

# Deloitte.

デロイト トーマツ



## GDPR (EU一般データ保護規則) の実務対応

デロイト トーマツ リスクサービス株式会社  
2019年2月24日

Making another half century of **Impact**  
デロイト トーマツ 50周年 次の50年へ

**50**<sup>th</sup>  
Deloitte Tohmatsu

# 目次

---

EU一般データ保護規則	3
説明責任	17
域外移転規制	21
遵守するための対策の実施	25
データセキュリティに関する義務	29
データ主体の権利	31

---

# EU一般データ保護規則

# 1995年以降、EUデータ保護指令が適用されてきました

## EUデータ保護指令

法令の名称	EUデータ保護指令 / EU Data Protection Directive	
概要	<ul style="list-style-type: none"><li>① 一元的な基本法。加盟国は、EUデータ保護指令に基づいて国内法を定める義務を負っています。</li><li>② 加盟国に第三者機関が存在し、立ち入り調査権を含む、強い権限を持っています。</li><li>③ 個人情報の取扱いに対する自然人の基本的権利及び自由、特にデータ保護が目的です。 適用対象は、加盟国ですが、域外の第三国への個人情報の移転を規制しています。</li></ul>	
データ主体の権利	<ul style="list-style-type: none"><li>✓ 情報提供を受ける権利(10条、11条)</li><li>✓ アクセス権(12条)</li><li>✓ 訂正・削除権(12条(b)号)</li><li>✓ 異議申立権(14条)</li><li>✓ 自動化された個人の判断に関する権利(15条) 等</li></ul>	
管理者及び処理者の義務	<ul style="list-style-type: none"><li>✓ 処理の安全性に関する規定(17条)</li><li>✓ 管理者の名称や処理の目的等を監督機関へ通知する義務(18条、19条)</li></ul>	
域外移転	原則	域外移転時の制約(第25条)が定められています。 「十分なレベル」※の保護措置を確保している場合には、域外移転が可能とされています。
	例外	域外移転時の例外(第26条)が定められています。 明確な同意の取得、拘束的企業準則(BCR)や標準契約(SCC)などがあります。

※：「十分なレベル」にあるとしてEUから認定を受けている国々は以下のとおりです。認定を受けていない国にデータを移転するには第26条に基づいた対応が必要です。  
スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージー島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド

# EUデータ保護指令では、加盟国により保護水準に差が生じていました

## 規則化の背景と理由

- 法制度に起因する課題に加えてインターネットをはじめとする急速な技術的進歩や グローバル化の進展に伴い、個人データ保護に関する課題が多く生じていました。

1	新技術への対応	組織が新しく導入した技術を用いて個人データを処理するようになっており、データ保護諸原則を新技術に対応したものとすることが求められていました。
2	グローバル化への対応と越境流通の改善	EU域外への越境移転が増加しているが、多くの組織は現在の枠組みを完全に充足しているわけではないため、組織の負担を軽減した、合理的な方法を検討することが求められていました。
3	EU域内市場の安定化・活性化	EUデータ保護指令があるにも関わらず、加盟国間でのデータ保護法制の調和が取れていないため、組織の経済的負担を軽減するとともに、法的安定性を確保した市場の形成が求められていました。
4	効果的な執行に向けた強力な制度設計の提供	データ保護機関に対して、EUデータ保護指令の実効性を確保するためにも、透明性を確保した上で、権限と任務を明確化し効率的な執行が求められていました。
5	法的枠組みの統一性向上	全てのデータ処理に適用される包括的な枠組みが求められていました。

出所：COM(2010) 609 final<[http://ec.europa.eu/justice/news/consulting\\_public/0006/com\\_2010\\_609\\_en.pdf](http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf)>

# 「規則」は、EU域内の全加盟国に直接適用されます

## EU法制の枠組み

種類	概要
規則 (Regulation)	すべての加盟国を拘束し、直接適用性(採択されると加盟国内の批准手続を経ずに、そのまま国内法体系の一部となる)を有する。
指令 (Directive)	指令の中で命じられた結果についてのみ、加盟国を拘束し、それを達成するための手段と方法は加盟国に任される。指令の国内法制化は、既存の法律がない場合には、新たに国内法を制定、追加、修正することでなされる。 一方、加盟国の法の範囲内で、指令内容を達成できる場合には、措置を執る必要はない。加盟国の既存の法体系に適合した法制定が可能になる反面、規則に比べて履行確保が複雑・困難になる。
決定 (Decision)	特定の加盟国、企業、個人を対象を限定し、限定された対象に対しては直接に効力を有する。一般的法規というよりは、個別かつ具体的内容を有する。
勧告・意見 (Recommendation/Opinion)	EU理事会および欧州議会が行う見解表明で、通常は欧州委員会が原案を提案するもので、(1)～(3)とは異なり法的拘束力を持たない。

# EU一般データ保護規則(GDPR)は、全11章から構成されています

## EU一般データ保護規則の構成

章	タイトル	概要
第1章	一般条項	規則の概要を示した上、適用範囲や用語の定義を規定している。
第2章	原則	個人データ処理に関する原則を規定している。
第3章	データ主体の権利	データ主体が有する権利を規定している。
第4章	管理者と処理者	管理者及び処理者が負う義務を規定している。
第5章	第三国又は国際機関への個人データの移転	いわゆる域外移転に関する規制を規定している。
第6章	独立監督機関	データ保護の権利と自由を保護し、個人データの自由な流通を促進するための機関の設置を規定している。
第7章	連携と一貫性	監督機関の間での連携、管理者及び処理者への対応の一貫性を確保することが規定されている。
第8章	救済、法的責任及び罰則	侵害発生時のデータ主体の救済、管理者及び処理者への罰則が規定されている。
第9章	特定の処理状況における条項	個人データ保護と表現の自由、情報の自由との関係について規定している。
第10章	委任法及び施行法	施行に関する事項を規定している。
第11章	最終規定	

# 義務の主体、データ種別、操作の観点から用語が定義されています

## 定義

義務の主体	管理者 (Controller)	単独若しくは合同で個人データ処理の目的と手段を決定する者。
	処理者 (Processor)	管理者に代わり、個人データ処理を行う者。
データ種別	個人データ (Personal Data)	識別された又は識別可能な自然人に関連する全ての情報。
	特別なデータ (Special Category of Data)	人種・民族的出自、政治的見解、宗教又は哲学的信念、労働組合の組合員たる地位、遺伝データ、生体データ、健康又は性生活及び性的嗜好を現す個人データ。
操作	処理 (Processing)	自動的手段で行なわれるか否かに関わらず、個人データに対して行なわれる全ての操作又は組単位の操作。
	プロファイリング (Profiling)	自然人に関連する特定の個人的側面を評価するため、特に当該自然人の職務遂行、経済的状況、健康、個人的嗜好、趣味、信頼性、態度、所在地又は行動に関する特定の個人的な側面を評価するための当該個人データの使用により構成される個人データの自動処理のあらゆる形態。



# 様々なデータが個人データとして規定されています

## GDPRにおける個人データ(例)

### 個人データ(特定の個人を識別することができるもの)

- コンタクト情報(氏名、住所、生年月日、連絡先、所属情報)
- ID情報(身分証明番号)
- 金融情報(クレジットカード情報、収入、借金金額)
- 位置データ(位置や移動に係る情報)
- コンピュータ情報  
(本人がアクセスしている端末のIPアドレス、Cookie)
- 嗜好データ(購買データ、飲食の好み等)
- 考課データ(評価や成績に関する情報)
- 画像データ(本人が識別できる映像情報)
- 雇用管理情報(従業員や採用応募者、退職者などに関する情報)

### 特別なカテゴリーのデータ(取扱いに特に配慮を要するもの)

- 人種、民族的出自、社会的身分(国籍や本籍の都道府県名のみ場合は除く)
- 宗教的または哲学的信念
- 労働組合への加盟、組合員たる地位
- 性生活に関するデータ
- 健康に関するデータ(精神疾患やアレルギー性疾患などの病歴、手術歴、健康診断結果等)
- 遺伝データ(個人の遺伝的特性に関するデータ等)
- 生体データ(顔認証、指紋認証、静脈認証等のデータ)

# 特定の場合にはEU域外であっても適用対象とされることがあります

## 域外適用

当社がEU域外であっても次の1～4に該当する場合はGDPRが適用されます

1

### EU域内に子会社が設立されている場合

- EU域内の子会社は、GDPRが直接適用されるため、GDPRに基づいた個人データの処理が求められます。

2

### EU域内で個人データを収集し、日本で処理を行っている場合

- Cookieなどを収集し、日本で処理している場合には、GDPRにおいて「行動の監視」(monitoring)に該当するため、GDPRに基づいた個人データの処理が求められます。

3

### EU域内に業務遂行に必要な機器がある場合

- 個人データを保存するサーバなど、業務遂行に必要な機器がEU域内にある場合には、GDPRに基づいた個人データの処理が求められます。

4

### EU域内へ日本から直接、商品やサービスを提供している場合







- EU域内の個人も対象として商品・サービスを提供するためWebサイトを設けており、日本から直接、商品・サービスを提供している場合には、GDPRに基づいた個人データの処理が求められます。

出所: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

# 個人情報処理にあたって「適法」となる要件が定められています

## 「適法な処理」のための根拠

### 「適法な処理」のための根拠(GDPR第6条第1項)

	本人の同意	(a) 本人が1つ以上の特定の目的のために自己の個人データの処理に同意を与えた場合
	本人の契約	(b) 本人が当事者となっている契約の履行のために処理が必要な場合、または契約の締結前の本人の求めに応じて手続きを履践するために処理が必要な場合
	法の遵守	(c) 管理者が従うべき法的義務を遵守するために処理が必要な場合
	本人／他者の利益保護	(d) 本人、または他の自然人の重大な利益を保護するために処理が必要な場合
	公共の利益	(e) 公共の利益、また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処理が必要な場合
	正当な利益	(f) 管理者または第三者によって追求される正当な利益のために処理が必要な場合。ただし、本人の、特に子どもが本人である場合の個人データの保護を求める基本的権利および自由が、当該利益に優先する場合を除く

出所: JETRO「EU一般データ保護規則(GDPR)」に関わる実務ハンドブック(入門編)P.9を基に作成

# 個人データを取得する際利用目的等を本人に知らせる必要があります

## 情報提供

凡例: ● 該当  
— 非該当

#	情報の項目	例	本人から取得の場合 (13条)	本人以外から取得の場合 (14条)
1	会社の名称および連絡先	会社名、代表番号	●	●
2	データ保護責任者の連絡先（設置している場合）	データ保護責任者の氏名、所在地、専用メールアドレス	●	●
3	個人データの利用目的、および取扱いの法的根拠	〇〇サービスの提供、マーケティング、調査、新サービスの開発	●	●
4	個人データの種類	氏名・住所・電話番号、健康情報、パスポート番号	—	●
5	当社もしくは提供先が得られる正当な利益（本人の同意ではなく、正当な利益として処理する場合）	貴社が得られる正当な利益について（例：サービス改善、マーケティング、セキュリティの確保など）	●	●
6	提供先の種類（個人データを他社に提供する場合）	委託先	●	●
7	域外移転に関する情報（EU/EEA域外に移転する場合）	移転先の国名、移転する個人データの項目	●	●
8	個人データの保存期間	サービス提供が完了した後、〇〇年間保管	●	●
9	本人の権利（本人の同意を得て処理する場合、いつでも同意を撤回できる旨を含めること）※1	本人が開示請求等を行えること、および受付方法	●	●
10	監督機関に不服を申し立てる権利	監督機関に不服を申し立てることができること	●	●
11	法令または契約締結のために個人データの提供の義務があるか否か、提供を拒否した場合の結果	個人データの提供を拒否された場合、サービス提供（輸送等）が行えない場合があること	●	—
12	EU個人データの取得元情報、および一般公開されている情報から取得した場合、その旨	取得元の会社名	—	●
13	プロファイリングも含む自動化された処理の有無、自動化された処理の判断の根拠となる情報、および想定される結果	当社HPの閲覧履歴を用いて、行動ターゲティング広告を実施すること	●	●

※1 異議を唱える権利は、初めて通知する際に、データ主体の注意を喚起し、明確にかつ他の通知とは分離して明示することが求められています。

# データ主体には、さまざまな権利が認められています

## データ主体の権利

同意の有効性に関する権利	データ主体は、管理者に対して個人データを提供するにあたり、必要な情報の提供を受けることができる(13条、14条)
制限権	データ主体は、管理者に対して個人データの処理を制限することができる(18条)
異議権	データ主体は、管理者又は第三者によって追求される正当な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱えることができる(21条)
削除権	データ主体は、管理者に対して自己に関する個人データを遅滞なく削除するよう求めることができる(17条)
アクセス権	データ主体は、自己の個人データへアクセスすることができる(15条)
訂正権	データ主体は、不正確な自己の個人データに関する訂正を管理者に求めることができる(16条)
データポータビリティの権利	データ主体は自己に関わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取ることができる(20条)
自動化された個人の判断に関する権利	データ主体は、自己に対する多大な影響を生じうるプロファイリングを含む自動処理のみに基づいた判断の対象にならないよう求めることができる(22条)

出所:REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)を基に作成

# 違反時には高額な制裁金が規定されています

## 違反の内容に応じた制裁金

制裁金	違反の内容
企業の全世界年間売上高の2%以下または€1,000万以下のいずれか高い方	<ul style="list-style-type: none"><li>• 子供の同意に適用される条件に従わなかった場合</li><li>• GDPR要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合</li><li>• 義務があるのにEU代表者を選任しない場合</li><li>• 責任にもとづいて処理行為の記録を保持しない場合</li><li>• 監督機関に協力しない場合</li><li>• リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合</li><li>• セキュリティ違反を監督機関に通知しなかった場合、データ主体に通知しなかった場合</li><li>• データ保護影響評価を行わなかった場合</li><li>• データ保護影響評価によって示されていたにも係わらず処理の前に監督機関に助言を求めなかった場合</li><li>• DPO(Data Protection Officer)を選任しなかった場合、またはその職や役務を尊重しなかった場合</li></ul>
企業の全世界年間売上高の4%以下または€2,000万以下のいずれか高い方	<ul style="list-style-type: none"><li>• 個人データの処理の原則を遵守しなかった場合</li><li>• 適法に個人データを処理しなかった場合</li><li>• 同意の条件を遵守しなかった場合</li><li>• 特別な個人データの処理の条件を遵守しなかった場合</li><li>• データ主体の権利およびその行使の手順を尊重しなかった場合</li><li>• 個人データの移転の条件に従わなかった場合</li><li>• 監督機関の命令に従わなかった場合</li></ul>

出所: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)をもとに作成

# EU当局によるGDPRのガイドラインがリリースされています

## GDPRに関するガイドラインの公表状況

正式リリース済み

未リリース(ドラフトなど)

2018年5月9日時点

No.	対象事項	文書番号	文書名	発行日／ステータス
1	データポータビリティ	WP242	Guidelines on the right to data portability	2016年12月13日採択 2017年4月5日改定
2	データ保護責任者	WP243	Guidelines on Data Protection Officers ('DPOs')	2016年12月13日採択 2017年4月5日改定
3	主要監督機関	WP244	Guidelines for identifying a controller or processor's lead supervisory authority	2016年12月13日採択 2017年4月5日改定
4	データ保護影響評価	WP248	Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679	2017年4月4日採択 2017年10月4日改定
5	同意	WP259	Guidelines on Consent under Regulation 2016/679	2017年11月28日採択 2018年4月10日改定
6	プロファイリング	WP251	Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679	2017年10月3日採択 2018年2月6日改定
7	透明性	WP260	Guidelines on transparency under Regulation 2016/679	2017年11月29日採択 2018年4月11日改定
8	第三国へのデータ移転	WP262	Guidelines on Article 49 of Regulation 2016/679*	2018年3月26日 パブリックコメント終了
9	侵害通知	WP250	Guidelines on Personal data breach notification under Regulation 2016/679	2017年10月3日採択 2018年2月6日改定
10	認証	WP261	Article 29 Working Party Draft Guidelines on the accreditation of certification bodies under Regulation (EU) 2016/679	2018年3月30日 パブリックコメント終了

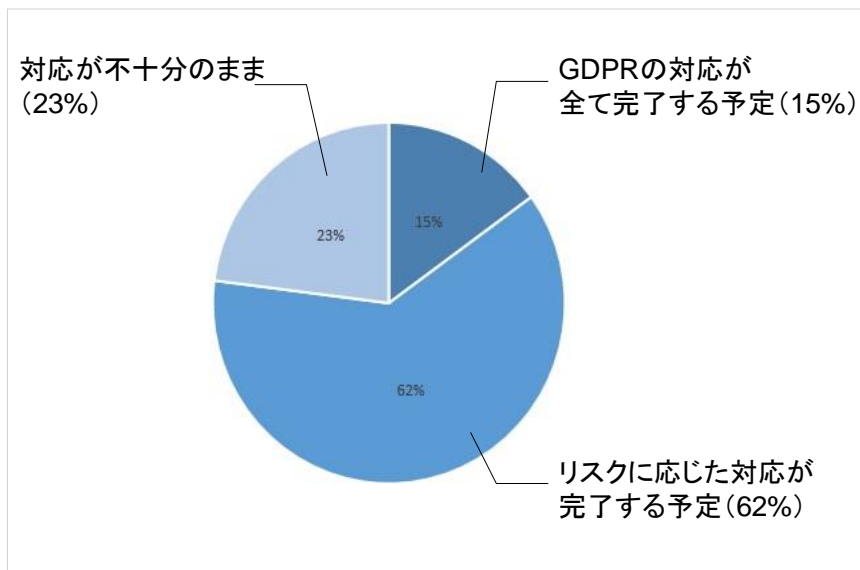
※一部のデータ移転の仕組み(例外での移転)だけが含まれるものであり、BCRやSDPC等に関しては別のガイドラインが公表される可能性があります。

# 多くの企業ではGDPR施行後も対応が継続する見通しとなっています

## 他社等の対応状況

### ■ 海外企業の対応の動向

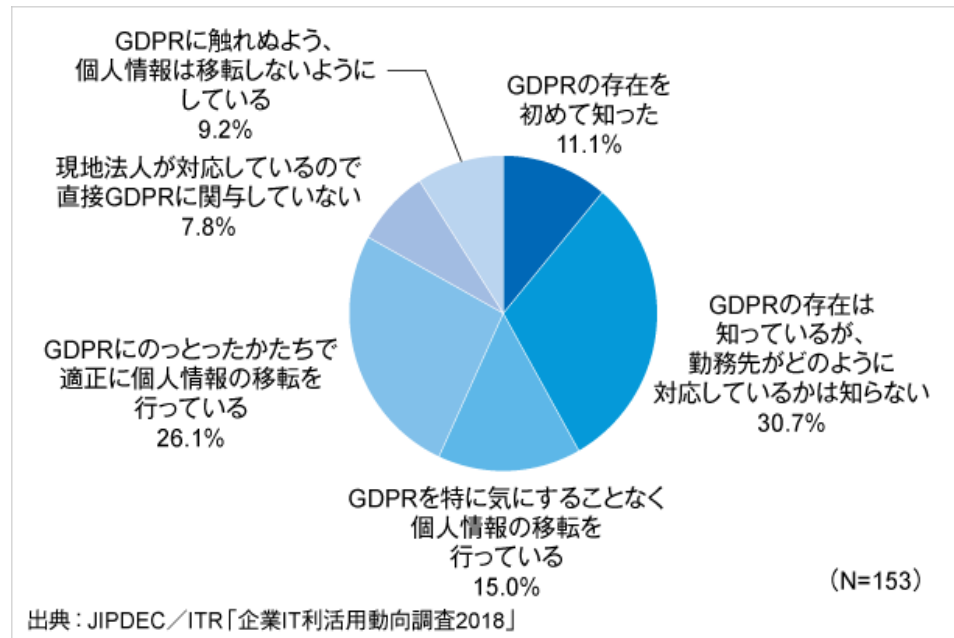
- ✓ 当社のメンバーファームの調査によると、GDPRの施行日までの対応状況は以下の通りとなります。
- ✓ グローバルでも各企業のGDPR対応は遅滞していることがうかがえます。



出所: The Deloitte General Data Protection Regulation Benchmarking Survey (<https://www2.deloitte.com/ru/en/pages/risk/articles/deloitte-gdpr-benchmarking-survey-the-time-is-now.html>)

### ■ 国内企業の対応の動向

- ✓ JIPDEC/ITRが実施した企業の動向調査では、国内企業において、いまだGDPRの対応が不十分であることが示されています。
- ✓ GDPRに則ったかたちで適正に個人情報の移転を行っていると回答したのは、わずか26.1%となります。



出所: 企業IT利活用動向調査2018 (<https://www.itr.co.jp/company/press/180327PR.html>)



# 説明責任

# 管理者は、個人データの処理において 以下の原則を遵守していることを説明する責任があります

## 説明責任

原則	内容
適法性、公平性及び透明性	適法、公平かつ透明性のある方法で処理すること(5条(a))
目的の限定	特定の、明確、かつ正当な理由のために収集され、それらの目的にそぐわない方法でそれ以上の処理を行わないこと(5条(b))
データの限定	処理を行う目的に関し、十分で関連性があり必要最低限に限定されていること(5条(c))
正確性	正確で、必要であれば常に最新状態に更新しておくこと。不正確な個人データは遅滞なく削除又は訂正すること(5条(d))
保管の限定	処理の目的に必要な期間以上、データ主体の識別が可能な状態で保管をしないこと(5条(e))
完全性と機密性	不正な又は違法な処理からの保護、不慮の損失、破壊からの保護を含み、個人データの適切なセキュリティが確保される形で処理すること(5条(f))

# 適法な個人データの処理のため、以下の条件を満たす必要があります

## 個人データ処理の適法性

### データ主体が同意した場合

データ主体が、一つ以上の具体的な目的のために、自分自身の個人データが処理されることに同意している場合(6条(1)(a))

### 処理が必要とされる場合

以下に示す状況にある場合。

- 契約前にデータ主体の要望による場合、あるいはデータ主体が関係者として契約を履行するため(6条(1)(b))
- 管理者が従うべき法律上の義務を遵守するため(6条(1)(c))
- 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(6条(1)(d))
- 公共の利益あるいは管理者に属する公式な権限の行使として実行する作業の履行のため(6条(1)(e))

### 正当な利益のために必要な場合

管理者あるいは第三者が追求する正当な利益のために必要である場合(6条(1)(f))

# 個人データを処理するためには、明確な同意を得る必要があります

## 同意の条件

### 同意の取得

データ主体の同意とは、自由に与えられ、特定の、情報に基づいた、明確なデータ主体の表示によって、データ主体が合意を示すことを意味する(4条(11))。

- Webサイトでチェックボックスにチェックを入れる
- 同意書への署名

### 同意の条件

データ主体の同意が、適切に取得されたものであるかを検討するためには、次の点を考慮する。

- 管理者及び処理者の身元、処理の目的等の情報がデータ主体に通知されていること(13条参照)
- 実質的な選択の自由がなく、不利益を被ることなしに同意を撤回することができないこと
- 分かりやすい言葉で明瞭かつ簡潔に表現されていること(7条(2))
- 処理の目的が複数ある場合には、全ての処理目的について同意が得られていること

### 子どもの場合

データ処理の対象が16歳未満の子どもの場合、同意は親としての責任を有する者によって承認されなければならない(8条(1))。

# 域外移転規制

# 原則EU域外への個人データの移転は禁止されています

## 域外移転(十分性認定が得られていない国・地域への移転)

方法	概要
明確な同意の取得	✓ データ主体から個人データ移転に関する明確な同意を得ます。
拘束的企業準則 (BCR: Binding Corporate Rules)	✓ グループ内で統一された情報管理を実施している場合に選択できます。 ✓ その情報管理の方法を文書化し、監督機関に申請して承認を得ます。これによりグループ企業を包括した個人データ移転が認められます。 ✓ 監督機関に提出する文書には、SDPC(次項参照)と比べて情報管理に関する詳細な記載が求められ、外部専門家の助力が必要になる場合が多いといえます。
標準契約 (SDPC: Standard Data Protection Clause) ※EUデータ保護指令におけるSCC	✓ 所定の契約フォーマットを使用して、監督機関への届出・申請・承認取得等を行います。 ✓ 個別契約を取交わした企業間のみ適用され、その種類は管理者間の契約である①セットI及び②セットIIのほか、管理者と処理者の間の契約である③CtoPの3種類のフォーマットがあります。
認証 (Certification)	✓ EDPB又は監督機関によって承認される基準に基づいて認証されます。 ✓ 認証は3年間有効であり、延長が可能です。 ✓ 今後、認証機関が設置される予定であり、詳細は未定です。
行動規範 (Codes of conduct)	✓ 業界団体がその特質を踏まえ、GDPRの遵守を目的とした行動規範を作成します。 ✓ 監督機関が適切な安全対策を講じているとして行動規範を承認した場合には、行動規範に基づいて行動する企業は、GDPRの要求事項を満たすものとされます。 ✓ 行動規範の作成、遵守状況の監視を行う機関など、未定な部分が多くあります。

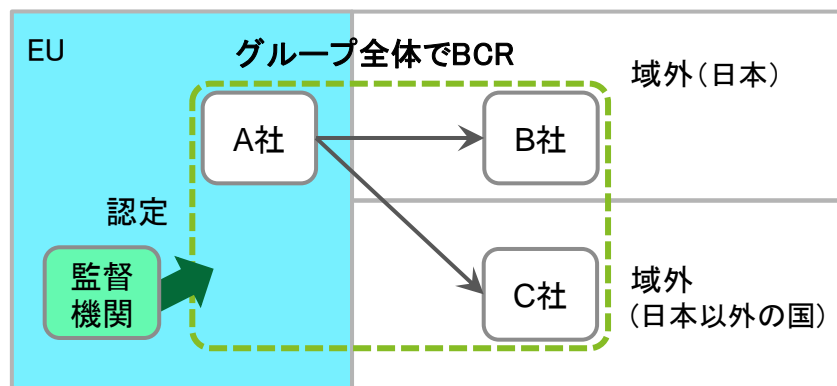
出所:REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)をもとに作成

# 多くの事業者がSDPCを締結し、個人データを移転しています

## Standard Data Protection Clauses

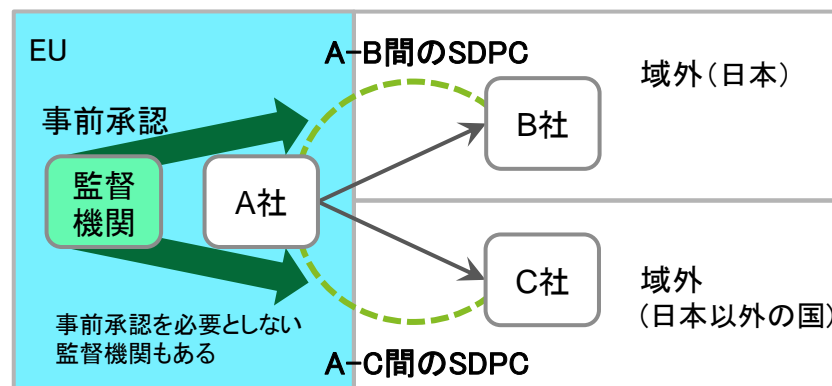
方法	メリット	デメリット	ポイント
BCR	<ul style="list-style-type: none"> <li>■ 新しいデータ移転ごとに契約を締結するといった対応の必要がなく、一つのルールによって全グループ企業を拘束することができるので、EU 域外にある多数の企業に対して個人データの移転が可能になります。</li> </ul>	<ul style="list-style-type: none"> <li>■ 監督機関による承認に時間を必要とします。</li> <li>■ 相互承認がない国の監督機関については、別途その監督機関に申請が必要になります。</li> </ul>	<ul style="list-style-type: none"> <li>■ データ移転が多数の企業間に行われる場合で、統一的なルールが強制できる場合に適しています。</li> </ul>
SDPC	<ul style="list-style-type: none"> <li>■ モデル契約を締結し、その条項を遵守するだけで、比較的容易にデータの移転を行うことができます。</li> </ul>	<ul style="list-style-type: none"> <li>■ 各企業間において個別に契約を締結する必要があります。</li> </ul>	<ul style="list-style-type: none"> <li>■ <u>データ移転が少数の企業間で行われる場合に適しています。</u></li> </ul>

BCRの例



→ データの移転

SDPCの例



# 2019年1月23日、日本が十分性認定を得ました

## 【ご参考】 日本の十分性認定について

日EU間の相互の円滑な個人データ移転を図る枠組みが、本年1月23日に発効します。

本枠組みの構築に関しては、日EU双方の経済界の要望等も受け個人情報保護委員会と欧州委員会との間で交渉を重ね、平成30年7月、個人情報保護委員会が個人情報保護法第24条に基づく指定をEUに対して行い、欧州委員会がGDPR第45条に基づく十分性認定を我が国に対して行う方針について合意に至りました。この合意を踏まえて、我が国においては、第85回個人情報保護委員会において、上記のEU指定を1月23日付けにて行うことを決定しました。また、欧州委員会においても、上記の我が国の十分性認定を同23日付けにて決定する予定となっています。（出所：個人情報保護法「日EU間の相互の円滑な個人データの移転～ボーダレスな越境移転が実現～」）

#	対応事項	概要
1	日本への移転	日本が十分性認定に依拠して移転を行う場合の、内部規程や処理者との契約については検討する必要がある。
2	日本以外の第三国への移転	日本が十分性認定にかかわらず、日本以外の第三国への移転（日本からの再移転も含む）がある場合は、移転の手続きが必要になる。
3	域外適用	日本が十分性認定にかかわらず、域外適用の対象になる場合には、同意取得やDPO任命など、GDPRの諸要件に対応する必要がある。

※ これまで十分性認定を受けていた国・地域は次のとおりです：

スイス、カナダ、アルゼンチン、ガーンジー島、マン島、ジャージー島、フェロー諸島、アンドラ、イスラエル、ウルグアイ、ニュージーランド



# 遵守するための対策の実施

# 管理者又は処理者は以下に示す措置等を実施しなければなりません

## GDPR遵守のための措置

### 管理者

- ① データ保護ポリシーを含む適切な措置を実施すること(24条(1)及び(2))
- ② データ主体の権利を保護するため仮名化等の措置を実施すること(25条(1))
- ③ 処理の目的を特定し、目的の達成に必要な個人データのみでの処理を行うこと
- ④ 処理の目的や採用したセキュリティ対策等の情報を含む個人データ処理行為の全ての事項の記録を保持すること(30条(1))

### 処理者

- ① 管理者は、GDPRの要件を充足する技術的組織的な対策の実行を保証できる処理者以外を使用してはならないこと(28条(1))
- ② 管理者と処理者との間には、拘束力のある契約がなければならないこと(28条(3))
- ③ 処理者は、管理者による特定の又は一般的な事前承諾なしに他の処理者に協力を求めることができないこと(28条(2))
- ④ 処理者は、管理者を代理して行なった個人データ処理行為の全ての事項の記録を保持すること(30条(2))

# 事業者に対して特定の役割を担う担当者の設置を求めています

## データ保護責任者の選任

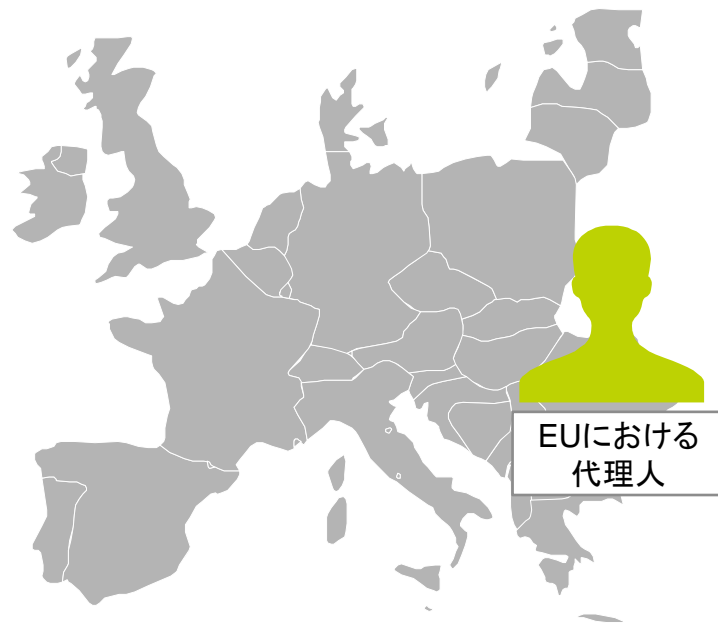
個人データの処理が定期的、組織的な場合や特別な種類のデータ(いわゆるセンシティブデータ)を処理する場合には、データ保護責任者(DPO)の設置が求められています。

選任	<ul style="list-style-type: none"><li>✓ 専門家としての質、特にデータ保護法及びその実務の専門知識並びに任務を遂行する技量に基づいて選任される(37条(5))。</li><li>✓ 企業グループは、各組織から簡単にアクセスできることを条件に単一のDPOを選任することができる(37条(2))。</li></ul>
地位	<ul style="list-style-type: none"><li>✓ 管理者・処理者は、DPOが個人データ保護に関する一切の事柄について適切、適時に取り組むことを確実にしなければならない。</li><li>✓ データ主体は、データ処理及びGDPRに基づく権利の行使に関わる一切の事柄についてDPOに連絡をとることができる。</li><li>✓ DPOは、自らの任務遂行に関わる指示を一切受けなければならない。</li><li>✓ DPOは、管理者又は処理者の最高経営レベルに直接報告を行なうものとする。</li></ul>
任務	<ul style="list-style-type: none"><li>✓ GDPR及びその他のEU及び加盟国の条項に基づく義務について管理者・処理者及び個人データを処理する事業者に対して、情報と助言を提供する。</li><li>✓ 監督機関と協力する。</li><li>✓ 事前相談、相談並びに個人データの処理に関する事項について監督機関との窓口となる。</li></ul>

## EUにおける代理人の選任

EU域内に本社や子会社等が存在しない場合であって、GDPRの適用対象となる場合(具体的には、EU域内で個人データを収集し、日本で処理を行っている場合、EU域内へ日本から直接、商品やサービスを提供している場合等)には、データ主体が居住するEU加盟国の1つにおいて、書面で代理人を任命する必要があります。

代理人は、監督機関やデータ主体との連絡窓口としての役割を果たします。



# 「データ保護責任者」を任命しなくてはならない場合があります

## データ保護責任者(Data Protection Officer)の任命

### 任命の義務に関する条件

#### ■【処理の実施主体、内容等】

第37条(1)によれば、以下の場合にDPOの任命を要求しています。

- 処理が公的機関または公的団体によって行われる場合
- 管理者または処理者の主活動がデータ主体の定期的及び体系的監視が大規模に要求される処理活動である場合
- 管理者または処理者の主活動が特別カテゴリのデータまたは有罪判決および犯罪に関連する個人データの大規模な処理である場合

#### ■【任命される者】

DPO第37条(6)によれば、DPOの自主的な任命の場合、管理者または処理者の職員(内部DPO)でも、外部者が「サービス契約に基づいて任務を果たす」こともできます。この場合、個人または組織と締結されたサービス契約に基づいてDPOの機能を実行することができますが、GDPR上のDPOではないことを明確にする必要があります。DPOが外部の場合でも、第37条から第39条※のすべての要件がそのようなDPOに適用されます。

※GDPR 第37条～第39条

第37条 Designation of the data protection officer (データ保護責任者の選任)

第38条 Position of the data protection officer (データ保護責任者の位置付け)

第39条 Tasks of the data protection officer (データ保護責任者の職務)

### 任命の仕方

- 第37条によれば、DPOの任命に関しては、管理者及び処理者の両方に該当します。義務的な任命に関する基準を満たす管理者または処理者が、場合によっては、管理者及び処理者両方がDPOを任命する必要があります。
- 「容易にアクセスできる」という条件のもと、グループ企業は単一のDPOを任命することができます。容易にアクセスできるとは、データ主体、監督当局及び組織内からDPOと連絡することができる状況を指します。

出所: REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 (2016/4/5)をもとに作成

# データセキュリティに関する義務

# セキュリティに関する義務が課せられています

## セキュリティに関する義務

義務		概要
侵害発生前	リスクに対して適切なセキュリティレベルを確保する技術的かつ組織的措置の実施	<ul style="list-style-type: none"><li>仮名化、暗号化、システム復元力の確保などの措置の実施、およびこれらの措置の定期的な検査</li></ul>
侵害発生後	差別、個人データ窃盗、詐欺、経済的損失、仮名化の不法解除、レピュテーションの棄損、経済的または社会的損害などの個人の自由および権利にとっての危険性が高い侵害に関する通知	<ul style="list-style-type: none"><li>不当な遅滞なく、可能な場合には侵害に気づいてから72時間以内に監督機関へ通知する義務</li><li>不当な遅滞なく、データ主体にその旨を通知する義務（処理者の場合は管理者へ通知する義務）</li></ul>

### データ保護影響評価(DPIA)

#### 【評価の契機】

新しい技術を使ったデータ処理で、個人の権利や自由に対するリスクが高い場合

#### 【評価に含まれる事項】

- 想定される処理の内容や処理の目的に関する体系的な説明
- 目的に関する処理の必要性および比例性の評価
- データ主体の権利および自由に対するリスク評価
- リスクに対処するための保護措置（セキュリティ措置、個人データ保護のための管理態勢、およびデータ主体ならびに関連するその他の個人の権利および正当な利益を考慮したGDPR遵守の実証を含む）

# データ主体の権利

# データ主体には、積極的、消極的の両面の権利が認められています

## データ主体の権利

同意の有効性に関する権利	データ主体は、管理者に対して個人データを提供するにあたり、必要な情報の提供を受けることができる(13条、14条)
制限権	データ主体は、管理者に対して個人データの処理を制限することができる(18条)
異議権	データ主体は、管理者又は第三者によって追求される正当な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱えることができる(21条)
削除権	データ主体は、管理者に対して自己に関する個人データを遅滞なく削除するよう求めることができる(17条)
アクセス権	データ主体は、自己の個人データへアクセスすることができる(15条)
訂正権	データ主体は、不正確な自己の個人データに関する訂正を管理者に求めることができる(16条)
データポータビリティの権利	データ主体は自己に関わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取ることができる(20条)
自動化された個人の判断に関する権利	データ主体は、自己に対する多大な影響を生じうるプロファイリングを含む自動処理のみに基づいた判断の対象にならないよう求めることができる(22条)



# 判例において認められた権利が、法制化されました

## 削除権(忘れられる権利)

削除権自体は、EUデータ保護指令12条(b)号にも規定されているが、あくまで不完全または不正確なデータの消去等を求めることができるにとどまっている。

これに対し、規則における削除権(「忘れられる権利」)は、取得目的との関係でデータが必要とされなくなった場合や同意を撤回した場合等一定の要件を満たす場合に、自らに関する個人データを削除させる権利や、当該データのさらなる拡散を停止させる権利を認めたものである。

なお、我が国でも、近時「忘れられる権利」を認める裁判例がある。

2014年5月13日に、EU司法裁判所がグーグル社に対し、個人が自己の名前を検索した際に表示される同人の過去の情報へのリンクを削除するよう命じる判決を出した。

### ■ 判決の概要

所有していた不動産が競売に掛けられたことを報じた10年以上前の新聞記事が、インターネットで自分の名前を検索した際の検索結果に今も表示されるのはプライバシーの侵害だとして、スペイン人男性がインターネット検索大手グーグルを提訴した。

この裁判で、2014年5月、欧州連合(EU)司法裁判所がプライバシー保護の観点からグーグルなどの検索企業は、一定の条件下でリンクを削除する義務がある、という「忘れられる権利」を認める判決を出した。

# 個人データを自らの意思に基づいて移転できます

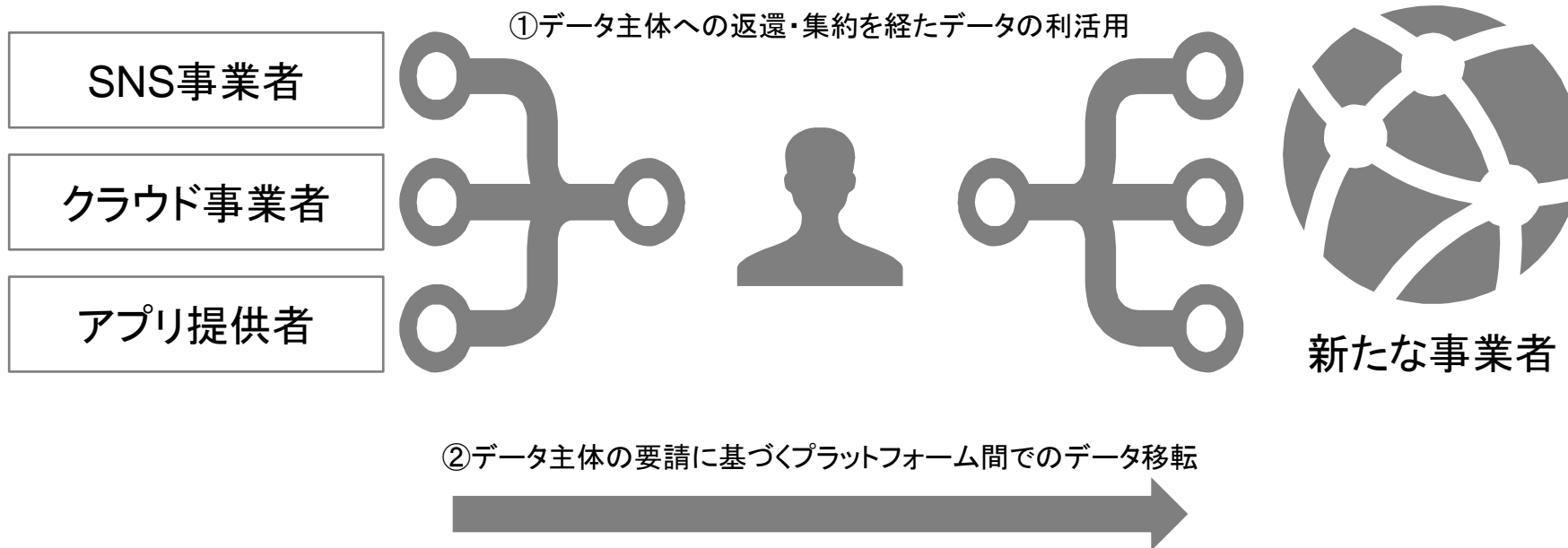
データポータビリティの権利は、2つの権利から構成されています。  
この権利は、個人データの保護と利活用とを両立しようとする権利です。

## データポータビリティの権利

### データポータビリティの権利

管理者からデータ主体が自らの個人データを扱いやすい電子的な形式で取り戻す権利

データ管理者から別のデータ管理者に移行させる権利



デロイト トーマツ グループは日本におけるデロイト トウシュ トーマツ リミテッド(英国の法令に基づく保証有限責任会社)のメンバーファームであるデロイト トーマツ 合同会社およびそのグループ法人(有限責任監査法人トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャルアドバイザー 合同会社、デロイト トーマツ 税理士法人、DT 弁護士法人およびデロイト トーマツ コーポレート ソリューション 合同会社を含む)の総称です。デロイト トーマツ グループは日本で最大級のビジネスプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスクアドバイザー、コンサルティング、ファイナンシャルアドバイザー、税務、法務等を提供しています。また、国内約40都市に約11,000名の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト ([www.deloitte.com/jp](http://www.deloitte.com/jp)) をご覧ください。

Deloitte(デロイト)は、監査・保証業務、コンサルティング、ファイナンシャルアドバイザーサービス、リスクアドバイザー、税務およびこれらに関連するサービスを、さまざまな業種にわたる上場・非上場のクライアントに提供しています。全世界150を超える国・地域のメンバーファームのネットワークを通じ、デロイトは、高度に複合化されたビジネスに取り組むクライアントに向けて、深い洞察に基づき、世界最高水準の陣容をもって高品質なサービスをFortune Global 500® の8割の企業に提供しています。“Making an impact that matters”を自らの使命とするデロイトの約245,000名の専門家については、[Facebook](#)、[LinkedIn](#)、[Twitter](#) もご覧ください。

Deloitte(デロイト)とは、英国の法令に基づく保証有限責任会社であるデロイト トウシュ トーマツ リミテッド(“DTTL”)ならびにそのネットワーク組織を構成するメンバーファームおよびその関係会社のひとつまたは複数を含みます。DTTLおよび各メンバーファームはそれぞれ法的に独立した別個の組織体です。DTTL(または“Deloitte Global”)はクライアントへのサービス提供を行いません。Deloitteのメンバーファームによるグローバルネットワークの詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。



IS 669126 / ISO 27001