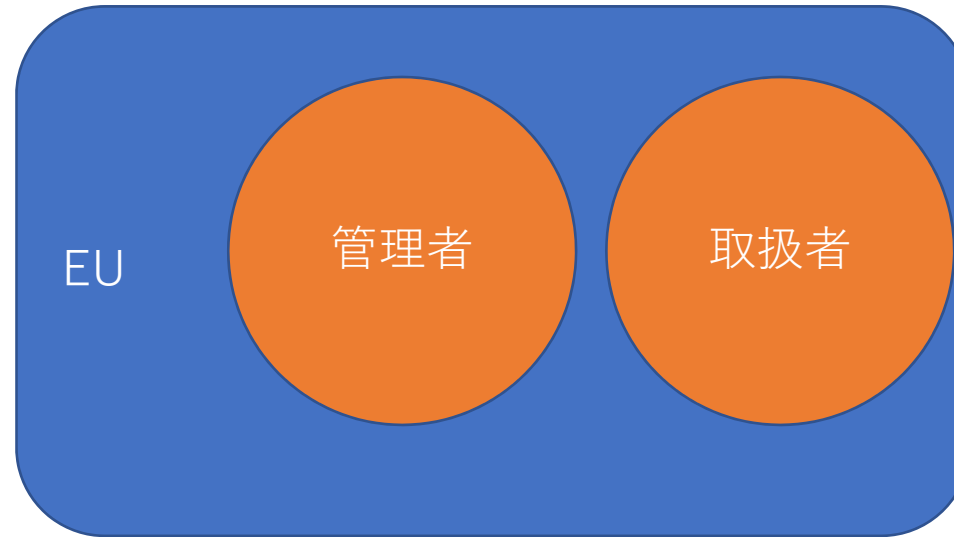
- 「ファイリングシステム」：電子的なもの、非電子的なものを含め、一般に何らかの方法によって検索することが可能なデータベースシステムのことを意味する（[夏井]）
 - ①自動処理される個人データ
 - ②データベースに収録される個人データ
- のみが、GDPRの対象となる。
- 散在情報である名刺であっても、名刺アプリで読み取ってデータベース化することが意図される（are intended to）のであれば入る（同）
 - 但し、2条2項(c)による制限

第3条 地理的範囲

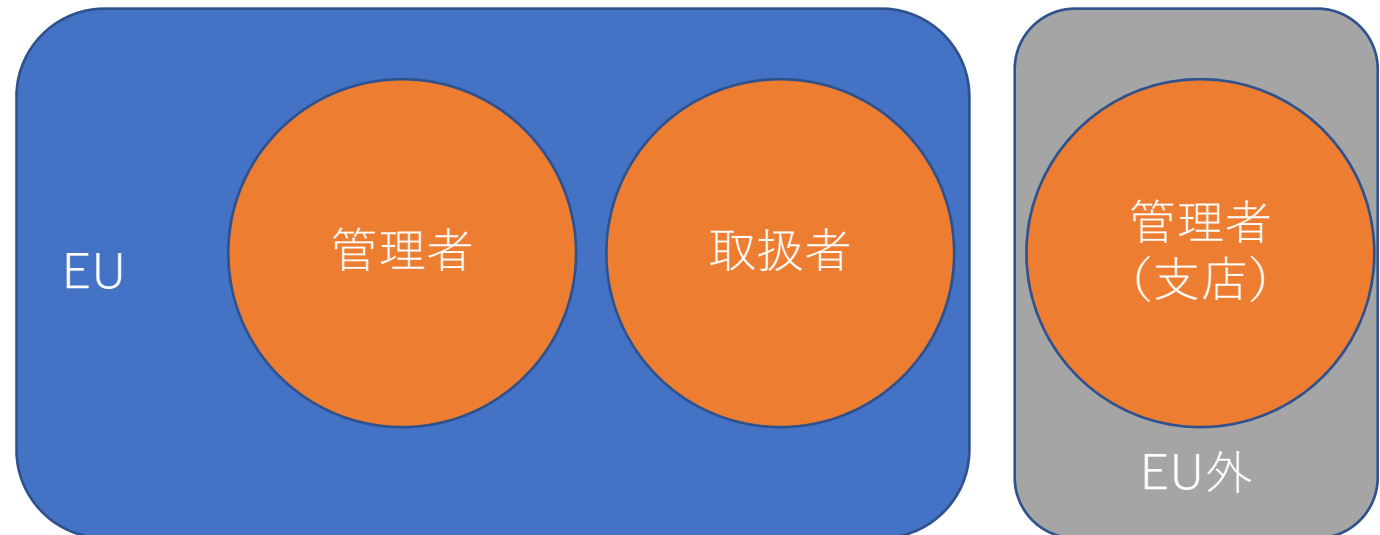
Article 3 Territorial scope

- 1. 本規則は、EU 域内の管理者又は取扱者の事業所の活動に関連してなされる個人データの取扱いに適用される。この場合、その取扱いがEU 域内又は域外でなされるか否かについては問わない。
- 1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

前段



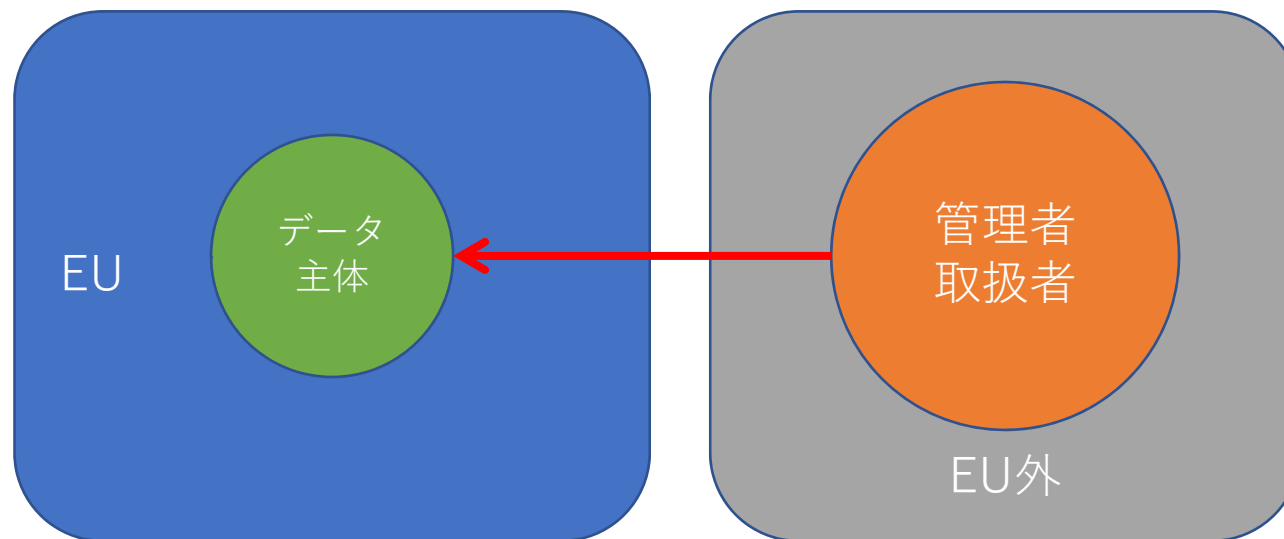
後段



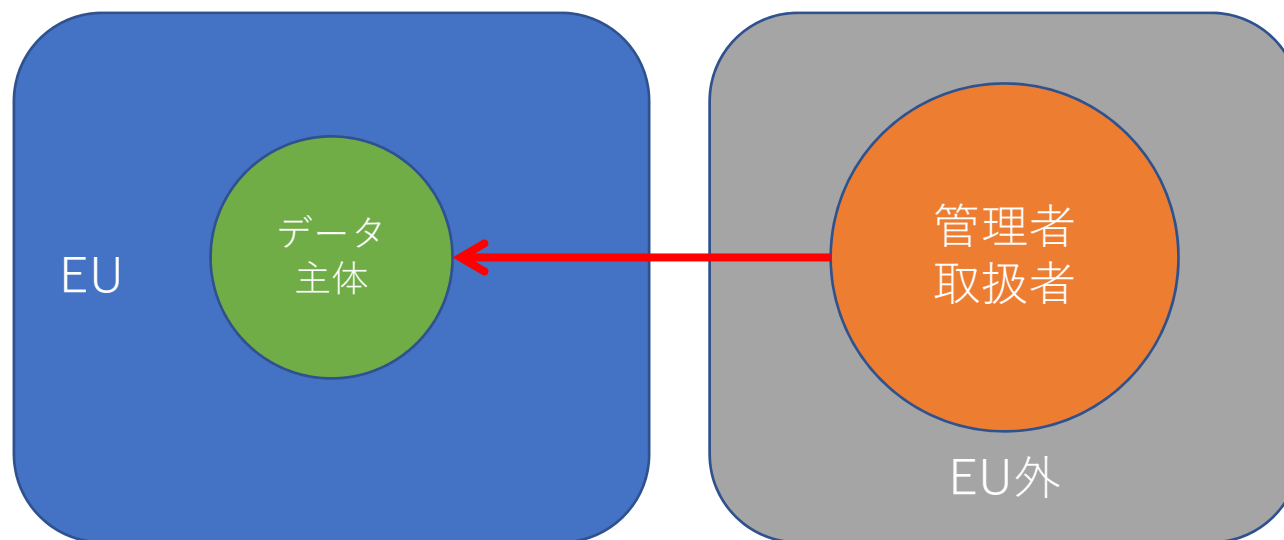
域外適用

- 2. 本規則は、EU 域内に拠点のない管理者又は取扱者による EU 在住のデータ主体の個人データの取扱いに適用される。ただし、取扱い活動が次に掲げる項目に関連しているものに限られる。
- 2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
 - (a) EU 在住のデータ主体に対する商品又はサービスの提供に関する取扱い。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。
 - (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
 - (b) EU 域内で行われるデータ主体の行動の監視に関する取扱い。
 - (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.
- 3. (略)

(a) EU 在住
のデータ主
体に対する
商品又は
サービスの
提供に関す
る取扱い



(b) EU 域内
で行われる
データ主体
の行動の監
視に関する
取扱い



(a) EU 在住のデータ主体に対する商品又はサービスの提供に関する取扱い

- 前文 (23)
- …管理者または処理者が欧州連合内のデータ主体に対して物品または役務を提供しているかどうかを判断するために、その管理者または処理者が欧州連合内の 1 または複数の構成国内のデータ主体に対して役務を提供しようとする意思が明確かどうかを確認しなければならない。管理者の欧州連合内の Web サイト、処理者の欧州連合内の Web サイトまたはその中間的な媒介者の欧州連合内の Web サイト、電子メールアドレスまたはその他の連絡用の詳細情報へのアクセスが容易ではないということ、あるいは、当該管理者が設けられている第三国において一般的に用いられている言語が使用されているということだけでは、そのような意思を確認するためには不十分であるが、1 または複数の構成国において、一般的に用いられており、その外国語を用いて物品及び役務の注文をすることができる言語及び通貨が利用されていること、あるいは、欧州連合内に居住する消費者または利用者に関する言及があることといったような要素は、その管理者が欧州連合内のデータ主体に対して物品または役務を提供しようとする意思があることを明確なものとすることができる。
- 「データ主体に対して役務を提供しようとする意思」
 - ×ウェブサイト、メールアドレス等に単にアクセスできる
 - ×一般的に用いられている言語が使用されている
 - ○一般的に用いられている言語及び通貨の利用
 - ○欧州連合内に居住する消費者又は利用者に関する言及
- 「EU 関係者に確認したところによると、英語圏である英国の場合は（離脱の問題はあるものの）、英語に加えてポンドでの取引を行えば適用されうる」（[石井]）。

(b) EU 域内で行われるデータ主体の行動の監視に関する取扱い

- 前文(24)と異なり、意思的要素が加味されていない。そのため、偶発的に欧州連合内のデータ主体が加わってくるような場合にも排除することが困難である。

 - 技術的な手段により排除することが適切か

第 4 条 定義

Article 4 Definitions

管理者, 取扱者

- (7) 「管理者」とは、単独で又は他と共同して、個人データの取扱いの目的及び手段を決定する自然人、法人、公的機関、行政機関又はその他の団体をいう。当該取扱いの目的及び手段が EU 法又は加盟国の国内法によって決定される場合には、管理者又は管理者の指定に関する特定の基準は、EU 法又は加盟国の国内法をもって定めることができる。
- (7) 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (8) 「取扱者」とは、管理者のために個人データの取扱いを行う 自然人、法人、公的機関、行政機関又はその他の団体をいう。
- (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- Processorの訳語は「処理者」とされていることもある。
- 日本個人情報保護法の「個人情報取扱事業者」は委託先を含むが、委託元（管理者）・委託先と概ね対応すると考えて良い。

個人データ，取扱い

- (1) 「個人データ」とは、識別された又は識別され得る自然人（以下「データ主体」という。）に関するあらゆる情報を意味する。識別され得る自然人は、特に、氏名、識別番号、位置データ、オンライン識別子のような識別子、又は当該自然人に関する物理的、生理的、遺伝子的、精神的、経済的、文化的若しくは社会的アイデンティティに特有な一つ若しくは複数の要素を参照することによって、直接的に又は間接的に、識別され得る者をいう。
- (1) ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) 「取扱い」とは、自動的な手段であるか否かにかかわらず、個人データ又は個人データの集合に対して行われるあらゆる作業又は一連の作業をいう。この作業は、取得、記録、編集、構造化、保存、修正又は変更、復旧、参照、利用、移転による開示、周知又はその他周知を可能なものにすること、整列又は結合、制限、消去又は破壊することをいう。
- (2) ‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- 「個人データ」の定義は極めて広汎であるが、「ファイリングシステム」概念による限定があることに注意（日本個人情報保護法のように「個人情報」「個人データ」「保有個人データ」には分かれていない）。
- 「取扱い」は取得から破壊までのライフサイクルすべてを指す。

1.4 GDPRは誰が執行するのか

- 第 51 条 監督機関
- Article 51 Supervisory authority
- 1. 各加盟国は、取扱いに関する自然人の基本的権利及び自由を保護するため、及び EU 域内における個人データの自由な流通を促進するため、本規則の適用を監視する責任を持つ一つ又は複数の独立した公的機関を設置しなければならない。
- 1. Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union.
- 「監督機関」「データ保護機関」「DPA (Data Protection Authority)」等と称される。「フライバシーコミッショナー」ということも多い（「コミッショナー」という場合には独任制の機関であるので、委員会方式の場合は正確には入らないことになるが、通商としてはよく使われる）。英国であればICO（情報コミッショナー事務局）、フランスであればCNIL（情報処理と自由に関する国家委員会）、ドイツであれば連邦データ保護観察官（連邦フライバシーコミッショナー）等。
- 一つの機関で、民間・公的機関の全てを監督しているのが普通であるが、国によっては微妙に構成が異なることもある。例えば、ドイツは、民間事業者は州の監督機関が監督している。
- 情報公開についても所管している場合があるが、必須ではない。

第 68 条 欧州データ保護会議

Article 68 European Data Protection Board

- 1. 欧州データ保護会議は本規則によって EU の団体として設置され、法人格を有するものとする。
- 1. The European Data Protection Board (the ‘Board’) is hereby established as a body of the Union and shall have legal personality.
- 2. 欧州データ保護会議は議長を代表とするものとする。
- 2. The Board shall be represented by its Chair.
- 3. 欧州データ保護会議は各加盟国のひとつの監督機関の長、欧州データ保護監察機関の長、又はそれら各代理人によって構成されるものとする
- 3. The Board shall be composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.
- 4. 加盟国において、複数の監督機関が本規則に基づく規定の適用の監視を担当している場合、共同代表者が当該加盟国の国内法に従って任命されるものとする。
- 4. Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, a joint representative shall be appointed in accordance with that Member State's law.
- 5.-6. (略)

参考情報の多重構造

- 法令
 - GDPR, GDPRの前文（リサイクル）
 - 各国の実施法
- ガイドライン
 - 29条作業部会→欧州データ保護会議のガイドライン
 - 欧州データ保護観察官（欧州委員会の行政機関を監督する監督機関に該当し、GDPR上の監督機関ではない）のガイドライン
 - 各国の監督機関のガイドライン
- 意見
 - 欧州議会の意見
 - 各国議会の意見

29条作業部会→欧州データ保護会議のガイドライン

- Guidelines on Consent under Regulation 2016/679 (wp259rev.01) (同意)
- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) (透明性, 通知事項)
- Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01) (個人の自動的決定, プロファイリング)
- Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01) (データ侵害通知)
- Guidelines on the application and setting of administrative fines (wp253). Now including available language versions. (課徴金)
- Guidelines on the Lead Supervisory Authority (wp244rev.01) (主要監督機関)
- Guidelines on Data Protection Officers ('DPOs') (wp243rev.01) (DPO, データ保護監督者)
- Guidelines on the right to "data portability" (wp242rev.01) (データポータビリティ)
- Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) (データ保護影響評価)

個人情報保護委員会による翻訳

- 「GDPRに関するガイドラインのうち、次に掲げるものについては、日本語仮訳を作成いたしましたので、掲載いたします。」
 - データポータビリティの権利に関するガイドライン
 - データ保護オフィサー（DPO）に関するガイドライン
 - 管理者又は処理者の主監督機関を特定するためのガイドライン
 - データ保護影響評価（DPIA）及び取扱いが2016/679規則の適用上、「高いリスクをもたらすことが予想される」か否かの判断に関するガイドライン

第83 条 制裁金の一般条件

Article 83 General conditions for imposing administrative fines

- 1.-3. (略)
- 4. 次に掲げる規定違反は、第2 項に従って、最大10 000 000 ユーロ、又は事業である場合、前会計年度の全世界年間売上高の2%までの、どちらか高い方を制裁金として科すものとする。
- 4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) 第8 条、第11 条、第25 条、第26 条、第27 条、第28 条、第29 条、第30 条、第31 条、第32 条、第33 条、第34 条、第35 条、第36 条、第37 条、第38 条、第39 条、第42 条及び第43 条による管理者及び取扱者の義務。
 - (a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 and 43;
 - (b) 第42 条及び第43 条による認証機関の義務。
 - (b) the obligations of the certification body pursuant to Articles 42 and 43;
 - (c) 第41 条第4 項による監視団体の義務。
 - (c) the obligations of the monitoring body pursuant to Article 41(4).

- 5. 次に掲げる規定の違反は、第2項に従って、最大20 000 000 ユーロ、又は事業である場合、前会計年度の全世界年間売上高の4%までの、どちらか高い方を制裁金として科されるものとする。
- 5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
 - (a) 第5条、第6条、第7条及び第9条による基本的取扱い原則（同意の条件を含む）。
 - (a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
 - (b) 第12条から第22条によるデータ主体の権利。
 - (b) the data subjects' rights pursuant to Articles 12 to 22;
 - (c) 第44条から第49条による第三国又は国際機関の取得者への個人データ移転。
 - (c) the transfers of personal data to a recipient in a third country or an international organization pursuant to Articles 44 to 49;
 - (d) 第9章に基づき採択された加盟国の国内法による義務。
 - (d) any obligations pursuant to Member State law adopted under Chapter IX;
 - (e) 第58条第2項による監督機関による取り扱いに関する命令若しくは一時的若しくは最終的制限又はデータ流通の中止の不遵守、又は第58条第1項違反のアクセス提供の不履行。
 - (e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

- 6. 第58 項第2 項で定める監督機関による命令不遵守は、本条第2 項に従って、最大20 000 000 ユーロ、又は事業である場合、前会計年度の全世界年間売上高の4%までの、どちらか高い方を制裁金として科されるものとする。
- 6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
- 7.-9. (略)
- 罰則（GDPR84条）は各国法の問題。

制裁金算定における一体性と DPOの管轄の範囲

- この「行政罰」は、行政手続法第101条及び第102条に定める行政罰に該当する。行政手続法第101条及び第102条に定める行政罰は、行政手続法第101条及び第102条に定める行政罰に該当する。行政手続法第101条及び第102条に定める行政罰は、行政手続法第101条及び第102条に定める行政罰に該当する。
- TFEUは欧州独禁法の規定であるので経済的一体性で判断されるが、GDPRに引いた場合、データ処理の一体性で判断されるか。それとも経済的一体性で判断されるか。
- DPOの管轄範囲が広ければ広いほど一体性が広く見積もられる可能性

2 GDPR上の権利・義務

2.1 GDPRにおける個人データ取扱いの原則

- 第5条 個人データの取扱いに関する原則
- Article 5 Principles relating to processing of personal data
- 第6条 適法な取扱い
- Article 6 Lawfulness of processing
- 第7条 同意の条件
- Article 7 Conditions for consent
- 目的外利用，第三者提供（及び要配慮個人情報^{の取}得）といった例外的な場面でのみ本人の同意を要求する日本個人情報保護法と異なり，取扱いに対する同意が「原則」として位置付けられていることに注意

第5条 個人データの取扱いに関する原則

Article 5 Principles relating to processing of personal data

- 1. 個人データは、
- 1. Personal data shall be:
 - (a) データ主体との関係において、適法、公正かつ透明性のある手段で取り扱われなければならない。（適法性、公正性及び透明性の原則）
 - (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
 - (b) 特定された、明確かつ適法な目的のために収集されなければならない。これら目的と相容れない方法で更なる取扱いがなされてはならない。ただし、公共の利益における保管目的、科学的若しくは歴史的研究の目的又は統計目的のための更なる取扱いは、第89条第1項により、当初の目的と相容れない方法とはみなされない。（目的の限定の原則）
 - (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');
 - (c) 取り扱われる目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない。（データの最小化の原則）
 - (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

- (d) 正確であり、必要な場合には最新に保たなければならない。取り扱われる目的に照らして、不正確な個人データが遅滞なく消去又は訂正されるのを確保するため、あらゆる合理的な手段が講じられなければならない。（正確性の原則）
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) 当該個人データが取り扱われる目的に必要な期間を超えない範囲で、データ主体の識別が可能な状態で保存されなければならない。個人データは長期間保存されてもよいが、個人データが第89条第1項に従った公共の利益における保管目的、科学的若しくは歴史的研究の目的又は統計目的だけに取り扱われることに限るものとし、データ主体の権利と自由を保護するため本規則によって求められる適切な技術的及び組織的対策の実施を条件とする。（保存の制限の原則）
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

- (f) 当該個人データの適切なセキュリティを確保する方法で取り扱われなければならない。
- それは、無権限の又は違法な取扱いに対する保護、及び偶発的な滅失、破壊、又は損壊に対する保護を含むものとし、適切な技術的又は組織的対策を用いるものとする。（完全性及び機密性の原則）
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').
- 2. 管理者は第 1 項の義務を負い、その遵守を証明可能にしなければならない。（アカウンタビリティの原則）
- 2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1('accountability')

第 6 条 適法な取扱い

Article 6 Lawfulness of processing

- 1. 取扱いは、次に掲げる少なくとも一つの項目が適用される場合に限り、適法とする。
- 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
- (a) データ主体が、一つ又は複数の特定の目的のために自己の個人データの取扱いに同意を与えた場合。
- (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- (b) データ主体が当事者となっている契約の履行のために取扱いが必要な場合、又は契約の締結前のデータ主体の求めに応じて手続を履践するために取扱いが必要な場合。
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) 管理者が従うべき法的義務を遵守するために取扱いが必要な場合。
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) データ主体又は他の自然人の重大な利益を保護するために取扱いが必要な場合。
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) 公共の利益又は管理者に与えられた公的権限の行使のために行われる業務の遂行において取扱いが必要な場合。
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

- (f) **管理者又は第三者によって追求される正当な利益のために取扱いが必要な場合**。ただし、データ主体の、特に子どもがデータ主体である場合の個人データの保護を求めている基本的権利及び自由が、当該利益に優先する場合を除く。
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a
- third party, except where such interests are overridden by the interests or fundamental rights and freedoms
- of the data subject which require protection of personal data, in particular where the data subject is a child.¹⁰
- 第1項前段(f)号は、公的機関が業務を遂行する際になす取扱いには適用されない。
- Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance
- of their tasks
- 2.-4. (略)
- どの条項に基づく移転であるかを意識する必要がある。日本個人情報保護法の場合同意は無敵のように取り扱われているが、7条（次条）により、同意による取扱いは撤回できることに注意しなければならない。

「正統な利益」

- 含一利掘者合が一が含。下び人あ行たのタ
 をデ権根埋場係デ理をう。況及個でての者一
 益く法的管る関人処から。状益が者の理的デ
 利づ的法のいな個に否あ。い利関法お目管人
 な基本の体て切、めか。で。の機立にのタ個
 当に基め主け適よたるる。き体政は行止一の
 正係はた。タ受でせのきあ。で主行の遂防デめ
 の関たの。一を当に的でが待タ。る。の。る。た
 者のま理。デ供安れ目。が要期一。る。め務為す。の。さ
 三と益処。提に。ず。該と必に。デ。す。定職行係。グ。定
 第者利。ば。の。間。い。当。こ。る。的。先。て。の。正。関。ン。推
 は理のりえ務の。、。る。す。理。け。優。つ。そ。不。ィ。と
 た管体限。例役と。る。て。す。を。合。わ。も。よ。が。は。デ。の
 ま。と。主。い。、。ら。者。あ。い。待。価。が。り。り。に。関。た。理。ケ。も
 者。体。タ。な。は。か。理。で。お。期。評。体。と。よ。律。機。ま。処。一。る
 理。主。一。が。益。者。管。す。に。に。く。主。、。益。法。政。の。マ。れ
 管。タ。デ。と。利。理。と。は。脈。的。深。タ。は。利。を。行。い。タ。ト。わ
 る。一。、。こ。な。管。体。る。文。理。意。一。に。の。掘。な。一。ク。行
 け。デ。し。る。当。や。主。す。の。合。注。デ。合。者。根。は。は。デ。レ。に
 受。、。慮。す。止。合。タ。在。そ。が。、。て。場。理。的。掘。で。人。イ。め
 を。は。配。と。な。場。一。存。、。体。は。、。い。る。管。法。根。き。個。タ。た
 示。益。に。の。う。る。デ。、。び。主。て。つ。れ。タ。の。的。的。べ。る。の。
 開。利。待。も。よ。あ。、。は。及。タ。い。に。さ。一。め。法。る。あ。る。の。益
 の。な。期。な。の。で。に。、。一。つ。理。理。デ。た。の。れ。の。す。利
 タ。当。な。的。そ。客。中。合。で。デ。に。処。処。、。る。そ。き。性。成。な。利
 一。正。的。後。顧。の。場。点。を。益。る。が。は。す。、。用。要。構。当
 デ。の。理。劣。る。の。況。る。時。と。利。よ。タ。利。理。み。適。必。を。正
 人。者。合。を。得。ス。状。い。の。こ。な。に。一。権。処。鑑。は。に。益
 個。理。の。由。じ。ビ。な。て。集。る。当。的。デ。な。を。に。に。格。利。は、
 管。体。自。供。一。う。し。収。れ。止。目。的。的。タ。と。理。嚴。な。理
 (47) 主。ひ。提。サ。よ。在。の。わ。れ。止。目。的。的。タ。と。理。嚴。な。理
 め。タ。及。を。の。の。存。タ。行。め。別。で。基。テ。る。う。め。正。の。処

三段階テスト (ICO "Lawful basis for processing --Legitimate interests")

- This can be broken down into a three-part test:
- 1. **Purpose test (目的テスト)** : are you pursuing a legitimate interest?
- 2. **Necessity test (必要性テスト)** : is the processing necessary for that purpose?
- 3. **Balancing test (balancingテスト)** : do the individual's interests override the legitimate interest?

ダイレクトマーケティングはすべて「正統な利益」か？（ICO "Lawful basis for processing -- Legitimate interests"）

- ダイレクトマーケティングは「正統な利益」に該当する「かもしれるない」が、GDPRでは「正統な利益」に基づいて合法だといえるかどうかは、具体的な状況によって異なる。
- **目的テスト**に関しては、他の法的または倫理的基準や業界の行動規範を遵守していないと、マーケティングのいくつかがその形態が正当な関係にある場合、ダイレクトマーケティングの正当性を示す必要がある。また、マーケティングの目的が、他の法的または倫理的基準や業界の行動規範を遵守していない場合、ダイレクトマーケティングの正当性を示す必要がある。依然として、処理が**必要性とバランステスト**に合格していることを示す必要がある。
- また、処理が必要であることと、処理のいくつかの要素について目的に適合していることを示す必要がある。たとえば、プロファイリングを使用してマーケティングをターゲットとする場合。
- マーケティングは個人の利益になることが示唆されることがある。例えば、彼らが自分のニーズに直接関連したお金を使った商品やサービスを受け取った場合など。しかし、**balancing testに大きな重みを加えることはまずない**。顧客の好みに非常に明確な証拠がない限り、顧客の主要な関心事に焦点を当てて、顧客に想定される利益に過度の集中を避けることをお勧めする。
- **場合によっては、マーケティングは、個人の状況に応じて、個人に重大な悪影響を及ぼす可能性がある**。例えば、高利貸しのためのマーケティングを定期的にターゲットとしている、財務上の困難を抱えている、またはそうである可能性がある人は、これらのオフアーにサインアップし、潜在的にさらなる債務を負う可能性がある。

ダイレクトマーケティングはすべて「正統な利益」か？（ICO "Lawful basis for processing -- Legitimate interests"）

Marketing method	Is legitimate interests likely to be appropriate?
Post	✓
'Live' phone calls to TPS/CPTS registered numbers	✗
'Live' phone calls to those who have objected to your calls	✗
'Live' phone calls where there is no TPS/CTPS registration or objection	✓
Automated phone calls	✗
Emails/text messages to individuals – obtained using 'soft opt-in'	✓
Emails/text messages to individuals – without 'soft opt-in'	✗
Emails/text messages to business contacts	✓



Bold voices

Stefan Sagmeister: Designing happiness

[Read more](#)

Cookies

This website uses cookies. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on [more information](#).

[Close](#)

En poursuivant votre navigation, vous acceptez le dépôt de cookies tiers destinés à vous proposer des vidéos, des boutons de partage, des remontées de contenus de plateformes sociales [✓ OK, tout accepter](#)


[Personnaliser](#)

CNIL.

UN PARTICULIER

UN PROFESSIONNEL

Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles

Poser une question ou rechercher un article, une délibération... 



COMPRENDRE VOS DROITS

Comment accéder à vos données personnelles, les rectifier, les supprimer ?

[> Découvrir vos droits](#)



MAÎTRISER VOS DONNÉES

Comment protéger sa vie privée dans le monde numérique ?

[> Découvrir les bonnes pratiques](#)



AGIR

Comment faire valoir ses droits sur ses données ou agir en cas de problème ?

[> Découvrir vos moyens d'actions](#)

BILAN 2017 L'EFFET RGPD : UNE ANNÉE DE PRÉPARATION ACTIVE DE LA TRANSITION, DOUBLÉE D'UNE TRÈS FORTE ATTENTE DES PARTICULIERS ET DES PROFESSIONNELS

Publié le 10/04/2018

#CNIL

[> BESOIN D'AIDE](#)

2018年2月16日ブリュッセル第一審裁判所判決

- The court supported all of the arguments put forward by the Privacy Commission.
- First, the court declared itself competent to rule on this matter. Facebook contested the jurisdiction of the Belgian judges vis-à-vis its American parent company and its Irish subsidiary. However, the Court found that it effectively has the jurisdiction to evaluate whether Facebook complies with Belgian privacy legislation when it tracks the browsing behavior of Internet users in Belgium.
- The Court also found that Facebook does not comply with Belgian privacy legislation on the basis of the investigation undertaken by the Privacy Commission.
- The investigation shows that Facebook collects information concerning all of us when we browse the Internet. To this end, Facebook uses various technologies, such as the well-known "cookies" or "social plug-ins" (for example, the "like" or "share" buttons) or also "pixels", which are invisible to the naked eye. It uses them on its own website, but also and most importantly on websites of third parties. The investigation reveals, for example, that even if you have never visited the Facebook domain, Facebook is still able to track your browsing behavior without you realizing it, let alone want it, through these invisible pixels that Facebook has placed on more than 10,000 other websites.
- **The Court concludes, in line with the Privacy Commission, that Facebook (1) does not sufficiently inform users about the fact that it collects information about us, on the nature of the collected information, on the use of this information and on how long it retains this information and 2) does not obtain valid consent from users to collect and process all this information.**

- In short, the Court orders, as requested by the Privacy Commission, that:
- Facebook must stop tracking and recording the browsing behavior of persons browsing from Belgium as long as it does not bring its practices in line with Belgian privacy legislation.
 - Facebook must destroy all illegally obtained personal data.
 - Facebook must publish the entire 84-paged judgment on its website and must publish in Dutch- and French-language Belgian newspapers the last three pages of this judgment where the imposed measures are listed.
 - If Facebook does not comply with this judgment, it will be forced to pay a penalty to the Privacy Commission amounting to 250,000 euros per day of delay, with a maximum of 100 million euros.
- *“Of course, we are very satisfied that the court has fully supported our position. Facebook is currently conducting a big advertising campaign through which it underlines its commitment to privacy. We hope it will put this commitment into practice”, says the Privacy Commission.*

第 7 条 同意の条件

Article 7 Conditions for consent

- 1. 取扱いが同意に基づく場合、管理者は、データ主体が自己の個人データの取扱いに対して同意しているということを証明できるようにしなければならない。
- 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
- 2. データ主体の同意が他の案件にも関係する書面において与えられている場合、その同意の要求は、明瞭かつ平易な文言を用い、理解しやすくかつ容易にアクセスし得る形で、その他の案件と明らかに区別できる方法によって明示されなければならない。 本規則違反を含んだあらゆる宣言は拘束力がないものとする。
- 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

- 3. ~~データ主体は、いつでも同意を撤回する権利があるものとする。また、同意の撤回は撤回前の同意に基づく取扱いの合法性に影響を与えない。~~
 データ主体は、同意を与える以前にその旨が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。
- 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw consent as to give it.
- 4. 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な個人データの取扱いに対する同意を条件としているか否かについて、最大限の考慮が払われなければならない。
- 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

第9条 特別な種類の個人データの取扱い Article 9 Processing of special categories of personal data

- 1. 人種若しくは民族的素性、政治的思想、宗教的若しくは哲学的信条、又は労働組合員資格に関する個人データの取扱い、及び遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータ又は自然人の性生活若しくは性的指向に関するデータの取扱いは禁止する。
- 1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

- 2. 第 1 項は次に掲げる場合には適用されない。
- 2. Paragraph 1 shall not apply if one of the following applies:
 - (a) データ主体が、一つ又は複数の特定された目的のために当該個人データの適用に対して **明示的な同意** を与えた場合。ただし、EU 法又は加盟国の国内法が、第 1 項で定める禁止事項がデータ主体によって解除されるべきではないと定めている場合を除く。
 - (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
 - (b)-(j) (略)
 - 3.-4. (略)

2.2 GDPRにおけるデータ主体の権利

- 第1 節 透明性及び手続
 - 第12 条 データ主体の権利行使のための透明性のある情報、通知及び手続
- 第2 節 情報及び個人データへのアクセス
 - 第13 条 データ主体から個人データを収集する場合に提供される情報
 - 第14 条 データ主体から個人データを取得しない場合に提供される情報
 - 第15 条 データ主体のアクセス権
- 第3 節 訂正及び消去
 - 第16 条 訂正の権利
 - 第17 条 消去の権利（忘れられる権利）
 - 第18 条 取扱い制限の権利
 - 第19 条 個人データの訂正若しくは消去又は取扱いの制限に関する通知義務

- 第4 節 異議を唱える権利及び個人に対する自動化された意思決定
 - 第21 条 異議を唱える権利
 - 第22 条 プロファイリングを含む自動化された個人意思決定
- 第5 節 制限
 - 第23 条 制限

第12 条 データ主体の権利行使のための透明性のある情報、通知及び手続

Article 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

- 1. 管理者は、第13 条並びに第14 条で定めるあらゆる情報及び第15 条から第22 条並びに第34 条に基づくあらゆる通知を提供するため適切な手段をとらなければならない。データ主体に対する取扱いに関し、明瞭かつ平易な文言が使われ、簡潔で、透明性があり、理解しやすくかつ容易にアクセスし得る形態をもつて情報及び通知が行われるものとする。とりわけ子どもに対して特に書かれた情報は適切な手段をとるものとする。当該情報は書面で提供されるものとし、適切な場合、電子的手段を含め、その他手段によっても提供されるものとする。データ主体によって要求され、データ主体の身元がその他の手段で証明されるならば、情報は口頭で提供されてもよい。
- 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.
- 2. (略)

- 3. 管理者は、第15条から第22条に基づく要求に基づいて取られた行為に関する情報を不当な遅滞なしに、いかなる場合でもその要求を受け取ってから1カ月以内に、データ主体に提供しなければならない。当該期間は、要求の複雑性又は数を考慮し、必要に応じて、更に2カ月まで延長することができる。管理者は、要求を受け取ってから1カ月以内に、遅滞の理由とともに、当該延長をデータ主体に通知するものとする。データ主体が電子的手段で要求を行う場合、データ主体によって要求がなされない限り、可能であるならば電子的手段で通知は提供されるものとする。
- 3. The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.
- 4.- (略)

第13 条 データ主体から個人データを収集する場合に提供される情報

Article 13 Information to be provided where personal data are collected from the data subject

- 1. データ主体に係る個人データがデータ主体から収集される場合、管理者は、個人データを取得
- する際、データ主体に次に掲げるすべての情報を提供するものとする。
- 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the
- time when personal data are obtained, provide the data subject with all of the following information:
- (a)-(f) (略)
- 2. (略)

第14 条 データ主体から個人データを取得しない場合に提供される情報

Article 14 Information to be provided where personal data have not been obtained from the data subject

- 1. 個人データがデータ主体から取得されない場合、管理者は次に掲げる情報をデータ主体に提供しなければならない。
- 1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information:
 - (a)-(f) (略)
 - 2.-5. (略)

第15 条 データ主体のアクセス権

Article 15 Right of access by the data subject

- 1. データ主体は、管理者から当該データ主体に関する個人データを取り扱っているか否か確認を得る権利を持ち、取り扱っている場合、個人データ及び次に掲げる情報にアクセスする権利を持つ。
- 1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and where that is the case, access to the personal data and the following information:
- (a)-(h) (略)
- 2. (略)
- 3. 管理者は取扱いを行っている個人データの複製を提供するものとする。データ主体によって要求されたあらゆる追加的複製に関して、管理者は管理費用に基づき過度にならない程度の手数料を徴収することができ、データ主体が電子的手段によって要求する場合、データ主体による要求がない場合を除き、情報は一般的に用いられる電子的形態で提供されるものとする。
- 3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
- 4. (略)

第16条 訂正の権利

Article 16 Right to rectification

- データ主体は当該データ主体に関する不正確な個人データを訂正させる権利を追加の記入も提供し、訂正を求め、データを完全にする権利を持つものとする。
- The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

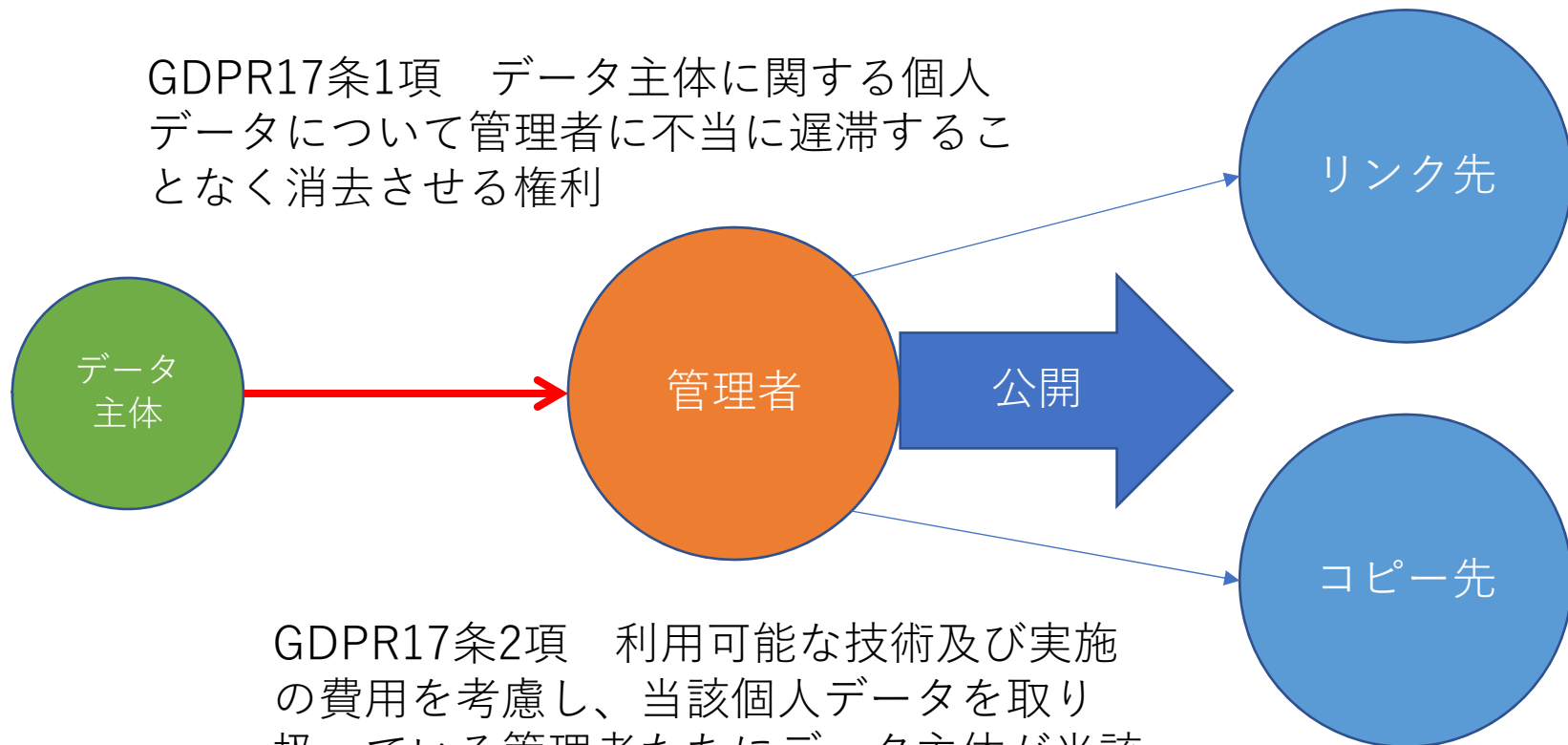
第17 条 消去の権利（忘れられる権利）

Article 17 Right to erasure ('right to be forgotten')

- 1. データ主体は当該データ主体に関する個人データについて管理者に不当に遅滞することなく消去させる権利を持つものとする。管理者は、次に掲げる根拠のいずれかが適用される場合、個人データを不当に遅滞することなく消去する義務を負うものとする。
- 1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
- (a) 個人データが収集された又はその他取扱いの目的に関して、当該個人データがもはや必要ない場合。
- (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- (b) 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取扱いの同意を撤回し、かつ取扱いに関して他の法的根拠がない場合。
- (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
- (c) データ主体が、第21 条第1 項により不服を申立て、かつ取扱い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。
- (c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
- (d) 個人データが不法に取り扱われた場合。
- (d) the personal data have been unlawfully processed;
- (e)-(f) (略)

- ~~2. 管理者が個人データを公開しており、第1項による個人データを消去する義務を負う場合、その管理者は、利用可能な技術及び実施の費用を考慮し、当該個人データを取り扱っている管理者たちにデータ主体が当該個人データのあらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならない。~~
- 2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
- 3. 第1項及び第2項は、取扱いが次に掲げるいずれかに必要な場合、適用されない。
- 3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
- (a)-(e) (略)
- 「忘れられる権利」としてここ数年問題となっているものには二種類の内実があり、
 - ①検索エンジンの検索結果削除の問題
 - ②GDPR17条2項の問題
- がある。①についてはGDPR上の問題でなく、データ保護指令上の問題として欧州司法裁判所の先決裁定 (Google Spain SL and Google Inc. v. AEPD(C-131/12)) で既に問題となり、認められたものである。

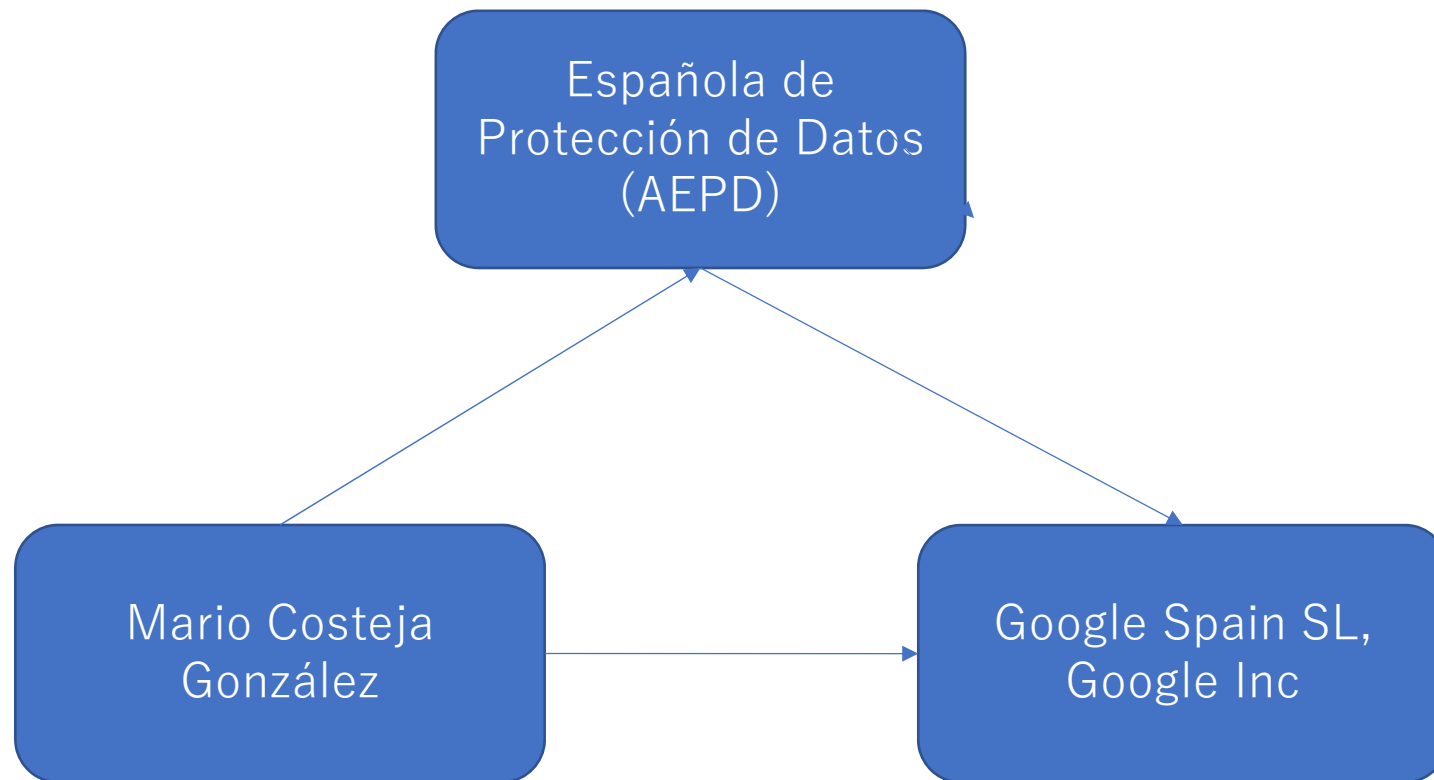
GDPR17条1項 データ主体に関する個人データについて管理者に不当に遅滞することなく消去させる権利



GDPR17条2項 利用可能な技術及び実施の費用を考慮し、当該個人データを取り扱っている管理者たちにデータ主体が当該個人データのあらゆるリンク又はコピー若しくは複製の消去を要求している旨を通知するために、技術的措置を含む合理的手段をとらなければならない

参考：グーグルスペイン事件

- Google Spain SL, Google Inc. V Agencia Española de Protección de Datos (AEPD), Mario Costeja González (Case C-131/12), 13 May 2014
- 請求根拠はデータ保護指令12条



論点

- ①データ保護指令の適用範囲
 - 「加盟国内に設置されたデータ管理者」（指令4条a項）といえるか
- ②データ処理者及び管理者該当性
 - 検索エンジンによるインデックス情報を一時的に蓄積しているだけで処理（指令2条b項），管理（指令2条d項）しているといえるか
- ③検索サイトから公表された情報について削除権（指令12条），異議申立権（指令14条）が認められるか

結論

- ①データ保護指令の適用範囲
 - 広告スペースの促進，販売の意図，加盟国の住民に向けた活動を行っている視点の加盟国内での設置→加盟国内の領土において管理者の設置の活動に関連して個人データの処理
- ②データ処理者及び管理者該当性
 - 検索エンジンは管理者
- ③検索サイトから公表された情報について削除権（指令12条），異議申立権（指令14条）が認められるか
 - 氏名による検索で表示される結果リストにおける情報及びリンクは削除されなければならない

欧州のプライバシー法に基づく検索結果の削除

欧州連合司法裁判所の 2014 年 5 月の判決で、個人が Google のような検索エンジンに対し、自身に関する特定の検索結果を削除するよう要請する権利が認められました。このレポートは、削除リクエストの数、実際に除外された URL の数、削除リクエストを提出したユーザーの数、リクエストで特定されたウェブサイトと URL のコンテンツに関するデータをまとめたものです。

プライバシー法に沿った Google 検索結果からの URL の除外

欧州連合司法裁判所の 2014 年 5 月の判決で、個人が Google のような検索エンジンに対し、個人の名前に基づく検索クエリの特定の検索結果を削除するよう要請する権利が認められました。検索エンジンは、個人の社会的役割を含め、公共の利益に資する要因を考慮し、問題のリンクが「不適切である、無関係である、現在は無関係になっている、または過度である」場合にこれに従う必要があります。検索結果から除外されるのは、個人の名前をキーワードとする検索で表示されるページのみです。Google は欧州のすべての Google 検索結果（フランス、ドイツ、スペインなどでのユーザーの検索結果）から該当 URL を除外し、削除リクエストを行った人の国からの該当 URL に対するアクセスを位置情報信号に基づいて制限します。次のグラフは、2014 年 5 月 29 日以降に Google が受け取ったリクエストの総数と除外がリクエストされた URL の総数を示しています。

除外リクエスト

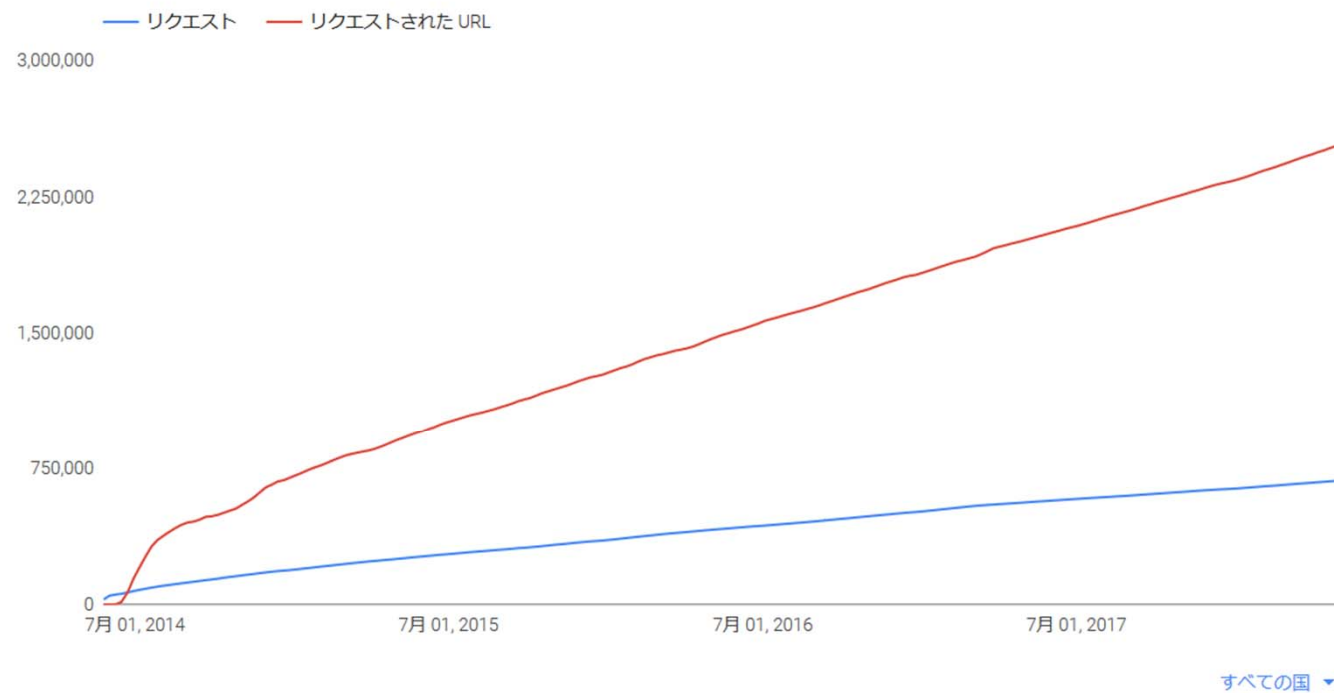
681,073

除外がリクエストされた URL

2,537,265

リクエスト数の推移

リクエスト数の推移



最も影響の大きいサイト

Google 検索からほとんどの URL を除外したドメインの一覧です。

すべての国 ▼

ドメイン	除外された URL	リクエストされた合計 URL 数
www.facebook.com	18,925	45,145
annuaire.118712.fr	13,027	16,762
profileengine.com	11,485	13,542
twitter.com	10,512	24,960
www.youtube.com	9,711	25,598
groups.google.com	8,522	17,531
plus.google.com	8,056	32,681
scontent.cdninstagram.com	7,491	13,080
badoo.com	5,765	10,614
www.wherevent.com	5,734	6,667

世界削除の問題・グーグル対CNIL事件（フランス）

- 2015年6月、フランスのデータ保護機関（CNIL）が、欧州司法裁判所決定を受けて、世界削除をするようにグーグルに命令。グーグルは欧州域内しか削除していなかった（97%は.fr等のローカルドメインを使用）。
- 2015年7月、グーグルは従わないこととし、informal appeal。
- 2016年3月24日、10万ユーロの課徴金。
- 2016年5月、Appealは棄却され、コンセイユ・デタに上告。
 - 「それを認めてしまうと、非民主的な国家が、情報を統制するための自国の法律を、国際的に認めるように要求し始めるだろう」と懸念を表明（Google、「忘れられる権利」に関する仏・CNILの命令に対して上告、カレントアウェアネス2016年5月23日）
- 2017年7月19日、コンセイユ・デタは欧州司法裁判所に判断を求めた。



LE CONSEIL D'ÉTAT ET LA JURIDICTION ADMINISTRATIVE

[Recherche](#)

[Recherche jurisprudentielle](#)

[Accueil](#)

[Conseil d'État](#)

[Tribunaux & Cours](#)

[Décisions, Avis & Publications](#)

[Actualités](#)

[Accueil](#) / [Décisions, Avis & Publications](#) / [Décisions](#) / [Sélection des décisions faisant l'objet d'une communication...](#) / CE, 19 juillet 2017, GOOGLE INC.

19 juillet 2017

CE, 19 juillet 2017, GOOGLE INC.

N° 399922

[> Lire le communiqué](#)

Le Conseil d'Etat statuant au contentieux (Section du contentieux, 10ème et 9ème chambres réunies) sur le rapport de la 10ème chambre de la Section du contentieux

Séance du 28 juin 2017 - Lecture du 19 juillet 2017

Vu la procédure suivante :

Par une requête sommaire, un mémoire complémentaire, un mémoire en réplique et trois autres mémoires, enregistrés le 19 mai, le 12 août, le 2 novembre et le 7 décembre 2016 et le 25 janvier et le 19 avril 2017 au secrétariat du contentieux du Conseil d'Etat, la société Google Inc. demande au Conseil d'Etat :



ECOUTER

Décisions, Avis & Publications

Décisions

[ArianeWeb](#)

[Sélection des décisions
faisant l'objet d'une
communication particulière](#)

[Les décisions les plus
importantes du Conseil d'État](#)

Avis

[Études & Publications](#)

[Se procurer les actes du Conseil
d'État](#)

Request for a preliminary ruling from the Conseil d'État (France)
lodged on 21 August 2017 — Google Inc. v Commission nationale de
l'informatique et des libertés (CNIL)(Case C-507/17)

- Questions referred
- 1. Must the 'right to de-referencing', as established by the Court of Justice of the European Union in its judgment of 13 May 2014¹ on the basis of the provisions of Articles 12(b) and 14(a) of Directive [95/46/EC] of 24 October 1995, 2 be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46/EC] of 24 October 1995?

- 2. In the event that Question 1 is answered in the negative, must the ‘right to de-referencing’, as established by the Court of Justice of the European Union in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester’s name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States of the European Union?

- 3. Moreover, in addition to the obligation mentioned in Question 2, must the ‘right to de-referencing’, as established by the Court of Justice of the European Union in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the ‘geo-blocking’ technique, from searches conducted on the basis of the requester’s name from an IP address deemed to be located in the State of residence of the person benefiting from the ‘right to de-referencing’, or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46/EC] of 24 October 1995, regardless of the domain name used by the internet user conducting the search?

第18条 取扱い制限の権利

Article 18 Right to restriction of processing

- 1. データ主体は、次に掲げる事項の一つでも当てはまる場合、管理者に取扱いの制限をさせる権利をもつ。
- 1. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
- (a) 管理者が個人データの正確性を検証できる期間内で、データ主体によって個人データの正確性に不服が申し立てられた場合。
- (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
- (b) 取扱いが違法であり、データ主体が、個人データの消去に反対するものの、利用の制限を要求する場合。
- (b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- (c) 管理者が取扱いの目的に関し個人データをもはや必要としないが、法的主張時の立証、行使又は抗弁のためにデータ主体によって要求された場合。
- (c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- (d) 管理者の法的根拠がデータ主体の主張に優先するか否かの検証が未決定時に、データ主体が第21条第1項により取扱いに不服を申し立てた場合。
- (d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.
- 2.-3. (略)

第20 条 データポータビリティー の権利

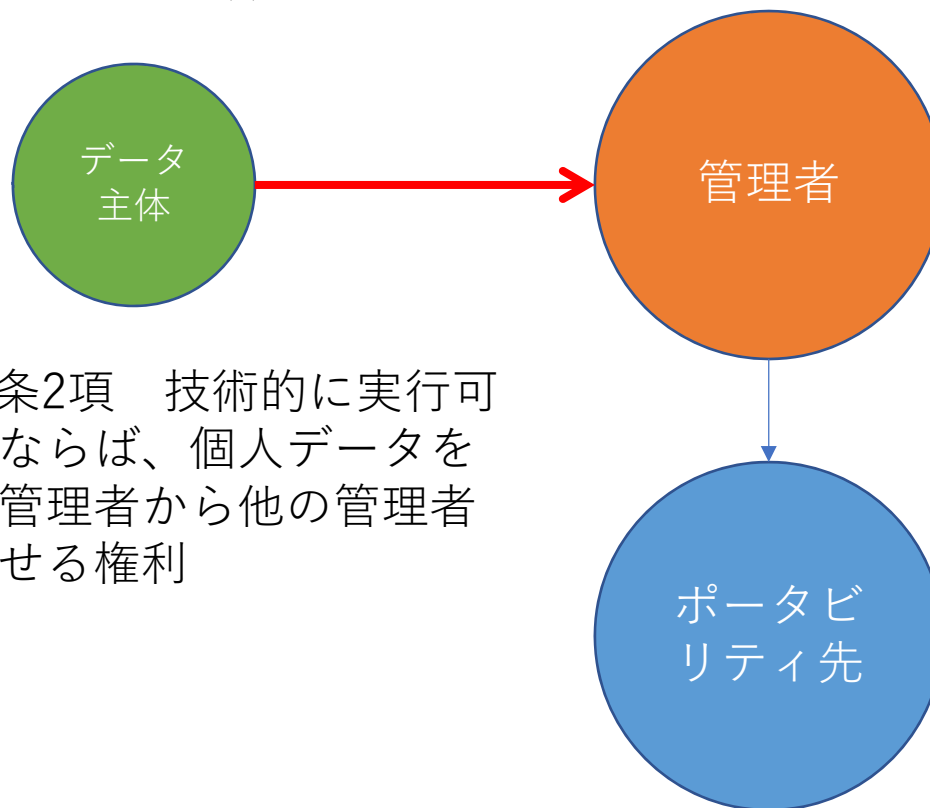
Article 20 Right to data portability

- 1. 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。
 - 1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided,
- where:
 - (a) 取扱いが第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か、第6 条第1 項(b)号による契約に基づく場合であり、かつ
 - (a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
 - (b) 取扱いが自動化された手法で実行されている場合。
 - (b) the processing is carried out by automated means.
- 2. 第1 項により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。
 - 2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
- 3.-4. (略)

GDPR20条1項 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

(a) 取扱いが第6条第1項(a)号又は第9条第2項(a)号による**同意**に基づくか、第6条第1項(b)号による**契約**に基づく場合であり、かつ

(b) **取扱いが自動化された手法で実行されている**場合。



GDPR20条2項 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

第21 条 異議を唱える権利

Article 21 Right to object

- 1. データ主体は、当該データ主体のそれぞれの状況に関する理由を根拠として、第6条第1項(e)号又は(f)号に基づくプロファイリングを含む当該条項を根拠とした自己に関する個人データの取扱いに対して、いつでも異議を唱える権利を有する。管理者は、データ主体の利益、権利及び自由に優先する取扱いのための、又は法的主張時の立証、行使若しくは抗弁のための差し迫った正当な根拠であることを示さない限り、もはや個人データを取り扱ってはならない。
- 1. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on points (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
- 2. 個人データがダイレクトマーケティングのために取り扱われるならば、データ主体は、当該マーケティングのための当該データ主体に関する個人データの取扱いに対して、いつでも異議を唱える権利を持つ。当該ダイレクトマーケティング範囲内のプロファイリングを含む。
- 2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
- 3. データ主体がダイレクトマーケティングの目的のための取扱いに異議を唱える場合、個人データは当該目的で取り扱われてはならない。
- 3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
- 4.-6. (略)

ダイレクトマーケティングに異議を唱えられたらどうなるのか

- 例：同意（6条1項(a)号）及び「正統な利益」（6条1項(f)号）を根拠として扱っていた場合
 - 同意の撤回（7条3項）→「正統な利益」のみが残る
 - 正統な利益への異議（21条1項）→「差し迫った正統な根拠」がなければ同意のみが残る
 - ダイレクトマーケティングへの異議（21条2項）→処理根拠にかかわらず異議が認められる
- 処理の法的根拠がなくなったらどうなるのか
 - 消去権（17条1項(a)(c)による）
 - 取扱い制限の権利（18条1項(b)による）

第22 条 プロファイリングを含む自動化された個人意思決定

Article 22 Automated individual decision-making, including profiling

- 1. データ主体は、当該データ主体に関する法的効果をもたらすか又は当該データ主体に同様の重大な影響をもたらすプロファイリングなどの自動化された取扱いのみに基づいた決定に服しない権利を持つ。
- 1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
- 2. 第1 項は次に掲げるいずれかの決定には適用されない。
- 2. Paragraph 1 shall not apply if the decision:
 - (a) データ主体とデータ管理者間の契約締結、又は履行に必要な決定。
 - (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - (b) データ主体の権利及び自由並びに正当な利益を保護するための適切な対策が定められた管理者が従うEU 法又は加盟国の国内法によって認められた決定。
 - (b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - (c) データ主体の明示的な同意に基づく決定。
 - (c) is based on the data subject's explicit consent

- 3. 第2項(a)号及び(c)号で定める状況に関して、データ管理者は、データ主体の権利及び自由並びに正当な利益を保護するための適切な対策を実施し、少なくとも管理者側で人を介在させる権利、当該データ主体の観点を表明する権利、及び決定に同意する権利を実施するものとする。
- 3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
- 4. 第2項で定める決定は、~~第9条第2項(a)号又は(g)号が適用されず、データ主体の権利及び自由並びに正当な利益を保護するための適切な対策が機能していないならば、第9条第1項で定める特別な種類の個人データに基づいてはならない。~~
- 4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) apply and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.
- 与信管理に適用されるか？
 - 22条1項柱書該当性
 - 22条1項(a)該当性
 - 22条4項該当性

2.3 GDPRにおけるデータ管理者・データ処理者の義務

- 第4章 管理者及び取扱者
 - 第1節 一般的義務
 - 第24条 管理者の責任
 - 第25条 データ保護バイデザイン及びデータ保護バイデフォルト
 - 第26条 共同管理者
 - 第27条 EU域内に拠点のない管理者又は取扱者の代理人
 - 第28条 取扱者
 - 第29条 管理者又は取扱者の権限下での取扱い
 - 第30条 取扱い活動の記録
 - 第31条 監督機関との協力
 - 第2節 個人データの保護
 - 第32条 取扱いの保護
 - 第33条 個人データ侵害の監督機関への通知
 - 第34条 データ主体への個人データ侵害の通知

- 第3 節 データ保護影響評価及び事前協議
 - 第35 条 データ保護影響評価
 - 第36 条 事前協議
- 第4 節 データ保護オフィサー
 - 第37 条 データ保護オフィサーの指名
 - 第38 条 データ保護オフィサーの地位
 - 第39 条 データ保護オフィサーの業務

第24 条 管理者の責任

Article 24 Responsibility of the controller

- 1. 取扱いの性質、範囲、文脈及び目的並びに自然人の権利及び自由に関するリスクの様々な可能性及び重大性を考慮し、管理者は本規則に従って取扱いが実行されていることを保証及び証明するため適切な技術的及び組織的対策を実施しなければならない。これら対策は見直され、必要に応じて更新されなければならない。
- 1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.
- 2. 取扱い活動に関して比例しているならば、第1 項で定める対策は、管理者によって適切なデータ保護方針の実施を含めるものとする。
- 2. Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.
- 3. (略)
- 「EEA域内の拠点から標準契約条項（SCC）によってEEA域外の拠点へ個人データを移転させる場合、当該個人データの処理に関して、GDPRに対応したデータ保護方針を制定・施行する必要がある。たとえば、日本企業の場合は、日本において、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ことが考えられる。」（[杉本]）

第25 条 データ保護バイデザイン及びデータ保護バイデフォルト

Article 25 Data protection by design and by default

- 1. 到達水準、実施の管理費用、取扱いの性質、範囲、文脈及び目的、並びに取扱いの様々な点（例えばデータの最小化）を考慮し、権利及び自由に関する要件（例えば匿名化）を効果的に実施する方法を、この条の趣意に従って、適切な技術的及び組織的保護措置を講ずるものとする。
- 1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.
- 2.-3. (略)

第27 条 EU 域内に拠点のない管理者又は取扱者の代理人

Article 27 Representatives of controllers or processors not established in the Union

- 1. 第3 条第2 項が適用される場合、管理者又は取扱者はEU 域内の代理人を書面で明示しなければならない。
- 1. Where Article 3(2) applies, the controller or the processor shall designate in writing a representative in the Union.
- 2. 当該義務は次に掲げるいずれかの場合には適用されない。
- 2. This obligation shall not apply to:
 - (a) 第9 条第1 項で定める特別な種類のデータの取扱い又は第10 条で定める有罪判決及び犯罪に関する個人データの取扱いを大規模に含まず、取扱いの性質、文脈、範囲及び目的を考慮して自然人の権利又は自由に対するリスクが生じそうにない、散発的になされる取扱い。
 - (a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or
 - (b) 公的機関又は団体。
 - (b) a public authority or body.

- 3. 代理人は、データ主体が居住し、当該データ主体への商品やサービスの提供に関連して当該データ主体の個人データが処理されるか、又は当該データ主体の行動が監視される加盟国の一つに拠点を持たなければならない。
- 3. The representative shall be established in one of those Member States where the data subjects are and whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored.
- 4. 代理人は、本規則遵守を確実にする目的のため、取扱いに関連するすべての問題について、管理者若しくは取扱者とともに又は代わりに、特に、監督機関及びデータ主体と対話をするため、管理者又は取扱者によって委任されなければならない。
- 4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.
- 5. 管理者又は取扱者による代理人の任命は、管理者又は取扱者自身に対して取られる法的行為を妨げることはない。
- 5. The designation of a representative by the controller or processor shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.
- 「日本の事業者は、受託者を含め、EUのデータ全体に向けて商品やサービスを提供したり、行動追跡を行う場合には、EU内に代理人を設置しなければならず、遵守しない場合は制裁の対象となる。」（[石井]）

第28 条 取扱者

Article 28 Processor

- 1. 管理者の代わりに取扱いが実施される場合、その管理者は、取扱いが本規則の要件に合致し、データ主体の権利の保護を確実にする取扱い方法で、適切な技術的及び組織的な対策を実施することを十分に保証する取扱者のみを利用しなければならない。
- 1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.
- 2. 取扱者は、事前の特定又は管理者の一般的な書面の許可なしに他の取扱者を従事させてはならない。一般的な書面の許可の場合、取扱者は、他の取扱者の追加又は代替に関するあらゆる意図された変更について管理者に通知しなければならず、それによって管理者に当該変更に対する不服を申し立てる機会を提供するものとする。
- 2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.
- 3.-10. (略)
- GDPRが適用される場合、取扱者（委託先）を利用する場合には、取扱者もGDPRに従っている必要がある。
- 取扱者（委託先）が再委託を行う場合の取扱者もGDPRに従っている必要がある。

第30 条 取扱い活動の記録

Article 30 Records of processing activities

- 1. 各管理者及び、該当する場合、管理者の代理人は、管理下にある取扱い活動の記録を管理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。
- 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
 - (a) 管理者の名前と連絡先の詳細。該当する場合、共同管理者、管理者の代理人及びデータ保護オフィサーを含む。
 - (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
 - (b) 取扱いの目的。
 - (b) the purposes of the processing;
 - (c) データ主体の種類と個人データの種類の概要。
 - (c) a description of the categories of data subjects and of the categories of personal data;

- (d) 第三国又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又は開示される取得者の種類。
- (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
- (e) 該当する場合、第三国又は国際機関を特定した形式による第三国又は国際機関への個人データ移転、及び、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。
- (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of appropriate safeguards;
- (f) 可能であれば、データ種類ごとの消去までの予測される期限。
- (f) where possible, the envisaged time limits for erasure of the different categories of data;
- (g) 可能であれば、第32条第1項で定める技術的及び組織的安全保護措置の概要。
- (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
- 2. (略, 取扱者に関する規定)

- 3. 第1 項及び第2 項で定める記録は、電子的形態を含め、書面でなければならない。
- 3. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
- 4. 管理者又は取扱者及び、該当する場合、管理者又は取扱者の代理人は要求に応じて記録を監督機関が入手可能にしなければならない。
- 4. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
- 5. 第1 項及び第2 項で定める義務は、**250 人未満を雇用している企業又は組織には適用されない**。ただし、取扱いの実施がデータ主体の権利及び自由へのリスクを生じさせ得るか、取扱いの頻度が稀ではないか、又は第9 条第1 項で定める特別な種類のデータ若しくは第10 条で定める有罪判決及び犯罪に関する個人データを含む取扱いを行っていない場合に限る。
- 5. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organization employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
- 参考：前文13 欧州連合の機関及び組織並びに構成国及びその監督官は、この規則の適用に際して、マイクロ企業及び中小企業の特別の必要性を考慮に入れることが推奨される。マイクロ企業及び中小企業概念については、委員会勧告 2003/361/EC1の別紙の第2 条に示すとおりである。
 - 中小企業：250名未満，年商5000万ユーロ未満，及び年次の貸借対照表の合計4300万ユーロ未満
 - 小規模事業者：50名未満，年商及び年次の貸借対照表の合計1000万ユーロ未満
 - 零細事業者：年商及び年次の貸借対照表の合計10名未満，200万ユーロ未満

第32 条 取扱いの保護

Article 32 Security of processing

- 1. 到達水準、実施の管理費用、取扱いの性質、範囲、文脈及び目的、並びに引き起こされる自然人の権利及び自由に関する様々な可能性及び重大性のリスクを考慮し、管理者及び取扱者は、保護レベルをリスクに見合ったものにすため、適切な技術的及び組織的対策を実施しなければならない。必要に応じて特に次に掲げる事項を含むものとする。
- 1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
 - (a)-(d) (略)
 - 2.-4. (略)
- いわゆる安全管理措置義務。

第33 条 個人データ侵害の監督機関への通知

Article 33 Notification of a personal data breach to the supervisory authority

- 1. 個人データの侵害が発生した場合、~~管理者は、不当な遅滞なしに、可能であれば、侵害に気が付いてから72時間以内に、第55条に従って個人データの侵害を管轄監督機関に通知しなければならない。~~ただし、個人データの侵害により自然人の権利又は自由に対するリスクが生じ得ない場合を除く。監督機関への通知が72時間以内になされない場合には、遅滞に関する理由と共に通知されなければならない。
- 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
- 域外適用の場合、どこを「管轄監督機関」として報告すればよいのか？
 - Guidelines on The Lead Supervisory Authority, wp244rev.01_en（主要監督機関）
 - 「主たる事業所又は管理者若しくは取扱者の単一の事業所の監督機関」（GDPR56条）

- 2. 取扱者は、個人データの侵害に気付いた後、不当な遅滞なしに管理者に通知しなければならない。
- 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
- 3. 第1項で定める通知は少なくとも次に掲げる事項が含まなければならない。
- 3. The notification referred to in paragraph 1 shall at least:
 - (a) 個人データ侵害の性質の記述。可能であれば、関連するデータ主体の種類及び概数並びに関連する個人データの記録の種類及び概数を含む。
 - (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (b) データ保護オフィサーの氏名及び詳細な連絡先又はより情報が入手できるその他連絡先の通知。
 - (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - (c) 個人データ侵害に関する起こり得る結果の記述。
 - (c) describe the likely consequences of the personal data breach;
 - (d) 個人データ侵害に対処するために管理者によって取られている又は取られることが意図された対策の記述。適切な場合、個人データ侵害により起こり得る悪影響を軽減するための対策を含む。
- 4.-5. (略)

「主たる事業所」とは

- [illegible]

第34 条 データ主体への個人データ侵害の通知

Article 34 Communication of a personal data breach to the data subject

- 1. 個人データ侵害が自然人の権利及び自由に対して高リスクを引き起こし得る場合、管理者は、不当な遅滞なしにデータ主体に個人データ侵害について通知しなければならない。
- 1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
- 2. 本条第1 項で定めるデータ主体への通知はデータ侵害の性質について明白で平易な文章で記述され、少なくとも、第33 条第3 項(b)号、(c)号及び(d)号で規定された情報並びに推奨事項を含むものとする。
- 2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and the recommendations provided for in points (b), (c) and (d) of Article 33(3).
- 3.-4. (略)

第35 条 データ保護影響評価

Article 35 Data protection impact assessment

- 1. 特に新たな技術を用いるなどの目的を考慮し、その性質、範囲、文脈及び取扱いが、自然人の権利や自由、取扱いの影響の程度、また、特定の個人データが、その管理に用いられる場合、個人データの保護に与える影響の程度を評価することができ、その結果、高リスクと認められる場合には、事前に評価を実施し、その結果、高リスクと認められる場合には、その取扱いを中止し、または、その取扱いを制限する必要がある。
- 1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
- 2.-11 (略)

第37 条 データ保護オフィサーの指名

Article 37 Designation of the data protection officer

- 1. 管理者及び処理者は、次に掲げるいずれかの場合には、データ保護オフィサーを指名しなければならない。
- 1. The controller and the processor shall designate a data protection officer in any case where:
 - (a) 取扱いが公的機関又は団体によって行われる場合。ただし、司法能力をもとにした裁判所の行為を除く。
 - (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
 - (b) 管理者又は処理者の中心的業務が、その性質、適用範囲及び/又は目的によって、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取扱い作業である場合。
 - (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
 - (c) 管理者又は処理者の中心的業務が、第9条で言及された特別な種類のデータ及び第10条で定める有罪判決及び犯罪に関する個人データを大規模に取扱う場合。
 - (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.
- 2.-3. (略)
- 4. 第1項で定める場合以外でも、管理者若しくは取扱者又は組織及び管理者又は処理者の分野を代表するその他の団体は、データ保護オフィサーを任命してもよく、EU法又は加盟国の国内法で要求されているならば、任命しなければならない。データ保護オフィサーは当該組織及び管理者又は取扱者を代表する団体のために行動することができる。
- 4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.
- 5.-7. (略)

DPOの設置義務についての国内法等

- 1項(b)(c)は大規模なデータの取扱い事態を中心的業務とするものだが、
- 「加盟国の国内法で要求されている」（4項）場合にはDPOの設置義務がある。ドイツ連邦データ保護法（実施法）では10名の従業員を雇用する企業は、DPOを専任する義務を負う。DPIAを行う場合にもDPOを選任する義務を追う。
- 「DPOの選任が義務付けられる実務であるかの判断は必ずしも容易ではないため、当該判断については文書化しておくことが望ましい。」（[杉本]）
- IAPPによればEU内で約28,000名、日本で約1,700名、全世界で約75,000名のDPOが必要となるとされている。
 - <https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/>

第38条 データ保護オフィサーの地位

Article 38 Position of the data protection officer

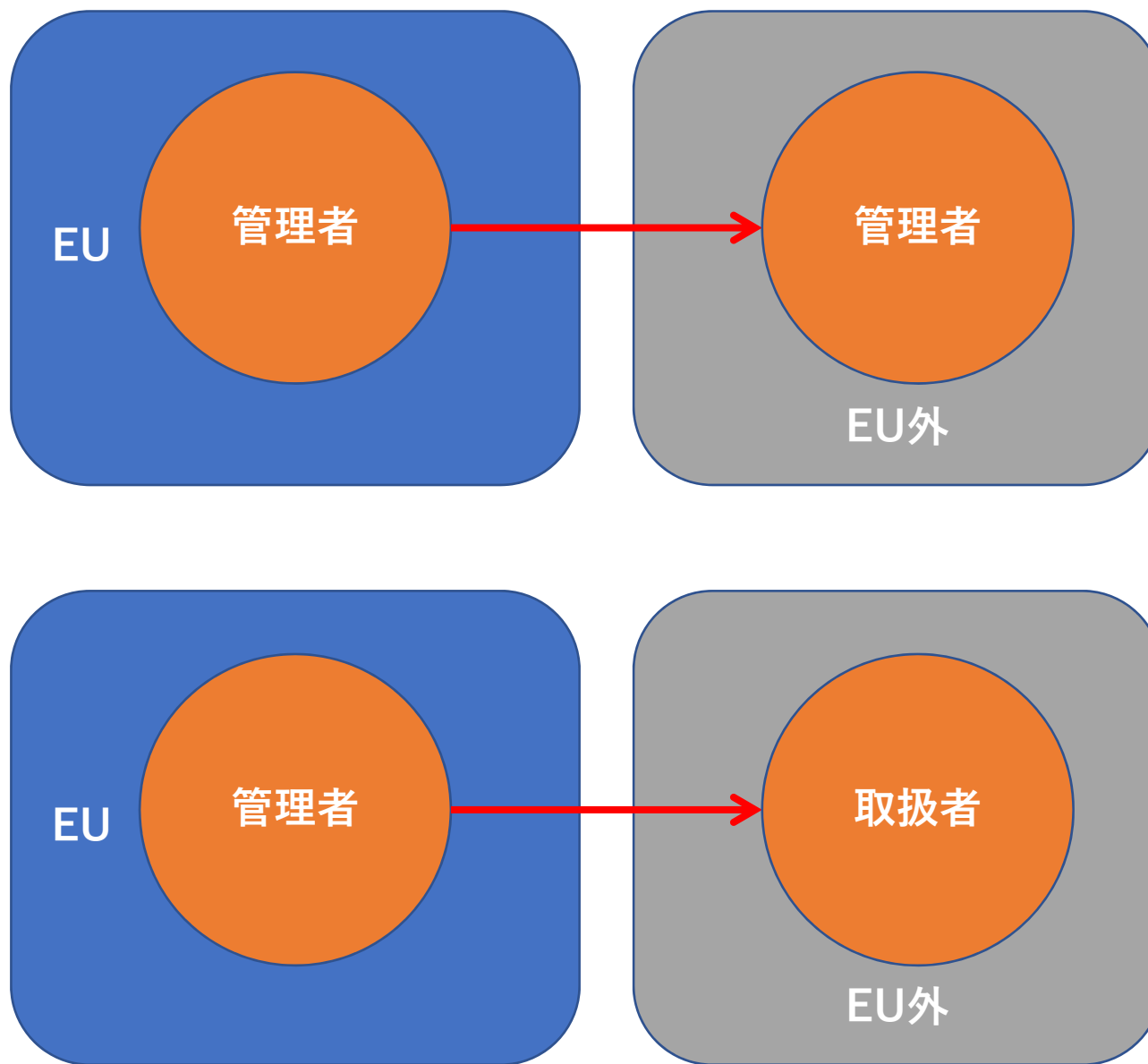
- 1. 管理者及び取扱者は、データ保護オフィサーが個人データ保護に関するすべての問題に、適切かつ直ちに関与できることを確実にしなければならない。
- 1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- 2. 管理者及び取扱者は、第39条で定める業務遂行においてデータ保護オフィサーを支援しなければならない。その支援は、当該業務の実行、個人データ及び取扱い作業へのアクセス、及びデータ保護オフィサーの専門知識を維持するのに必要な資源を提供することによってなされるものとする。
- 2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
- 3. 管理者又は処理者はデータ保護オフィサーがその業務の遂行に関してあらゆる指図を受けないことを確実にしなければならない。当該データ保護オフィサーは管理者又は取扱者によって当該データ保護オフィサーの業務遂行に関して解雇又は罰則を受けることがあってはならない。データ保護オフィサーは管理者又は取扱者の最高レベルの経営者に直接報告するものとする。
- 3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.
- 4. データ主体はデータ主体の個人データの取扱い及び本規則に基づく権利の履行に関するすべての問題に関してデータ保護オフィサーに連絡を取ることができる。
- 4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

- 5. データ保護オフィサーは、EU 法又は加盟国の国内法に従って、データ保護オフィサーの業務に関連した秘密又は機密を守らなければならない。
- 5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
- 6. データ保護オフィサーは他の業務又は義務を遂行することができる。管理者又は取扱者は当該業務及び義務が利益相反を招かないよう確保しなければならない。
- 6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.
- 「DPOは、個人データの処理の目的及び手段を決定する地位を有することはできない。たとえば、利益相反が問題となる地位として、経営陣（最高経営責任者、最高執行責任者、最高財務責任者、最高医療責任者、マーケティング部門長、人事部門長、IT部門長等）があげられるが、その他の組織構造の中で比較的低い地位であっても当該地位や役割が処理の目的および手段を決定することにつながる場合もあげられる。」（[杉本]）
- DPOネットワークの構築例（[柳池]）
 - ①集中型（本社主導型）
 - ②分散型（子会社主導型）
 - ③混成型（組み合わせ）

3 EUによる日本の十分性認定

3.1 GDPRにおける越境移転制限

- ①原則としての、十分性認定に基づく移転（GDPR45条）
- ②十分性認定がなされていない場合の、適切な安全性確保措置を施した移転（GDPR46条）
- ③十分性認定がなされておらず、適切な安全性確保措置も認められない場合の、特別の状況における特則（GDPR49条）



3.2 GDPRにおける十分性認定

- 十分性認定（判定）がなされたのは，
 - アンドラ，アルゼンチン，カナダ（民間部門），フェロー諸島，ガーンジー島，イスラエル，マン島，ジャージー島，ニュージーランド，スイス，ウルグアイ（7カ国4地域）
 - EU-USプライバシースールドスキーム
- 個人情報の保護に関する法律についてのガイドライン（E U域内から十分性認定により移転を受けた個人データの取扱い編）（案）（パブリックコメント中。～平成30年5月25日）
 - 「個人情報保護委員会は、日 E U間で相互の円滑な個人データ移転を図るため、法第 24 条に基づき、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として E Uを指定し、これにあわせて、欧州委員会は、G D P R第 45 条に基づき、日本が個人データについて十分な保護水準を確保していると決定した。」

第45条 十分性決定に基づく移転

Article 45 Transfers on the basis of an adequacy decision

- 1. 第三国又は国際機関への個人データの移転は、当該第三国、第三国域内の領域若しくは一つ若しくは複数分の特定のレベルを保証しているとの欧州委員会が決定した場合に行うことができる。この移転は、いかなる個別的許可も要しない。
- 1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

- 2. 保護レベルの十分性を評価するとき、欧州委員会は、次に掲げる要素を特に考慮しなくてはならない。
- 2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:
- (a) 法の支配、人権及び基本的自由の尊重、公安、国防、国家の安全及び刑事法並びに個人データへの公的機関のアクセスに関するものを含む一般的な又は分野別の関連法令及びその履行。第三国又は国際機関への個人データの再移転に関連し、当該第三国又は国際組織によって遵守される規定及び判例法並びに効果的かつ執行力のあるデータ主体の権利を含むデータ保護規定、専門的規定及び安全対策。個人データが移転されるデータ主体のための効果的な行政上及び司法上の是正措置。
- (a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

- (b) データ保護規定遵守の保障及び執行並びに適切な執行権限に対する責任、データ主体が権利を行使する際にこれを支援する又はこれに対し助言する責任、及び、加盟国の監督機関と協働する責任を有する第三国における一つ又は複数の独立した監督機関、又は国際機関が従うべき監督機関の存在及び実効的権限行使。
- (b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and
- (c) 当該第三国若しくは国際組織が加入している国際的取決め。特に個人データ保護に関する法的拘束力のある慣行若しくは法律文書から又は、多国間又は地域における制度への参加から生じるその他義務。
- (c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.
- 3.-9. (略)

Maximillian Schrems v Data Protection

Commissioner(C-362/14)

(interpretation of Directive Art.25-26)

- ...in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union
- ...the term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter.

the Charter of Fundamental Rights of the European Union

- ***Article 7***

- Respect for private and family life

- Everyone has the right to respect for his or her private and family life, home and communications.

- ***Article 8***

- Protection of personal data

- 1. Everyone has the right to the protection of personal data concerning him or her.
 - 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
 - 3. Compliance with these rules shall be subject to control by an independent authority

3.3 例外事由

- 適切な安全性確保措置
 - 監督機関の個別承認不要
 - 従来からの方法
 - 標準データ保護約款（GDPR46条2項(c)(d)）
 - 拘束的企業準則（BCR）（GDPR46条(b)）
 - GDPRでの新規導入
 - 行動準則（GDPR40条ないし41条）
 - 認証（GDPR42条ないし43条）
 - 監督機関の個別承認
 - 詳細はまだ不明
- 特別の状況における特例
 - 同意が含まれるが、「大量，構造的，反復的な移転には適用されない」との指摘

第46 条 適切な保護措置に従った移転

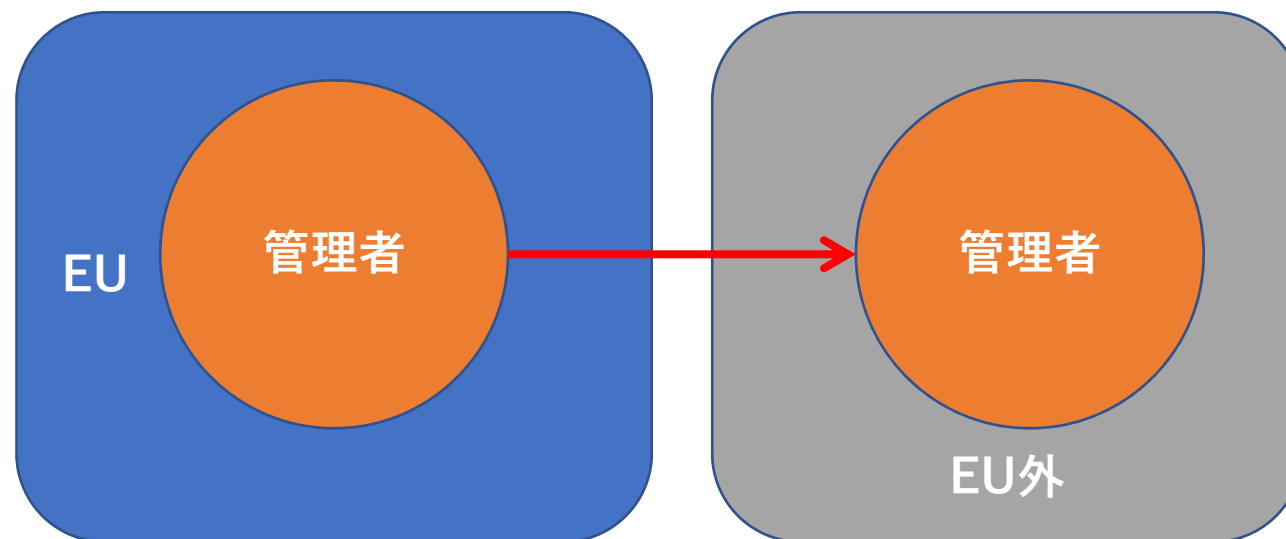
Article 46 Transfers subject to appropriate safeguards

- 1. 第45 条第3 項による決定がない場合は、管理者又は取扱者が適切な保護措置を提供しており、執行力あるデータ主体の権利及びデータ主体に関する効果的な法的救済が利用可能な状態である場合に限り、管理者又は取扱者は第三国又は国際機関に個人データを移転することができる。
- 1. In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.
- 2. 第1 項で定める適切な保護措置は、監督機関からの特定の認可を必要とせず、次に掲げるものによって講じられてもよい。

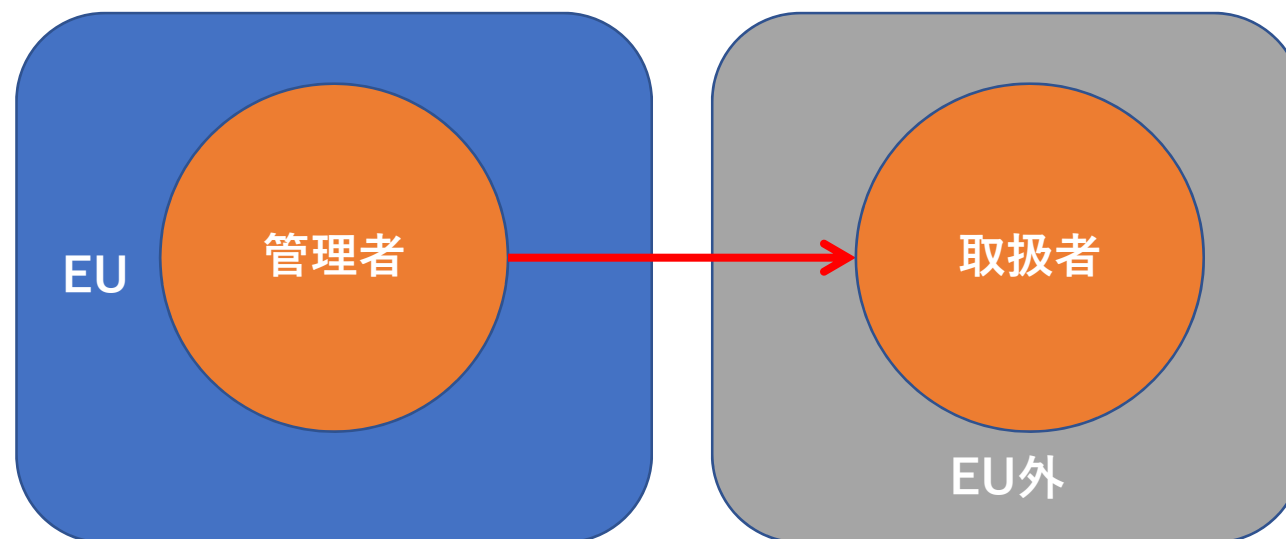
- 2. The appropriate safeguards referred to in paragraph 1 may be provided for, without requiring any specific authorisation from a supervisory authority, by:
 - (a) 公的機関又は団体間の法的拘束力又は執行力のある法律文書。
 - (a) a legally binding and enforceable instrument between public authorities or bodies;
 - (b) 第47 条に従った拘束的企業準則。
 - (b) binding corporate rules in accordance with Article 47;
 - (c) 第93 条第2 項で定める審査手続に従って欧州委員会によって採択された標準データ保護条項。
 - (c) standard data protection clauses adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);
 - (d) 監督機関によって採択され、第93 条第2 項で定める審査手続により欧州委員会によって承認された標準データ保護条項。
 - (d) standard data protection clauses adopted by a supervisory authority and approved by the
 - Commission pursuant to the examination procedure referred to in Article 93(2);

- (e) 適切な保護措置（データ主体の権利に関することを含む）を適用するための第三国の管理者又は取扱者の拘束力及び執行力のある公約を伴った、第40条による承認された行動規範。又は、
- (e) an approved code of conduct pursuant to Article 40 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- (f) 適切な保護措置（データ主体の権利に関することを含む）を適用するための第三国の管理者又は取扱者の拘束力及び執行力のある公約を伴った、第42条による承認された認証メカニズム。
- (f) an approved certification mechanism pursuant to Article 42 together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
- 従来のSCCは経過措置によってGDPRにおいても有効。

管理者-管理者
SCC

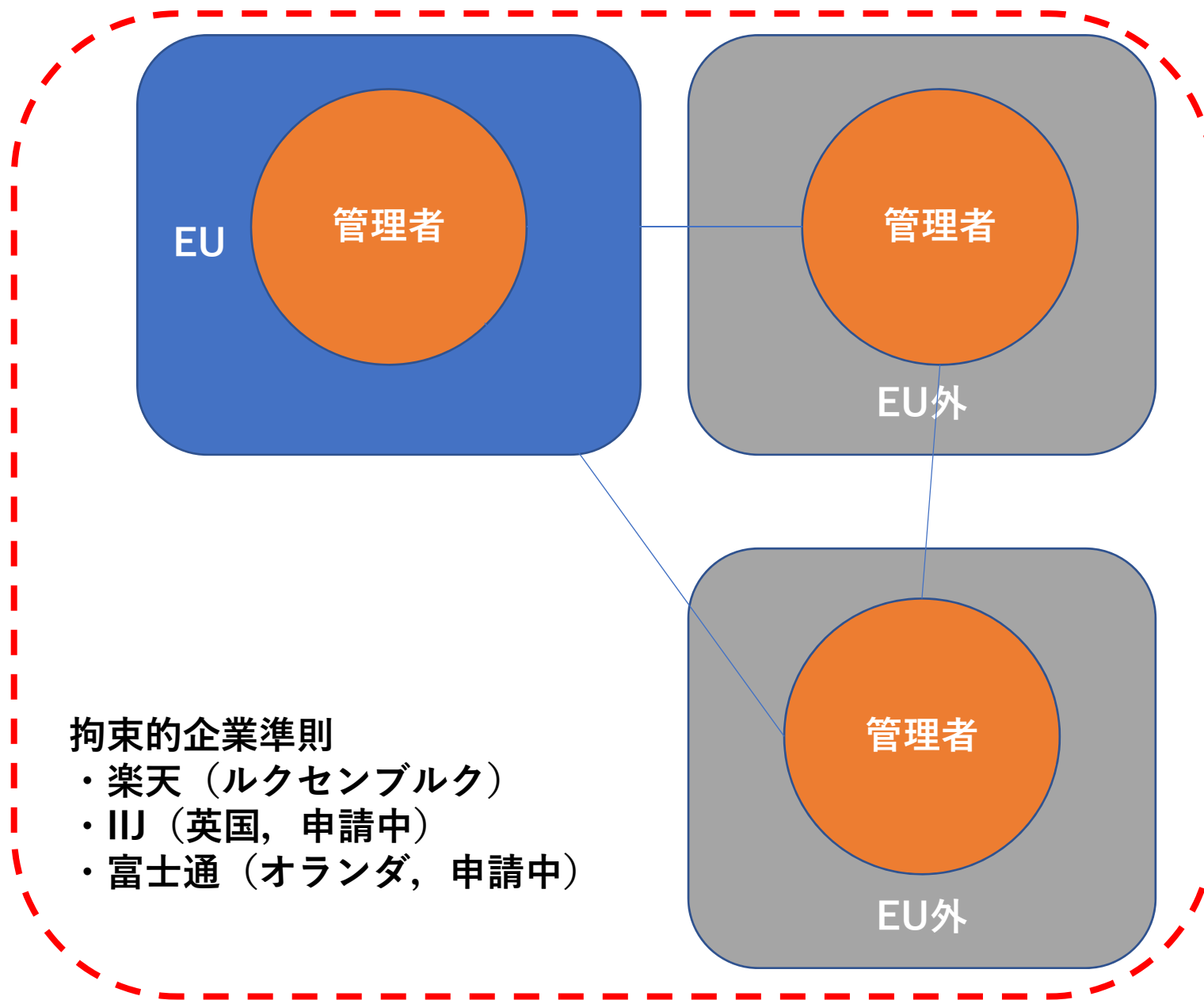


管理者-処理者
SCC



SCCの法遵守義務及び準拠法

- 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)
- **II. Obligations of the data importer**
- 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 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, or
- iii. the data processing principles set forth in Annex A.
- Data importer to indicate which option it selects:
- Initials of data importer: ;
- **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.



4 「個人情報保護に関する法律についてのガイドライン（E U域内から十分性認定により移転を受けた個人データの取扱い編）」（案）

4.1 経緯

- 個人情報保護委員会は、日EU間の個人データの移転について、相互の円滑な移転を図る枠組みの構築を視野に、欧州委員会との間で累次の対話を重ねてきている。
- 昨年（2017年）12月14日には、当委員会委員と欧州委員会委員との間で会談を行い、**双方の制度間の関連する相違点に対処するための、法令改正を行わない形で解決策について確認する**とともに、今後、その詳細について作業すること、また、本年前半に、最終合意することを想定し、委員レベルで会談をもつことで一致した。
- この解決策として、本年（2018年）2月14日に、「個人情報保護に関する法律についてのガイドライン（E U域内から十分性認定により移転を受けた個人データの取扱い編）」について、当委員会で審議を行った。
- 当該ガイドラインは、**各国政府との協力の実施等に関する個人情報保護法上の規定等（個人情報保護法第4条、第6条、第8条、第24条、第60条及び第78条、並びに本年5月9日に公布・施行予定の改正後の個人情報保護法施行規則第11条）**に基づき、欧州委員会から日本への十分性が認められた際、E U域内から十分性認定により移転を受ける個人データの取扱いに関して最低限遵守すべき規律を示すものである。

4.2 ガイドラインの位置付け

- 個人情報保護委員会は、日EU間で相互の円滑な個人データ移転を図るため、法第24条に基づき、個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国としてEUを指定し、これにあわせて、欧州委員会は、GDPR第45条に基づき、日本が個人データについて十分な保護水準を確保していると決定した。
- たU相定るよ務るンしEる認すに義すイ保護日す性保定な関ラ保。連分確認効にド保。関十を性有等イ準なのら護分つ施ガ水とかか保十か実本いとつ内のら切のは高こく域準か適力会をるいU水内び協員益れ、Eい域及の委利らの、高Uいと護利図のてE扱府保権がもしいる取政報の転るらつよな国情人移い照にに切各個人タてに報者適、個で、一し実情業のらき人間類う個扱情点基U個ていた取人観にEなめとけ報個る日滑極る受情たす1、円はすを人け保※りの度存転個受確た。に相のがりに転行規定よ互制存移、をを定しこれで方点よめ移履の策こ上双違にたりの法を

- 個人情報保護委員会による執行に関しては、個人情報取扱事業者が本個を有する。一般的に、EU域内から十分に認定により移転を受けた個人情報について、法第42条第1項の規定による勧告を受けた個人情報取扱事業者が正当な理由（※2）がなくその勧告に係る措置をとらなかった場合は、法第42条第2項に定める「個人の権利利益の重大な侵害が切迫している」と認められる。
- （※1）法第4条、第6条、第8条、第24条、第60条及び第78条、並びに規則第11条
- （※2）正当な理由とは、個人情報取扱事業者にとって合理的に予測可能な場合や、個人情報が取扱い事業者が違反を完全に是正する個人情報が失われた場合が考えられる。
- ※「EU」 欧州連合加盟国及び欧州経済領域（EEA: European Economic Area）協定に基づきアイスランド、リヒテンシュタイン及びノルウェーを含む、欧州連合（European Union）

個人情報保護法6条

- 政府は、個人情報の性質及び利用方法に鑑み、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるとともに、国際機関その他の国際的な枠組みへの協力を通じて、各国政府と共同して国際的に整合のとれた個人情報に係る制度を構築するために必要な措置を講ずるものとする。

4.3 ガイドラインの内容

- (1) 要配慮個人情報（法第2条第3項関係）
- (2) 保有個人データ（法第2条第7項関係）
- (3) 利用目的の特定、利用目的による制限（法第15条第1項・法第16条第1項・法第26条第1項・第3項関係）
- (4) 外国にある第三者への提供の制限（法第24条・規則第11条の2関係）
- (5) 匿名加工情報（法第2条第9項・法第36条第1項第2項関係）

(1) 要配慮個人情報（法第2条第3項関係）

- E U域内から十分性認定に基づき提供を受けた個人データに、GDPRにおいて特別な種類の個人データと定義されている性生活、性的指向又は労働組合に関する情報が含まれる場合には、個人情報取扱事業者は、当該情報について法第2条第3項における要配慮個人情報と同様に取り扱うこととする。

「性生活、性的指向又は労働組合に関する情報」の執行は？

- 取得規制
 - （適正な取得）
 - 第17条 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。
 - 2 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
 - （各号略）
- 提供規制（取得側の規制で執行することが考えられる？）
 - 23条2項 個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
 - 一 第三者への提供を利用目的とすること。
 - 二 第三者に提供される個人データの項目
 - 三 第三者への提供の方法
 - 四 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
 - 五 本人の求めを受け付ける方法

(2) 保有個人データ（法第2条第7項関係）

- 個人情報取扱事業者が、E U域内から十分性認定に基づき提供を受けた個人データについては、消去することとしている期間にかかわらず、法第2条第7項における保有個人データとして取り扱うこととする。なお、E U域内から十分性認定に基づき提供を受けた個人データであっても、「その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの」は、「保有個人データ」から除かれる（政令第4条、通則ガイドライン「2-7 保有個人データ」参照）。

6ヶ月要件を満たさない個人データについての開示等の請求等？

- （個人情報取扱事業者による苦情の処理）
- 第35条 個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。
- 2 個人情報取扱事業者は、前項の目的を達成するために必要な体制の整備に努めなければならない。

(3) 利用目的の特定、利用目的による制限（法第15条第1項・法第16条第1項・法第26条第1項・第3項関係）

- 個人情報取扱事業者は、法第15条第1項により特定した利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならず（法第16条第1項）、また、第三者から個人データの提供を受ける際は、規則で定めるところにより、当該第三者に当該個人データの取得の経緯等を確認し、記録しなければならないこととなっている（法第26条第1項・第3項）。
- 個人情報取扱事業者が、EU域内から充分性認定に基づき個人データの提供を受ける場合、法第26条第1項及び第3項の規定に基づき、EU域内から当該個人データの提供を受ける際に特定された利用目的を含め、その取得の経緯を確認し、記録することとする。
- 同様に、個人情報取扱事業者が、EU域内から充分性認定に基づき個人データの提供を受けた他の個人情報取扱事業者から、当該個人データの提供を受ける場合、法第26条第1項及び第3項の規定に基づき、当該個人データの提供を受ける際に特定された利用目的を含め、その取得の経緯を確認し、記録することとする。
- 上記のいずれの場合においても、個人情報取扱事業者は、法第26条第1項及び第3項の規定に基づき確認し、記録した当該個人データを当初又はその後提供を受ける際に特定された利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用することとする（法第15条第1項、法第16条第1項）。

(4) 外国にある第三者への提供の制限（法第 24 条・規則第 11 条の 2 関係）

- 個人情報取扱事業者は、~~E U 域内から十分性認定に基づき提供を受けた個人データを外国にある第三者へ提供するに当たっては、法第 24 条に従い、次の①から③までのいずれかに該当する場合を除き、[本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で]、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得ることとする。~~
 - ① 当該第三者が、個人の権利利益の保護に関して、我が国と同等の水準にあると認められる個人情報保護制度を有している国として規則で定める国にある場合
 - ② 個人情報取扱事業者と個人データの提供を受ける第三者との間で、当該第三者による個人データの取扱いについて、適切かつ合理的な方法（契約、その他の形式の拘束力のある取決め又は企業グループにおける拘束力のある取扱い）により、本ガイドラインを含め法と同等水準の個人情報の保護に関する措置を連携して実施している場合
 - ③ 法第 23 条第 1 項各号に該当する場合

(5) 匿名加工情報（法第2条第9項・法第36条第1項第2項関係）

- EU域内から十分性認定に基づき提供を受けた個人情報については、個人情報取扱事業者が、加工方法等情報（匿名加工情報の作成に用いた個人情報から削除した記述等及び個人識別符号並びに法第36条第1項の規定により行った加工の方法に関する情報（その情報を用いて当該個人情報を復元することができるものに限る。）をいう。）を削除することにより、匿名化された個人を再識別することを何人にとっても不可能とした場合に限り、法第2条第9項に定める匿名加工情報とみなすこととする。

裁判例におけるガイドラインの取扱い

- 福岡地久留米支部判平成26年8月8日判時2239号88頁
 - …上記「第三者」に当たるか否かは外形的に判断されるべきであって、ある情報を保有する個人情報取扱事業者（法2条3項）及び当該情報の主体である本人（同条6項）以外の者を意味するといふべきである（なお、個人情報ガイドラインにおいても、同一事業者内で情報提供する場合に当該個人データを第三者に提供したことはないこととされている（乙口1・26頁））…
- 東京地判平成26年1月23日判時2221号71頁
 - 証拠（甲24の1・2、甲25）によれば、厚生労働省及び経済産業省が平成19年3月30日に改正した「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（同日厚生労働省・経済産業省告示第1号）では、クレジットカード情報等（クレジットカード情報を含む個人情報）について特に講じることが望ましい安全管理措置として、利用目的の達成に必要な最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄することを例示し、IPAは、同年4月、前記「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、データベース内格納され、重要なデータや個人情報については暗号化することが望ましいと明示していたことが認められる。しかし、上記告示等は、いずれも上記対策を講じることが「望ましい」と指摘するものにすぎないし、上記IPAの文書においては、データベース内データの暗号化は暗号化の処理を行うと、サーバー自体の負荷になること（甲25）のよう、特定データの暗号化の程度によって異なるため、それによって被る作業量や代金も増減するとの考慮がなされ、契約で特別に合意していなくとも、当然に、被告がクレジットカード情報を本件サーバー及びログに保存せず、若しくは保存しても削除する設定とし、又はクレジットカード情報を暗号化して保存すべき債務を負っていたとは認められない。

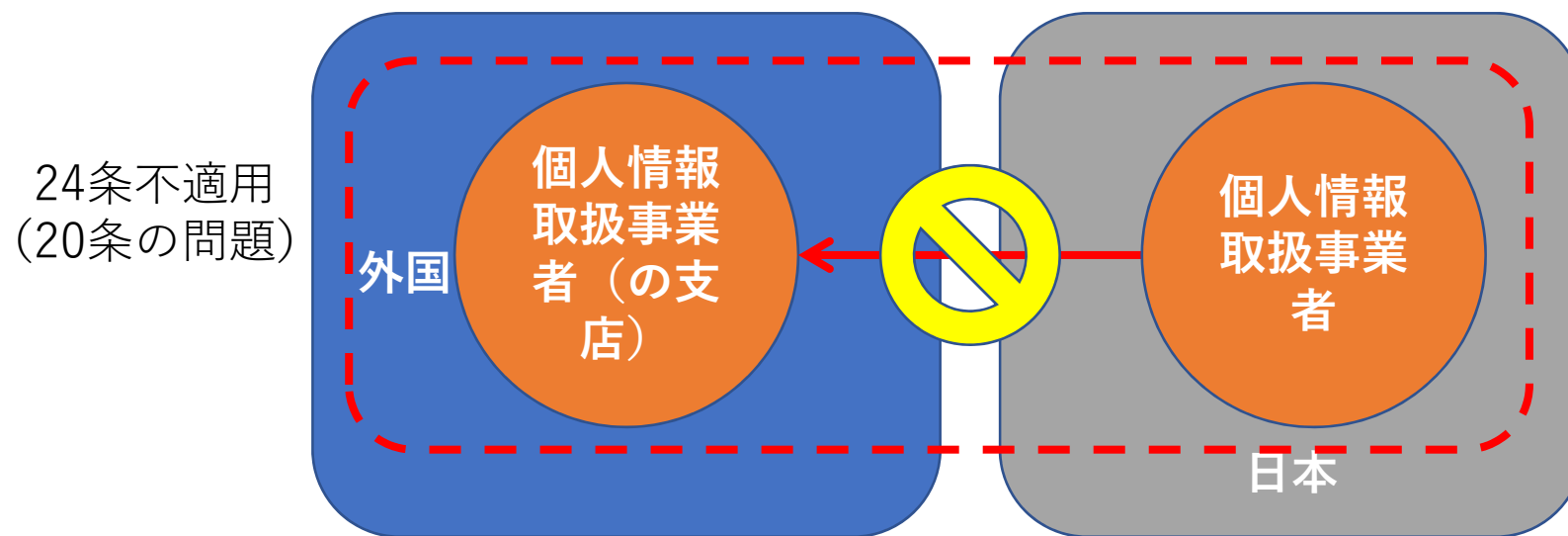
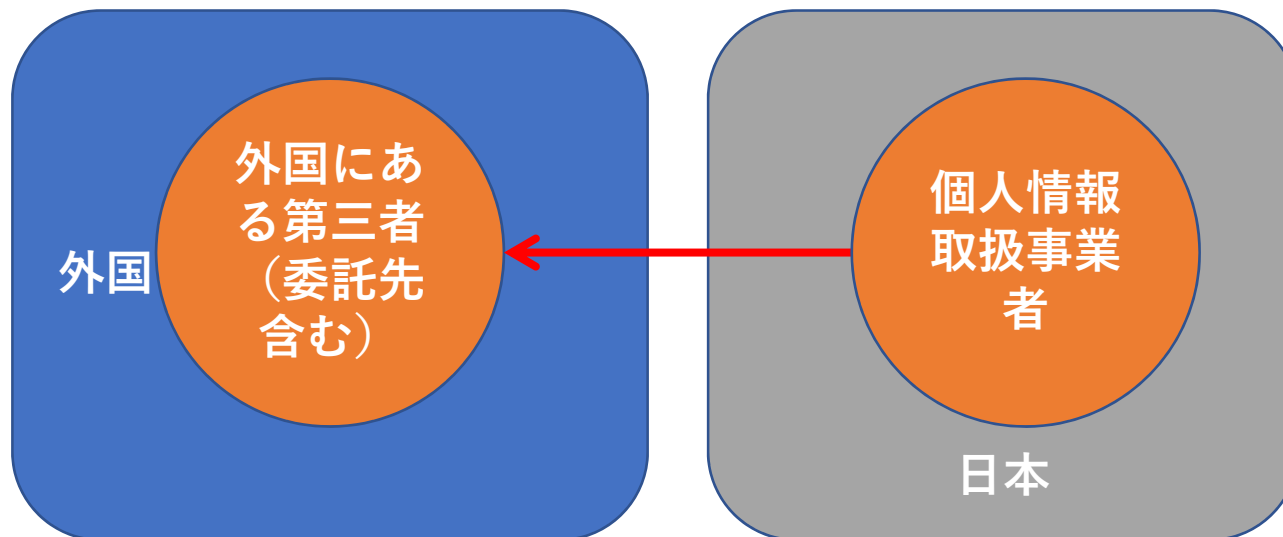
4.4 今後の展望

- 平成30年5月25日までパブリックコメント
- 公布・施行期日「本年前半を予定。」
 - European Data Protection Board, European Commissionの決定を経て…
 - 平成30年6月30日までに公布・施行か？

5 日本によるEUの同等性認定

5.1 個人情報保護法24条

- 個のう。人。情。報。取。扱。事。業。者。は。外。国。の。本。邦。の。域。外。に。あ。る。国。又。は。地。域。を。い。等。て。以。に。と。も。を。一。か。を。用。
 情。以。準。に。国。条。こ。い。て。て。供。じ。れ。
 取。同。あ。と。に。の。る。個。い。す。め。ば。
 扱。じ。る。し。お。節。措。人。る。る。外。な。
 事。と。て。い。の。置。情。者。場。国。ら。
 業。認。個。て。規。に。報。を。合。に。な。
 者。め。人。同。定。相。保。除。に。あ。い。
 は。個。人。情。報。に。当。護。く。は。る。
 外。の。保。護。に。個。措。会。下。条。者。場。
 国。権。個。護。に。個。措。会。下。条。者。場。
 本。利。情。員。る。情。を。則。の。一。の。に。
 邦。益。報。会。第。報。継。で。条。項。提。お。
 の。を。の。規。三。取。続。定。に。各。供。い。
 域。保。保。則。者。扱。的。め。お。号。を。て。
 外。護。護。で。事。に。る。い。に。認。は。
 に。す。に。定。個。業。講。基。て。掲。め。
 あ。る。関。め。人。者。す。準。同。げ。る。同。
 る。上。す。る。デ。が。る。に。じ。る。旨。条。
 国。で。る。も。一。講。た。適。場。の。の。
 又。我。制。の。タ。ず。め。合。合。本。規。
 は。が。度。を。の。べ。に。す。に。を。人。定。
 地。国。を。除。取。き。必。る。個。除。の。は。
 域。と。有。く。扱。こ。要。体。人。く。同。
 を。同。し。い。と。な。制。デ。は。意。適。
 い。等。て。以。に。と。も。を。一。か。を。用。



5.2 「個人情報保護に関する法律施行規則の一部を改正する規則」

- ○個人情報保護委員会規則第1号
- 個人情報保護に関する法律施行規則（平成28年個人情報保護委員会規則第3号）の一部を改正する規則を次のように定める。
- **平成30年5月9日**
- 個人情報保護委員会委員長 堀部政男
- 個人情報の保護に関する法律施行規則の一部を改正する規則
- 個人情報の保護に関する法律施行規則の一部を次のように改正する。
- 第11条を第11条の2とし、第10条の次に次の1条を加える。

新第11条（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報保護に関する制度を有している外国）

- 法第24条の規定による個人情報保護に関する制度を有している外国として個人情報保護委員会規則で定めるものは、次の各号のいずれにも該当する外国として個人情報保護委員会が定めるものとする。
- 一 法における個人情報取扱事業者に関する規定に相当する法令その他の定めがあり、その履行が当該外国内において確保されていると認めるに足りる状況にあること
- 二 個人情報保護委員会に相当する独立した外国執行当局が存在しており、かつ、当該外国執行当局において必要かつ適切な監督を行うための体制が確保されていること
- 三 我が国との間において、個人情報の適正かつ効果的な活用と個人の権利利益の保護に関する相互理解に基づく連携及び協力が可能であると認められるものであること
- 四 個人情報の保護のために必要な範囲を超えて国際的な個人データの移転を制限することなく、かつ、我が国との間において、個人情報の保護を図りつつ、相互に円滑な個人データの移転を図ることが可能であると認められるものであること
- 五 前四号に定めるもののほか、当該外国を法第24条の規定による外国として定めることが、我が国における新たな産業の創出並びに活力ある経済社会及び豊かな国民生活の実現に資すると認められるものであること

- 2 個人情報保護委員会は、前項の規定による外国を定める場合において、我が国における個人の権利利益を保護するため、必要があるときは、当該外国にある第三者への提供を認める旨の本人の同意を得ることなく提供できる個人データの範囲を制限することその他の必要な条件を付することができる。
- 3 個人情報保護委員会は、第一項の規定による外国を定めた場合において、当該外国が第一項各号に該当し付ていた条と又が満たさきは、当該外国に係る対応の状況に保護に關する調査を行うものとする。
- 4 個人情報保護委員会は、第一項の規定による外国を定めた場合において、前項の調査の結果その他の状況を踏まえ、当該外国が第一項各号に該当しなくなったと認めるとき又は当該外国について第二項の規定により付された条件が満たされなくなったと認めるときは、第一項の規定による定めを取り消すものとする。

5.3 パブリックコメントにおける意見等

- 「個人情報保護委員会が定めるもの」について、当該事由を定める方法（例：貴委員会規則の制定又は改定、告示又は通知の発出、貴委員会 HP での告知など）をご教示されたい。【番号1】
 - 本規則案に適合すると認められる具体的な外国の名称については、告示で定めて当委員会 HP に掲載することを予定しています。
- 海外各国が同条項各号事由を満たすか否かについて、貴委員会が主体となって審査すると思われる。この審査は、どのような形式で実施する予定かご教示されたい。例えば、有識者による検討会（各省庁が行っているような審議会形式、審議会とは別の貴事務局直轄の検討会形式など）が想定されると思われる。また、当該検討会において、議事や資料の公開を行うか否かもご教示されたい。
【番号1】
 - ある外国が本規則案に適合するか否かについては、当委員会において審議の上決定し、資料及び議事録・議事概要は公表する予定です。
- 今回意見募集されている個人情報保護委員会規則改正案に係る個人情報保護法24 条に基づく外国の指定は、EU のデータ保護指令および一般データ保護規則に規定されている「充分性認定」に対応する措置と見受けられます。そこで、今回意見募集されている、指定対象の外国の要件や指定にあたる条件に加えて、前述の一般データ保護規則に規定されているようなレビュー条項（同規則 45 条 3 項・4 項）や認定取消条項（同規則 45 条 5 項）も規定されるべきと考えます。【番号16】
 - 御意見を踏まえ、レビューや取消に係る条項の追加について検討します。

- 「個人情報の保護に関する法律についてのガイドライン（E U域内から充分性認定により移転を受けた個人データの取扱い編）」（案）
 - 平成30年5月25日までパブリックコメント，本年前半（平成30年6月30日までに公布・施行）
 - 公布時までに「G D P R第 45 条に基づき、日本が個人データについて十分な保護水準を確保していると決定した」。
- 日本によるEUの同等性認定
 - 「個人情報の保護に関する法律施行規則の一部を改正する規則」が平成30年5月9日に公布・施行
 - 個人情報保護委員会の審議を経て，EUが告示により指定

6. 関連する話題

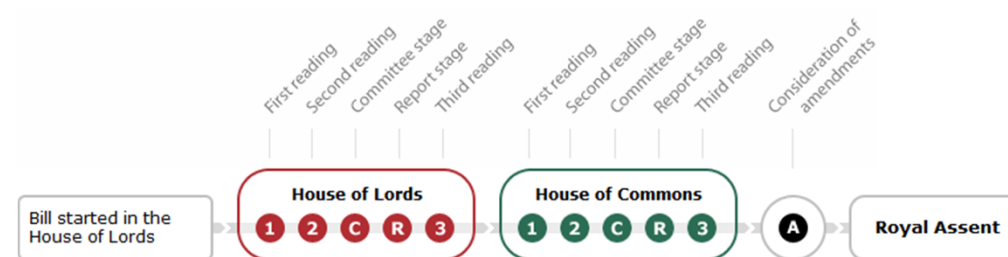
6.1 BREXITのGDPRへの影響

- 2018年5月25日 GDPR適用
- 2019年3月まで BREXITに伴う英国の対応
- BREXITを踏まえた新法案が議論されている

Data Protection Bill [HL] 2017-19

Type of Bill: Government Bill
Sponsors: Lord Ashton of Hyde
Department for Digital, Culture, Media and Sport
Matt Hancock
Department for Digital, Culture, Media and Sport

Progress of the Bill



Last events

- R** Report stage: House of Commons 9 May, 2018 | 09.05.2018
- 3** 3rd reading: House of Commons 9 May, 2018 | 09.05.2018

Next event

- Ping Pong** | 14.05.2018

2018/05/19

■ [Read debates on all stages of the Data Protection Bill \[HL\] 2017-19](#)

6.2 e-プライバシー規則案における規律

DEPARTURE DEMAND DEPARTURES EXPECTED ARRIVALS ON HOLD ARRIVED DERAILED

DEPARTURES

20

CONSUMER SALE OF GOODS

DIGITAL CONTENT AND DIGITAL SERVICES

SG ACTION PLAN

BEREC

ELECTRONIC COMMUNICATIONS CODE

LEGISLATIVE TRAIN SCHEDULE
CONNECTED DIGITAL SINGLE MARKET

PROPOSAL FOR A REGULATION ON PRIVACY AND ELECTRONIC COMMUNICATIONS

DEPARTURES 201509

I Departed

Strengthening online users' trust is necessary for the development of a digital single market. This includes ensuring a high level of privacy and personal data protection.

A Proposal for a Regulation on the respect for private life and the protection of personal data in electronic communications has been published the 10 January 2017 in order to update the existing 2002 legislation. Other measures include a regulation on data processing by the Union institutions (see file on data protection in EU institutions). The intention is to provide citizens, companies (and institutions) with a complete and consistent legal framework.

- Among the changes introduced with the reform, the proposal now includes in its scope other market-players using the internet (e.g. OTTs), with the aim of ensuring a level playing field for companies. The objectives of the review include:
 - Enhancing security and confidentiality of communications, while reducing unjustified barriers to the free flow of data.
 - Defining better and clearer rules on tracking technologies such as cookies.
 - Addressing fragmentation of legislation across Europe.
 - Consistent enforcement of e-Privacy rules by independent supervisory authorities already competent to enforce the GDPR.

- Although the file is among the priorities of the Bulgarian Presidency, discussions seem still to be required within the Council. Trilogues did not start yet but are expected to start during the current semester. Issues under analysis regard in particular the grounds for data processing, other than consent, as well as the applicability of the new provisions to service providers assisting competent authorities for national security purposes or the concept of public interests grounds justifying restrictive measures. A revised text by the Council has been debated in March 2018 within its working party configuration (TELE), with clarifications on some aspects like the link with the GDPR, the consent requirement, the applicability to ancillary services and to machine-to-machine communications. The Council Presidency has proposed a new revised text in April. In particular, discussions seem focused on how the new rules should apply to communications content and to meta-data (Permitted processing of communications data, Art 6), to the protection of the terminal equipment (Art 8), on privacy settings (Art 10) as well as on restrictions to obligations and rights (Art 11). A General Approach is not expected before summer.
- Therefore, the proposed date of 25 May 2018 for the entry into force of the new regulation seem difficult to achieve.

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) - Examination of the Presidency text
Brussels, 13 April 2018(OR. en)

- *Article 6*
- *Permitted processing of electronic communications data*
- *Article 8*
- *Protection of **end-users' terminal equipment** information ~~stored in terminal equipment of end-users and related to or processed by or emitted by end-users' terminal such equipment~~*
- *Article 16*
- *Unsolicited and ~~D~~direct marketing communications*

7 まとめ

- GDPRが適用されるのは
 - 域外適用の場合
 - 標準データ保護約款，BCRで移転する場合（契約上の義務）
 - ※十分性認定による移転の場合は日本側のガイドライン
- 適用される場合
 - GDPR上の権利，義務にフルセットで対応する必要
 - 課徴金の可能性も否定できない
 - 2017年になってから，GDPRを睨んで？日本企業にICOが執行した例
 - しかし，執行リソースは限られている