JETRO
日本貿易振興機構（ジェトロ）

「英国一般データ保護規制（UK GDPR）」実務ハンドブック

2022 年 4 月

日本貿易振興機構（ジェトロ）
ロンドン事務所
海外調査部

【免責条項】

本レポートで提供している情報は、ご利用される方のご判断・責任においてご使用下さい。ジェトロでは、できるだけ正確な情報の提供を心掛けておりますが、本レポートで提供した内容に関連して、ご利用される方が不利益等を被る事態が生じたとしても、ジェトロおよび執筆者は一切の責任を負いかねますので、ご了承下さい。

〈目次〉

はじめに

英国の一般データ保護規則（GDPR：General Data Protection Regulation、以下「UK GDPR」という）とは、英国のブレグジット（欧州連合（EU: European Union、以下「EU」という）からの離脱）に伴って、EU の一般データ保護規則（GDPR: General Data Protection Regulation、以下「EU GDPR」という）の内容に基づいて、2021 年 1 月 1 日に施行された英国の法律である。本レポートは、UK GDPR について、その概要や実務対応などを日本企業向けに解説するものである。

本レポートは、ジェトロが S&K Brussels 法律事務所代表パートナーの杉本武重弁護士および同事務所アソシエイトの伊藤美奈子弁護士に委託して執筆したものであり、その著作権はジェトロに帰属する。本レポートの内容は別途表記がない限り、2022 年 3 月 27 日時点で公表された情報に基づいているものであり、その後の法律改正などによって変わる場合がある。また、掲載した情報・コメントは執筆者および日本貿易振興機構（ジェトロ）の判断によるが、一般的な情報・解釈がこのとおりであることを保証するものではない。

本レポートが、日本企業の皆様にとって、英国をはじめ、欧州ビジネス展開の上での一助となれば幸いである。

2022 年 4 月
日本貿易振興機構（ジェトロ）
海外調査部 欧州ロシア CIS 課

I. UK GDPR の概要

1. UK GDPR の位置づけ

UK GDPR[1]は、法執行機関や情報機関を除き、英国における個人データのほとんどの処理について、重要な原則、権利および、義務を定めている。また、2018 年データ保護法[2]（Data Protection Act 2018、以下「DPA 2018」という）は、英国におけるデータ保護法の枠組みを定めたものであり、1998 年データ保護法を更新するもので、2018 年 5 月 25 日に発効した。英国の EU 離脱状況を反映して、2018 年 EU 離脱法に基づく規制により 2021 年 1 月 1 日に改正された。

DPA 2018 は、免除規定などにより、UK GDPR と並立し、補足する役割を果たしている。また、法執行機関のための個別のデータ保護規則を定め、国家安全保障や防衛など他の一部の分野にデータ保護を拡大し、英国の独立した第三者機関としてのデータ保護監督当局である情報コミッショナーオフィス（Information Commissioner's Office、以下「**ICO**」という）の機能と権限を定めている。言い換えると、DPA 2018 には、一般的な個人データの処理に関する規制である UK GDPR（Part2）、法執行機関のための個別の制度（Part 3）、3 つの諜報機関のための独立した制度（Part 4）という 3 つの独立したデータ保護制度が含まれている。

2. UK GDPR とは何か

（1）UK GDPR とは

UK GDPR を一言で表現すると、「個人データの処理および英国国外への移転を行うための要件を定めるとともに、処理または移転を行う者が遵守すべき規範・義務を定めた規則」である。UK GDPR は、英国国内の「管理者」または「処理者」の拠点の活動の過程において行われる「個人データ」の「処理」に適用される（UK GDPR3 条 1 項）（以下、本レポートでは特に断りがない限り条文番号は UK GDPR 本文のそれを意味するものとする）ため、それぞれの定義を概説する。なお、UK GDPR は一定の場合に英国国内に拠点を持たない管理者または処理者による個人データの処理にも適用される（3 条 2 項）。

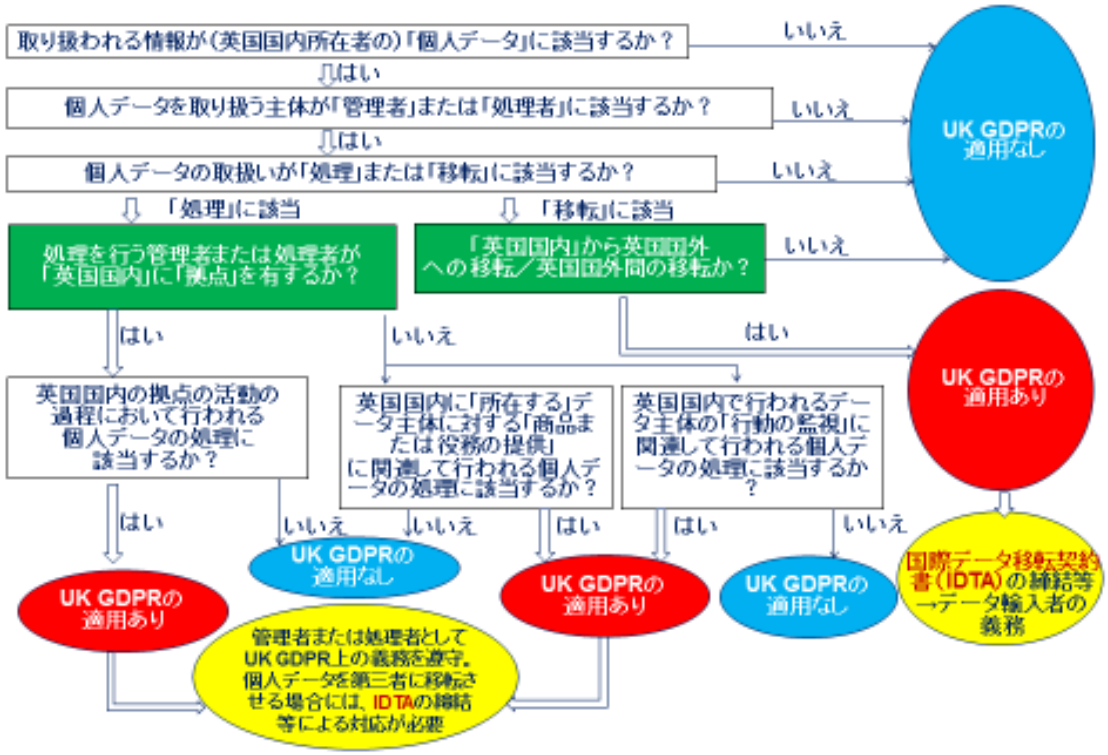
UK GDPR の適用範囲に関する検討のフローチャートは以下の図 1 の通りである。このフローチャートで登場する基本概念を 2.（2）以下で説明する。

---

[1]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 (United Kingdom General Data Protection Regulation) (Text with EEA relevance), https://www.legislation.gov.uk/eur/2016/679/contents

[2] Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents

図１：UK GDPR の適用範囲に関する検討のフローチャート



(2)「個人データ」

UK GDPR において、「**個人データ**」とは、識別された、または識別可能な自然人（データ主体）に関するあらゆる情報[3]をいう（4 条 1 号）。「**識別可能な自然人**」とは、特に、氏名、識別番号、位置データ、オンライン識別子等の識別子、または当該自然人の身体的、生理的、遺伝的、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 1 つ、若しくは複数の要素を参照することによって、直接的または間接的に識別されうるものをいう[4]。ここでの個人データは、英国居住者ではなく、英国国内に所在するデータ主体に関するものである。また、英国国外に所在するデータ主体に関する個人データであっても、英国国内で処理される場合には UK GDPR の適用がある。

「**仮名化**」とは、個人の特定につながる追加情報とは別途保管され、かつ技術的および組織的措置によって、追加情報なしでは個人を特定できないような方法で個人データを処理することをいう（4 条 5 号）[5]。匿名化とは異なり、追加情報と組み合わせることで自然

[3] 個人データには、特別なカテゴリの個人データや、犯罪歴・犯罪行為に関するデータが含まれる場合がある。これらのデータはよりセンシティビティが高いと考えられ、より限定された状況でのみ処理することができる。

[4] 具体的には、氏名、役職、自宅住所、識別番号（顧客番号等）、位置データ、E メールアドレス（個人用/業務用）、電話番号（個人用/業務用）、雇用者、オンライン識別子（IP アドレス、クッキー識別子）、犯罪歴、クレジットカード・銀行口座情報、記録された顧客の通話内容、監視カメラの映像、従業員の人事考課記録・採用情報（履歴書、証明書、配偶者の有無、生年月日、推薦状等）等の幅広い情報が個人データに該当する。

[5] 典型例として、小売店や百貨店等が、ポイントカードの会員となった顧客の情報を、氏名ではなく顧客

人の特定が可能になることから、仮名化された情報は「個人データ」に該当し、UK GDPR の規制が適用される。仮名化によって、データ主体の特定が困難になるため、データ主体のリスクは緩和される。

(3)「処理」

UK GDPR は、全部または一部が自動的手段による個人データの「処理」に適用され、また、「ファイリングシステム」[6]の一部であるまたは「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手段以外による「処理」にも適用される（2 条 1 項）。個人データの「**処理**」とは、自動的な手段であるか否かを問わず、個人データ（またはその集合）に対して行われる、収集、記録、編集、構造化、保存、修正または変更、復旧、参照、利用、移転による開示、周知、またはその他の周知を可能とすること、整列若しくは結合、制限、消去または破壊等のあらゆる単独または一連の作業を意味する（4 条 2 号）。

UK GDPR における「処理」の概念は、EU GDPR におけるそれと同様に、非常に広範であり、個人データに関する作業は原則として処理に該当するものと考えて問題はない[7]。個人データの処理は原則として禁止され、一定の適法化根拠が存在する場合のみ、処理が許容される[8]。

ID やイニシャルで管理しているが、別途保管している住所や購買履歴等の他の情報と組み合わせることによって、当該顧客を特定することができる場合が挙げられる。氏名、住所、生年月日が黒塗りされていても、他の情報との組み合わせによってデータ主体を特定しうる場合はなお仮名化に該当するとされている（つまり、匿名化には該当しない）。

[6] 「**ファイリングシステム**」とは、機能的または地理的に、集積、分散または拡散されているか否かを問わず、特定の基準にしたがってアクセス可能なあらゆる構造化された個人データの集合をいう（4 条 6 号）。ファイリングシステムは、データを保管し、処理する 1 つまたは複数の手段のことを指し、例えば、紙のキャビネットである場合も、電子的なシステムである場合もあり得る。後者はデータベースや登録ソフトウェア（SAP 等）、電子メール処理ツール（Outlook 等）、データ処理ツール（Excel 等）、自動データログ（Web サイトのアクセス記録、登録や入室に関するログ等）やその他のデータを含む。ファイリングシステムの一部とすることが意図された個人データの処理、例えば、名刺を五十音順やアルファベット順に整理して管理している場合にも適用があり得ることに留意が必要である。

[7] **「処理」の具体例**は、㋐電子メールアドレスの収集、㋑クレジットカード情報の保管、㋒従業員の連絡先詳細の変更、㋓顧客氏名の開示、㋔社内業務評価の閲覧、㋕オンライン上の識別子の削除、㋖従業員の氏名、社内での職務、事業所の住所等を含むディレクトリの作成が挙げられる。特に注意を要するのは、クラウド事業者が顧客から委託を受けたクラウドサーバ上での顧客の従業員の個人データの含まれるデータの保管を行う場合、クラウド事業者が当該データの中身を全く見ることができない前提であっても、この保管自体が「処理」に該当し、また保守管理業者が保守点検の委託を受けて当該データにアクセスすること自体も「処理」に該当するという点である。

[8] 事業者は英国国内で事業を営んでいる以上、何らかの個人データの処理を行っており、適法化根拠の有無のチェックを行わない限り、知らず知らずのうちに、UK GDPR に違反しているということがあり得る。

(4)「移転」

個人データの**制限付き移転**[9]について、UK GDPR は定義規定を置いていないが、以下の各要件を満たす場合に制限付き移転に該当する[10]。

- UK GDPR が、組織が移転させる個人データの処理に対して適用される。
- データの処理に関して UK GDPR が適用されない受信者に、個人データを送付するまたは個人データへのアクセスを可能にする場合であって、通常受信者が英国以外の国に所在する場合に該当する。
- 受信者が別の会社、組織、個人であるため、送信者とは法的に区別される。これには、同じ企業グループ内の別の会社への移転も含まれる。もっとも、組織が個人データを当該組織の従業員に送っている場合は、移転制限の対象にはならない。移転規制は、個人データを自分の会社や組織の外に送る場合にのみ適用される。

個人データの英国国内から英国国外の第三国または国際機関への移転は、個人データの処理と同様、原則として「制限付き移転」として禁止され、一定の要件を充足する場合にのみ許容される。

(5)「データ管理者」と「データ処理者」

「**データ管理者**」とは、単独または他の者と共同して、個人データの処理の目的および手段を決定する自然人、法人、公的機関、行政機関またはその他の団体をいう（4 条 7 号）[11]。「**データ処理者**」とは、管理者のために個人データの処理を行う自然人、法人、公的機関、行政機関またはその他の団体をいう（4 条 8 号）[12]。ある事業者が管理者であるか処理者であるかは、個々の処理ごとに判断されるため、同一の事業者の事業活動のうち、ある処理行為については管理者として、他の処理行為については処理者として UK GDPR の規制が適用される可能性がある点に留意を要する[13]。

(6) 組織への UK GDPR の適用の有無

UK GDPR は以下の①から③の場面で組織による個人データの処理に対して適用される。UK GDPR の適用関係を整理したものが以下の表 1 である。

---

[9] 欧州データ保護会議（**EDPB**: European Data Protection Board）が公表した GDPR 第 3 条と GDPR 第 V 章における国際移転に関する規定との適用の相互関係に関するガイドライン 05/2021 のパブリックコンサルテーション版（https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf）において、「**移転**」は、特定の処理に関して GDPR の適用を受ける管理者または処理者（輸出者）が、当該処理に関して輸入者が GDPR の適用を受けるか否かにかかわらず、個人データを第三国の異なる管理者または処理者（輸入者）に送信または利用可能にすることと定義される。

[10] ICO, Guide to the General Data Protection Regulation (GDPR), International transfers after the UK exit from the EU Implementation Period, 1) Are we making a restricted transfer? (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#arewemaking)

[11] 事業を遂行するために顧客の個人データを処理する場合（マーケティング、カスタマーサービス等）や、労務管理のために自社の従業員の個人データを処理する場合、管理者に該当する。

[12] 典型的には、顧客に対してクラウドサービスを提供する事業者や、顧客従業員の給与計算代行を行う事業者等は、当該顧客との関係で処理者となる。

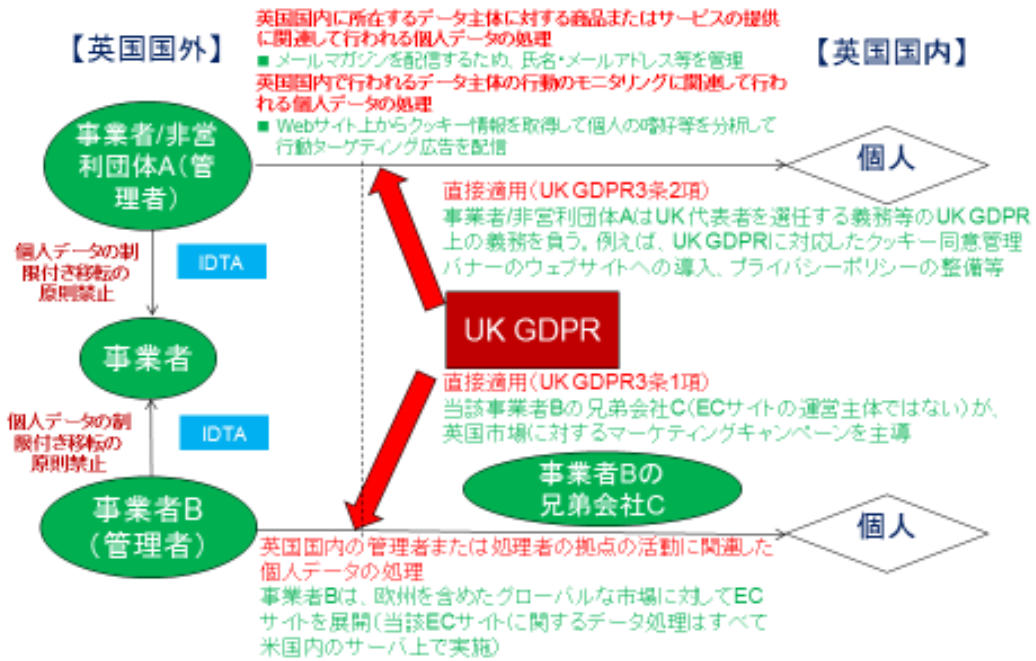
[13] 例えば、顧客企業の従業員の給与計算を請け負う事業者は、給与計算に関して顧客企業の従業員の個人データを処理する場合は処理者となる一方、自社における労務管理のために自らの従業員の個人データを処理する場合には、管理者に該当することになる。

表 1：UK GDPR の適用関係

拠点	適用対象となる処理	適用されるケースの例
英国国内に拠点あり	①英国国内の管理者または処理者の拠点の活動に関連した個人データの処理	日本国内の事業者 B が欧州を含めたグローバルな市場に対して EC サイトを展開（当該 EC サイトに関するデータ処理はすべて米国内のサーバ上で実施）、当該事業者 B の兄弟会社 C（EC サイトの運営主体ではない）が、欧州市場に対するマーケティングキャンペーンを主導し、これにより日本国内の事業者 B が欧州市場から収益をあげている。
英国国内に拠点なし	②英国国内に所在するデータ主体に対する商品またはサービスの提供に関連して行われる個人データの処理	■ 日本国内の事業者がゲームアプリを英国国内所在のプレイヤーに配信し、プレイヤーの氏名・課金履歴等を収集 ■ ポンド決済可能で英語表記があり、英国向け配送に言及している EC サイトで顧客の住所・氏名・口座情報等を収集 ■ 日本国内の事業者/非営利団体 A が、英国国内所在の個人に対してメールマガジンを配信するため、氏名・メールアドレス等を管理
	③英国国内で行われるデータ主体の行動のモニタリングに関連して行われる個人データの処理	■ 日本国内の事業者が英国国内に所在する個人から、アプリで位置情報を取得して分析 ■ 日本国内の事業者が Web サイト上からクッキー情報を取得して個人の嗜好等を分析して行動ターゲティング広告を配信 ■ 日本国内の事業者が、ウェアラブル端末（スマートウォッチ等）を通じて英国国内に所在する個人の健康関連情報を取得・管理

UK GDPR の英国国外の組織への適用関係について、上の表における適用されるケースを図 2 に示した。

図 2：UK GDPR の英国国外の組織への適用関係



3. UK GDPR 違反のリスク

UK GDPR の適用を受ける事業者が UK GDPR に違反した場合、大別して以下の 3 種類のリスクが生じ得る。

- ICO から多額の制裁金を含む罰則を科せられるリスク
- データ主体等による損害賠償請求等の法的請求を受けるリスク
- 個人データの保護に関する対応が不十分であるとしてビジネスにおける信用を失うリスク

4. 監督当局

英国のデータ保護監督当局は、ICO（情報コミッショナーオフィス）である。同局のトップは情報コミッショナーである。エリザベス・デナム（Elizabeth Denham）氏が 2021 年 11 月 30 日をもって退任し、2022 年 1 月 4 日から、ジョン・エドワーズ（John Edwards）氏（前ニュージーランド・プライバシーコミッショナー）が就任した[14]。

5. UK GDPR 上の諸義務

UK GDPR 違反に対する制裁金の上限額には、①1,750 万ポンド以下または事業者である場合は前会計年度の全世界年間売上高の 4%以下のいずれか高い方（83 条 5 項）と、②870 万ポンド以下、または事業者である場合は前会計年度の全世界年間売上高の 2%以下のいずれか高い方（83 条 4 項）の 2 つのレベルが定められている。事業者が遵守しなければならない UK GDPR の規制を①と②に分類すると以下の表 2 の通りである。

表 2：UK GDPR の規制

UK GDPR 上の諸義務（組織が遵守しなければならない UK GDPR の規制）
①1,750万ポンド以下または事業者である場合は前会計年度の全世界年間売上高の4%以下のいずれか高い方
1. データ処理に関する原則を遵守する義務（5条）
2. 適法に個人データを処理する義務（6条）
3. 同意の条件を遵守する義務（7条）
4. 特別カテゴリの個人データ処理の条件を遵守する義務（9条）
5. データ主体の権利およびその行使の手順を尊重する義務（12-22条）
6. 情報通知義務（13、14条）
7. 個人データの移転の条件に従う義務（44-49条）
8. ICOの命令に従う義務（58条1項、2項）
②870万ポンド以下、または事業者である場合は前会計年度の全世界年間売上高の2%以下のいずれか高い方
9. 16歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理に、子どもの保護責任者による同意または許可を取得する義務（8条）
10. 適切な技術的・組織的な対策を実施する処理者を利用する義務（28条）
11. 設計によるデータ保護・デフォルトとしてのデータ保護を確保するために適切な技術的措置および組織的措置を実装する義務（25条）
12. 該当する場合、英国代理人の選任義務（27条）
13. 責任に基づいて処理行為の記録を保持する義務（30条）
14. ICOに協力する義務（31条）

[14] ICO の新しい情報コミッショナーであるジョン・エドワーズ氏は、2014 年 2 月にニュージーランドのプライバシーコミッショナーという独立した法定の役職に任命され、ニュージーランドで新たに成立したプライバシー法 2020 の執行を担当し、2014 年から 17 年まで Global Privacy Assembly（当時は International Conference of Data Protection and Privacy Commissioners）の議長を務めるなど数多くの国際会議の議長やホストを務めてきた。また、ニュージーランドのプライバシーコミッショナーへの就任前、エドワーズ氏はニュージーランドのウェリントンで 20 年以上にわたり、情報法を専門に弁護士として活動し、公的機関や民間企業のクライアントを幅広く担当していた。

UK GDPR 上の諸義務（組織が遵守しなければならない UK GDPR の規制）
15. 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する義務（32条） 16. データ侵害通知義務がある場合、当局への通知義務およびデータ主体への通知義務（33条、34条） 17. 該当する場合、データ保護影響評価を実施する義務（35条） 18. 影響評価において緩和できないリスクがあった場合の当局への事前相談義務（36条） 19. データ保護責任者の選任義務、およびその職や役務を尊重する義務（37条から39条）

6. ICO による GDPR 違反に基づく制裁金決定の実例

ICO のウェブサイトには、数多くのデータ保護法違反の制裁金決定の実例が掲載されているが、そのうち 2018 年 5 月 25 日以降の GDPR 違反に基づいた制裁金決定の実例のうち、代表的なものは以下の通りである。

（1）ブリティッシュ・エアウェイズ（British Airways）

表 3-1 の通り、ブリティッシュ・エアウェイズは、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ていなかったため、ICO により、2,000 万ポンドの制裁金を課せられた。

表 3-1：制裁金決定事例 1（ブリティッシュ・エアウェイズ）

2020 年 10 月 16 日	2,000 万ポンド（約 30 億円）	ブリティッシュ・エアウェイズ（航空会社）	32 条
ブリティッシュ・エアウェイズのウェブサイトへのアクセス記録が不正サイトに転用されたことにより、2018 年 6 月から約 50 万人以上の顧客データが侵害されたため、同社は 2018 年 9 月に ICO にデータ侵害に関する通知を行った。ICO の調査の結果、 同社による脆弱なセキュリティ対策によって、氏名、住所、ログイン、カード支払、カード情報（カード番号、期限、裏面の 3 桁コード）、旅程予約の詳細を含む様々な情報が侵害されたことが判明した。ICO は、2019 年 6 月、セキュリティ対策義務違反があったとして、1 億 8,339 万ポンド（約 250 億円）の制裁金を課する意向を発表した（同社の前事業年度の全世界売上高の約 1.5%）。最終的には新型コロナウィルス感染爆発による航空業界への経済的影響を考慮し 2,000 万ポンドの制裁金が課された。			

（2）マリオット・インターナショナル（Marriott International Inc）

表 3-2 の通り、マリオット・インターナショナルは、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ていなかったため、ICO により、1,840 万ポンドの制裁金を課せられた。

表 3-2：制裁金決定事例 2（マリオット・インターナショナル）

2020 年 10 月 30 日	1,840 万ポンド（約 27.5 億円）	マリオット・インターナショナル（ホテル）	32 条
マリオット・インターナショナル社の予約システムからハッカーが顧客データを 4 年にわたって取得していたことが発覚し、2018 年 11 月に同社から ICO に通知された。これにより、約 3 億 3,900 万件の宿泊者データ（氏名、住所、電話番号、メールアドレス、約 525 万件の暗号化されていないパスポート番号と約 1,850 万件の暗号化されたパスポート番号、優遇者アカウント情報、生年月日、性別、宿泊情報、予約日、910 万件の暗号化されたカード番号（38 万 5 千件は 2018 年 9 月時点で期限切れ）が影響を受けた。また、EEA 加盟国 31 カ国に所在する個人のデータは約 3,000 万件（英国国民のデータは 700 万件）流出した。ICO は、セキュリティ対策義務違反があったとして、9,920 万 396 ポンド （約 148 億円）の制裁金を課する意向を発表した（同社の前事業年度の全世界売上高の約 3.5%）。最終的には同社が過去に違反や不作為を犯していないこと、調査に全面的に協力し、関係者に通知する措置をとったこと、他の企業、特に欧州のデータ保護当局に課された他の制裁金との整合性も考慮し 1,840 万ポンドの制裁金が課された。			

（3）チケットマスターUK （Ticketmaster UK Limited）

表 3-3 の通り、チケットマスターUK は、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ていなかったため、ICO により、125 万ポンドの制裁金を課せられた。

表 3-3：制裁金決定事例 3（チケットマスターUK）

2020 年 11 月 13 日	125 万ポンド（約 1.9 億円）	チケットマスターUK	5 条 1 項 f), 32 条
2018 年 2 月から 2018 年 6 月 23 日までの間に、チケットマスターUK が、同社のオンライン決済サイトにおいて、不十分なセキュリティのチャットボットを使用していた。そのため、ハッカーが顧客の金融情報にアクセスできる状態であり、欧州の顧客 940 万人がサイバー攻撃の影響を受けた可能性があった。ICO によると、これにより、名前、カード番号、同社サイトのユーザー名とパスワード、有効期限、カード検証値（CVV）番号などの個人データが影響を受けたとされている。また、バークレイズ銀行の顧客が所有する 6 万枚の支払い用カードが不正行為の対象となったことが判明している。さらに、同社に対して、複数の国際銀行から不正行為が報告されている。ICO は、同社に対して、セキュリティ対策義務違反があったとして、125 万ポンドの制裁金を課した。			

（4）内閣府（Cabinet Office）

表 3-4 の通り、内閣府は、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ていなかったため、ICO により、50 万ポンドの制裁金を課せられた。

表 3-4：制裁金決定事例 4（内閣府）

2021 年 12 月 2 日	50 万ポンド (約 7,979 万円)	内閣府	5 条 1 項 f), 32 条
2019 年 12 月 27 日、内閣府は、新年の栄誉賞リストで発表された 1,000 人以上の人々の名前と修正されていない住所を含むファイルを英国政府サイトで公開した。英国国内の幅広い職業の人々が影響を受け、その中には世間的な知名度の高い個人も含まれていた。内閣府は、データ流出に気づいた後、ファイルへのウェブリンクを削除したものの、ファイルは依然としてキャッシュされており、正確なウェブページのアドレスを知っている者はオンラインでアクセスすることができる状態にあった。そのため、当該個人データは、2 時間 21 分にわたってオンラインで公開され、3,872 回のアクセスを受けた。データが公開されていたため、ICO は、被害を受けた個人から情報漏えいにより個人の安全性が懸念されるという 3 件の内容の苦情を受け、内閣府にも同様の懸念を持つ 27 件の連絡があった。そのため、ICO は、2020 年の新年の栄誉賞受賞者の郵便物の住所をオンラインで開示したとして、内閣府に対して、50 万ポンドの制裁金を課した。			

7. UK GDPR 改正案

英国のデジタル・文化・メディア・スポーツ省（Department for Digital, Culture, Media and Sport、以下「DCMS」という）は、2021 年 9 月 10 日、「Data: A new direction」という UK GDPR の改正案に関する文書[15]を公表した。DCMS による UK GDPR 改正案のうち代表的なものは、表 4 の通りである。

[15] United Kingdom, Department for Digital, Culture Media & Sport, Data: A new direction (10 September 2021) (available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document__Accessible_.pdf)以下、当該リンク先については、「**DCMS コンサルテーション**」といい、パラグラフごとに、「**DCMS コンサルテーション・パラグラフ**」という形で参照先を言及する。

表 4：UK GDPR 改正案の概要

分野	UK GDPR 改正案（DCMS “Data: A new direction”）の例
研究およびデータの再利用	■ 研究に関連する GDPR および DPA の法的規定をすべてまとめ、読みやすくする。 ■ 科学的研究の定義を法律に盛り込む（現在は GDPR の前文にあり、解釈の助けとなっている）。 ■ 大学が 6 条の公共の利益の条件に頼ることができる場合を明確にする。 ■ 6 条の研究に関する新たな法的根拠を設ける。 ■ 研究目的のための広範な同意を許容する。 ■ 二次加工の目的が当初の目的と両立しないかどうかを評価する方法の変更。 ■ プライバシー通知に関する「不相応な労力」の場合の例外的な免除規定を 14 条だけでなく 13 条にも適用する。
正当な利益	正当な利益の評価「ホワイトリスト」を作成しどのような場合に利益が正当であるとみなされ比較衡量のテストが必要でないかを説明する。
説明責任	■ コンプライアンス要件として「プライバシー管理プログラム」を導入すること。 ■ データ保護責任者の要件を、プライバシー管理プログラムに責任を持つ適切な個人の要件に変更すること。 ■ データ保護影響評価を廃止し、プライバシーリスクを評価するための独自のアプローチを組織が選択できるようにすること。 ■ 処理活動の記録を、プライバシー管理プログラムの一環として、個人データのインベントリに置き換える。 ■ ICO へのデータ違反報告の閾値を引き上げる。
データ移転	■ 必要に応じて組織が独自のメカニズムを特定できるようにするなど、代替となる移転メカニズムを導入する。 ■ 反復的な移転に対する 49 条の例外規定の使用を拡大する。 ■ 認証メカニズムの使用を奨励する。
AI・機械学習	■ 公平性の概念がこの分野にどのように適用されるのか、意見を募集する。 ■ バイアスの監視と修正を正当な利益評価のホワイトリストに追加する。 ■ DPA 2018 の Schedule 1 を改正し、バイアスモニタリングのためのセンシティブな個人データの処理を明示的に許可する。 ■ 自動化された決定に対する人間によるレビュー：22 条を削除するか、その適用を明確にする可能性 ■ データ仲介者を支援する。 ■ UK GDPR の本文に前文 26 項を組み込み、匿名化は管理者がデータ主体を特定できる合理的な可能性に基づいて評価すべきであることを明記する。 ■ 公共データを使用して処理する公共サービスが使用するアルゴリズムの透明性報告を義務付ける。
データ主体の権利	■ データ主体のアクセス要求規定を修正し、情報公開法をモデルとしたコスト制限を導入する。
電子プライバシー	■ 分析用クッキーおよびその他の「低リスク」トラッカーについては、同意は必要ない。 ■ クッキーへの同意の疲労を軽減する方法について意見を求める。 ■ ソフトオプトインを非営利団体に拡大し、政党をプライバシー・電子通信規則から完全に除外する可能性
ICO の改革	■ 管理者は、苦情処理プロセスを導入しなければならない。 ■ ICO への追加権限：技術報告書の提出、証人の強制など ■ 制裁通知の発行期限を、意図的な通知から 6 カ月後から 12 カ月後に延長 ■ ICO の調査中、当事者が必要な情報を提供しない場合、期限を一時的に停止する Stop the clock メカニズムを導入する。 ■ ICO は、調査開始時に、関連するデータ管理者に対して、調査の各段階のタイムラインを提示する。

これに対して、ICO は、2021 年 10 月 6 日、「Response to DCMS consultation “Data: a new direction”」という DCMS のパブリックコンサルテーションに対応した回答の文書[16]を公表した。

以上のように UK GDPR については大改正が行われる現実的な可能性が浮上している。本ハンドブックでは、現行の UK GDPR のルールに関する解説を行うとともに、組織による UK GDPR コンプライアンス対応との関係で重要と思われる点との関係では、DCMS による改正案の要点およびそれに対する ICO のスタンスを関連する箇所において示す。

[16] ICO, Response to DCMS consultation “Data: a new direction” (https://ico.org.uk/media/about-the-ico/consultation-responses/4018588/dcms-consultation-response-20211006.pdf)

II. 組織が遵守しなければならない UK GDPR の規制

組織が遵守しなければならない UK GDPR の規制の内容は以下の通りである。

1. データ処理に関する原則を遵守する義務（5 条）

（1）個人データ処理の諸原則と説明責任の原則

管理者は、以下の表 5 に列記した個人データ処理の原則の遵守に責任を負い、その遵守を証明できる必要がある（説明責任の原則）。組織として UK GDPR 対応を取るにあたっては、常に ICO に対する説明責任をどのように果たすかという観点から方針を決めていくことが望ましい。

表 5：個人データ処理の諸原則

原則	内容
適法性、公正性および透明性	適法、公平かつ透明性のある方法で処理すること（5 条 1 項(a)）
目的の限定	特定的で、明確、かつ正当な理由のために収集され、それらの目的にそぐわない方法でそれ以上の処理を行わないこと（5 条 1 項(b)）[17]
データの最小化	処理を行う目的に関し、十分で関連性があり必要最小限に限定されていること（5 条 1 項(c)）
正確性	正確で、必要であれば常に最新状態に更新しておくこと。不正確な個人データは遅滞なく削除または訂正すること（5 条 1 項(d)）
保管の限定	処理の目的に必要な期間以上、データ主体の識別可能な状態で保管をしないこと（5 条 1 項(e)）
完全性と機密性	不正または違法な処理からの保護、不慮の損失、破壊、損失からの保護を含み、個人データの適切なセキュリティが確保される形で処理すること（5 条 1 項(f)）

（2）適法性、公正性、透明性の原則とは

個人データは、データ主体に関連して、適法に、公正に、かつ透明性のある方法で処理する必要がある（適法性、公正性、透明性）[18]。6 条から 10 条には、適法性と「処理のための法的根拠」についてより詳細な規定がある。また、13 条および 14 条には、「情報を提供される権利」の一部として、より詳細な透明性の義務が定められている。適法性、公正性、透明性の 3 つの要素は重複しているが、3 つ全てを満たすようにしなければならない。関係者にとって根本的に不公正であったり、関係者から隠されていたりする場合は、処理が適法であることを示すだけでは不十分である。

---

[17] 当初収集した目的と異なる目的で、個人データを処理するためには、当該別の目的のための処理がその個人データが当初収集された目的と適合することが必要とされている（6 条 4 項）。もっとも、個人データの収集時には、明確に全ての処理目的を特定することができない場合があり、常に、厳格に当該要件の遵守を求めることは、収集時の個人データの利用目的・方法の不確実性の高い分野において、データの利活用を阻害してしまうと考えられる。上記のような二次的な処理の目的に関し、DCMS のコンサルテーションで、不確実性の高い 3 つの主要な分野を特定し、二次的な処理の目的が当初の目的と両立しないかどうかを評価する方法の変更旨の提案がされている（DCMS コンサルテーション・パラグラフ 54）。

[18] ICO, Guide to the General Data Protection Regulation (GDPR), Principle (a): Lawfulness, fairness and transparency (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/lawfulness-fairness-and-transparency/).

(3) 適法性とは

個人データの処理が適法であるためには、処理を行う具体的な理由を特定する必要がある[19]。これは個人データの処理の**法的根拠（legal basis）**と呼ばれ、目的やデータ主体との関係に応じて 6 つの選択肢があり、UK GDPR6 条に規定されている。また、センシティブデータ（特別カテゴリの個人データ）を処理するための特定の追加条件もあり、UK GDPR9 条に規定されている。法的根拠がない場合、その処理は違法であり、適法性の原則に違反することになる。

適法性とは、より一般的な意味で、違法となる個人データの処理をしないことも意味する。これには、刑事上または民事上の法令およびコモンロー上の義務が含まれる。処理が犯罪行為に関わる場合は、明らかに違法である。さらに、以下に該当する場合は、処理が違法となる可能性がある。

- 信義則上の義務に違反した場合
- 組織が法的権限を超えた場合、またはその権限を不適切に行使した場合
- 著作権の侵害
- 強制力のある契約上の合意に違反する場合
- 業界固有の法律または規制の違反
- 1998 年人権法への違反

上のリストは例であり網羅的なものではない。個人データを違法に処理した場合、UK GDPR では、データ主体がそのデータを消去したり、その処理を制限することを要求する権利が与えられている。

(4) 公正性とは

個人データの処理は、適法であると同時に、常に公正である必要がある[20]。たとえ処理に法的根拠があることを示すことができたとしても、処理のいずれかの側面が不公正であれば、この原則に違反していることになる。一般的に、**公正**とは、データ主体が合理的に期待する方法でのみ個人データを処理し、データ主体に不当な悪影響を与える方法で個人データを使用してはならないということである。個人データをどのように処理できるかだけでなく、処理すべきかどうかについても考える必要がある[21]。

個人データを公正に処理しているかどうかの評価は、個人データの入手方法にも左右される。特に、個人データを取得する際にデータ主体を騙したり、誤解させたりした場合は、公正とは言えない。個人データを公正に処理しているかどうかを評価するためには、データ主体（グループおよび個人）の利益にどのように影響するかを、より一般的に考慮する必要がある。個人データを取得して処理する際に、当該個人データに関連するほとん

[19] 前掲・注 16
[20] 前掲・注 16
[21] AI 技術との関係で、特に、公正性の原則につき、DCMS のパブリックコンサルテーションの中で、取り上げられており、公正性の概念がこの分野にどのように適用されるのか、意見を募集する旨の提案がなされており、留意すべきである（DCMS コンサルテーション・パラグラフ 80）。DCMS からは具体的な提案があるわけではなく、意見募集を行っている状況にあるが、ICO が示した公正性の概念の適用に関する考え方は DCMS が念頭においているそれと異なるものと考えられ、改正法の内容は不透明であると考えられる。

どのデータ主体に対しては公正に行っているが、あるデータ主体に対しては不当に行っている場合でも、公正性の原則に違反していることになる。

個人データは、必ずしも不公正でなくても、データ主体に不利益という悪影響を与える方法で処理されることがある。重要なのは、そのような不利益が正当化されるかどうかである。

例えば、納税義務を評価するために個人データを収集したり、制限速度を破ったとして罰金を科したりする場合、個人データは関係するデータ主体に不利益をもたらす方法で処理されているが、これらの目的のために個人データを適切に処理することは不公正ではない。

また、データ主体が自分の個人データに関する権利を行使しようとするときには、公平に扱うようにする必要がある。これは、データ主体の権利の行使を促進する義務と関連している。

(5) 透明性とは何か

透明性は、基本的に公正さと関連している[22]。**透明性のある処理**とは、管理者が何者であるか、そして個人データをどのように、またなぜ処理するかについて、最初から明確で、オープンで、正直であることである。透明性は常に重要であるが、特にデータ主体が管理者との関係を希望するかどうかを選択できる状況では重要である。データ主体は、管理者が自らの個人データを何に使うかを最初に知っていれば、関係を形成するかどうか、あるいは関係の条件を再交渉しようとするかどうかについて、十分な情報を得た上で判断することができる。

透明性は、データ主体との直接的な関係がなく、別の情報源から個人データを収集する場合にも重要である。場合によってはさらに重要になることもある。なぜなら、データ主体は、管理者が自分の個人データを収集して処理していることを知らないかもしれず、そのことが、データ主体が自らの個人データに対する権利を主張する能力に影響するためである。管理者は、簡単にアクセスでき、理解しやすい方法で、自らによる処理についてデータ主体に伝えることを保証する必要がある。すなわち、明確でわかりやすい言葉を使う必要があるということである。

2. 適法に個人データを処理する義務（6 条）

(1) 法的根拠の種類

管理者が個人データの処理を行う場合には、各処理行為について、以下の表 6 のいずれの法的根拠に基づいて処理行為を行うかについて分析を行い、適切な法的根拠を選択する必要がある[23]。

---

[22] 前掲・注 16

[23] 研究目的の個人データの処理の場合、「公共の利益」を法的根拠とされることが多いものの、同意等他の法的根拠に基づく場合もある。研究目的の処理との関係では、法的根拠に関するいずれの規定も適用関係が不明確な部分があり、適法なデータ処理に該当するか否かの判断が難しく、研究の促進を阻害している面があった。そのため、DCMS のコンサルテーションにおいて、研究に関連する UK GDPR および DPA の法的規定をすべてまとめ、読みやすくする旨の提案（DCMS コンサルテーション・パラグラフ

表 6：処理行為の法的根拠

法的根拠	要件
同意（6 条 1 項(a)）	データ主体が、1 つまたは複数の特定の目的について、自己の個人データが処理されることに同意した場合
契約の履行（6 条 1 項(b)）	データ主体が当事者となっている契約の実行のため、または、データ主体の要求により契約締結前の手続を実行するために処理が必要である場合
法的義務の遵守（6 条 1 項(c)）	管理者が負う英国法上の法的義務を遵守するために必要である場合
重大な利益の保護（6 条 1 項(d)）	データ主体、または他の自然人の重大な利益を保護するために必要である場合
公共の利益（6 条 1 項(e)）	公共の利益、あるいは管理者に属する公的権限の行使として実行する業務遂行のために必要である場合
正当な利益（6 条 1 項(f)）	データ処理が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。ただし、そのような利益が、データ主体の利益または基本的権利および自由に優先される場合、特にデータ主体が子どもである場合を除く

(2) 正当な利益の判断基準

「正当な利益（legitimate Interest）」は、3 つのテストに分けられる[24]。

① 目的のテスト：「正当な利益」を追求しているか。

② 必要性のテスト：その目的のために処理が必要か。

③ 比較衡量のテスト：個人の利益が正当な利益を上回るか。

【テスト①：目的のテスト：「正当な利益」を追求しているか】

まず、幅広い利益が正当な利益として認められる。これには、顧客自身の利益、第三者の利益、商業的利益、より広い社会的利益が含まれる。これらの利益は、やむを得ないものであったり、些細なものであったりするが、些細な利益は比較衡量のテストでより簡単に覆される可能性がある。UK GDPR の下では潜在的な正当な利益として、顧客または従業員データの使用、マーケティング、不正防止、グループ内移転、または IT セキュリティが具体的に挙げられるが、これらは網羅的なリストではない。また、犯罪行為の可能性やセキュリティ上の脅威に関する情報を規制当局に開示することも正当な利益である。

【テスト②：必要性のテスト：その目的のために処理が必要か】

次に、**「必要」**とは、処理が目的を達成するための的を射た適切な方法である必要があることを意味する。同じ目的を達成するために、他に合理的でより侵害性の低い方法がある場合、正当な利益に依拠することはできない。

【テスト③：比較衡量のテスト：個人の利益が正当な利益を上回るか】

---

40)、科学的研究の定義を法律に盛り込む旨の提案（DCMS コンサルテーション・パラグラフ 42)、6 条の研究に関する新たな法的根拠を設ける旨の提案（DCMS コンサルテーション・パラグラフ 44)、研究目的のための広範な同意を許容する旨の提案（DCMS コンサルテーション・パラグラフ 48）を行っている。

[24] ICO, Guide to the General Data Protection Regulation (GDPR), Legitimate interests (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/).

さらに、管理者の利益とデータ主体の利益のバランスを取る必要がある。特に、データ主体が、管理者がそのようにデータを使用することを合理的に期待していない場合や、データ主体に対し不当に損害を与える場合は、データ主体の利益が管理者の利益を上回る可能性が高い。しかし、管理者の利益は必ずしもデータ主体の利益と一致する必要はない。相反する場合であっても、データ主体への影響を明確に正当化する理由があれば、管理者の利益を優先することができる。

(3) 正当な利益に依拠できる場面－どのような場合に正当な利益に依拠できるか？

正当な利益は最も柔軟な法的根拠であるが、すべての処理に対して常に適切であると仮定することはできない[25]。正当な利益に依拠することを選択すると、人々の権利と利益が十分に考慮され保護されていることを保証するための特別な責任を負うことになる。正当な利益は、データ主体が合理的に期待する方法で個人データを使用し、プライバシーへの影響が最小限である場合に、最も適切な法的根拠となる可能性がある。データ主体への影響がある場合でも、その処理により説得的な利益があり、当該影響が正当化されることを示すことができれば、正当な利益が認められる場合がある。

データ主体の個人データの処理方法が適切で、プライバシーへの影響が最小限であり、データ主体が驚いたり異議を唱えたりすることがないことを示すことができれば、マーケティング活動のために正当な利益に依拠することができる。ただし、英国のプライバシー・電子通信規則に基づく同意が不要な場合に限る。

子どもの個人データを処理する際には、法的根拠として正当な利益を検討することができるが、子どもの利益が保護されていることを確認するために特別な注意を払う必要がある。

個人データを第三者に適法に開示するために、正当な利益に依拠することができる場合がある。第三者が情報を必要とする理由、実際に必要かどうか、そして当該情報を使って何をするのかを検討する必要がある。管理者は開示が正当化されることを証明する必要があるが、自らの処理についての法的根拠を決定するのは第三者の責任となる。

データ主体が理解できず、合理的に期待できない方法で個人データを処理している場合や、当該方法についてデータ主体に説明すると反対すると考えられる場合は、正当な利益の法的根拠としての使用を避けるべきである。また、データ主体に被害をもたらす可能性のある処理については、その影響を正当化するやむを得ない理由があると確信できる場合を除き、正当な利益という法的根拠の使用を避けるべきである。

管理者が公的機関である場合、公的機関としての業務を遂行するために行うあらゆる個人データの処理について、正当な利益に依拠することはできない。しかし、公共機関としての業務の範囲外に他の正当な目的がある場合は、必要に応じて正当な利益を考慮することができる。これは商業的利益を有する公的機関に特に関連する。

[25] 前掲・注 22

（4）正当な利益の法的根拠に関する DCMS のコンサルテーション

上記の「正当な利益」の判断に関し、DCMS のコンサルテーションで、比較衡量のテストを適用せず、ホワイトリストを作成する旨の提案[26]、AI システムに関する偏りの監視、検出、修正を確実に行う目的で個人データを処理することを当該ホワイトリストに追加する旨の提案[27]、および、DPA 2018 の Schedule 1 において、偏りの監視、検出、修正がセンシティブな個人データを使用しなければ実施できない場合、必要なセンシティブ個人情報の処理を明示的に許可する旨の提案[28]がなされている。ICO は、いずれの DCMS の提案にも、概ね賛成しており、改正法に含まれる可能性が高いと考えられる。

3. 同意の条件を遵守する義務（7 条）

データ主体の同意とは、自由に与えられた、特定性のある、情報提供がなされた、不明瞭ではないデータ主体の意思表示によって、データ主体が陳述または明確な積極的行動により同意を示すことを意味する（4 条 11 号）。同意を取得する場合には、上記の定義から導かれる要素やその他の様々な条件を遵守する必要がある。管理者は、データ主体が同意したことについて証明できなければならず（7 条 1 項）、データ主体は同意をいつでも撤回することが可能である（7 条 3 項）。このように同意の有効性については厳格な条件が定められている。

（1）なぜ同意が重要なのか

UK GDPR は同意について高い基準を設けている[29]。同意は、曖昧さがなく、明確な肯定的行動（オプトイン）を伴うものである必要がある。特に、事前にチェックしたオプトインボックスを禁止している。また、個別の処理業務に対しては、個別の粒度の高い同意の選択肢を要求している。同意は、他の条件とは別に設定されるべきであり、一般的にサービスへの登録の前提条件とすべきではない。また、同意を証明するために、明確な記録を残す必要がある。

UK GDPR では、同意を撤回する特定の権利が与えられている。同意を撤回する権利についてデータ主体に伝え、いつでも同意を撤回する簡単な方法を提供する必要がある。

公的機関、雇用者、その他権力を持つ立場の組織は、自由に与えられた有効な同意を示すことがより困難になる可能性がある。既存の同意と同意の仕組みを見直し、UK GDPR の基準を満たしているかどうかを確認する必要がある。この基準を満たしていれば、新たな同意を得る必要はない。

また、明示的な同意は、特別カテゴリの個人データの処理を正当化することもできる。また、明示的な同意は、自動化された意思決定や個人データの国外移転を正当化することができる。

---

[26] DCMS コンサルテーション・パラグラフ 60
[27] DCMS コンサルテーション・パラグラフ 90
[28] DCMS コンサルテーション・パラグラフ 91
[29] ICO, Guide to the General Data Protection Regulation (GDPR), Consent (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).

真の同意は、データ主体にコントロールを与え、信頼と関与を築き、企業の評判を高めるものである。不適切または無効な同意に頼ると、信頼を失い、企業の評判を落とし、多額の制裁金を課せられる可能性がある。

(2) どのような場合に同意が適切か

データ主体の同意は、個人データの処理の法的根拠の一つであるが、それに代わる法的根拠もある[30]。同意は、これらの代替的な法的根拠よりも本質的に優れているわけでも、重要であるわけでもない。同意に依拠することが難しい場合は、代替的な法的根拠の使用を検討すべきである。

同意は、個人データの使用方法についてデータ主体に真の選択とコントロールを提供でき、データ主体の信頼と関与を構築したい場合に適切である。しかし、真の選択肢を提供できない場合、同意は適切ではない。同意がなくても個人データを処理するのであれば、同意を求めることは誤解を招きやすく、本質的に不公正である。同意をサービスの前提条件としている場合、同意が最も適切な法的根拠であるとはいえない。公的機関、雇用者、その他データ主体に対して力のある立場にある組織は、同意が自由に与えられたものであることを証明できる自信がない限り、同意に依拠することは避けるべきである。

(3) 有効な同意とは

- 同意は自由に与えられたものである必要がある[31]。これは、管理者がデータ主体のデータをどのように使用するかについて、データ主体に真の継続的な選択と管理を与えることを意味する。同意は明瞭であり、オプトインするための積極的な行動を必要とする。同意の要請は、目立つように、他の条件から切り離され、簡潔で理解しやすく、ユーザーフレンドリーである必要がある。
- 同意は、管理者の名前、処理の目的、処理活動の種類を具体的にカバーするものである必要がある。明示的な同意は、他の積極的な行動ではなく、言葉で明示的に確認する必要がある。
- 同意には一定の期限はない。同意がいつまで続くかは、状況によって異なる。適切に同意を見直し、更新する必要がある。

(4) 同意の取得、記録、管理はどのように行うべきか

- 同意の要請は、目立つように、簡潔に、他の条件とは別に、理解しやすいようにする必要があり、以下を含めることが求められる[32]。
    - 管理者の名称
    - 同意に依拠する第三者である管理者の名称
    - 個人データを取得する理由
    - 当該データをどのように使用するのか
    - 個人がいつでも同意を撤回できること。

[30] 前掲・注 27
[31] 前掲・注 27
[32] 前掲・注 27

- 管理者は、データ主体に積極的に同意を求める必要がある。事前にチェックされたボックスやオプトアウトボックス、その他のデフォルト設定は使用してはならない。可能な限り、異なる目的および異なる種類の処理に同意するための個別の（粒度の高い）オプションを提供する必要がある。
- 誰が、いつ、どのように、何を言われて同意したかなど、同意を証明する記録を残す。
- いつでも簡単に同意を取り消すことができるようにする。プリファレンス管理ツールの使用を検討する。
- 同意を常に見直し、変更があれば更新する。定期的な同意の見直しを業務プロセスに組み込む。

4. 特別カテゴリの個人データの処理の条件を遵守する義務（9 条）

人種的もしくは民族的出自、政治的意見、宗教上もしくは思想上の信条、または、労働組合への加入を明らかにする個人データの処理、ならびに、遺伝子データ、自然人を一意に識別することを目的とする生体データ、健康に関するデータ、または、自然人の性生活もしくは性的指向に関するデータ、すなわち**特別カテゴリの個人データ**の処理は、原則として禁止される（9 条 1 項）。特別カテゴリの個人データはデータ保護の観点から特にセンシティブなデータであるため、例外的に処理が認められる範囲が限定されている（データ主体の明示的同意等）。

（1）特別カテゴリの個人データとは何か

UK GDPR では、特別カテゴリの個人データを以下のように定義する[33]。

- 人種や民族の起源を明らかにする個人データ
- 政治的意見を明らかにする個人データ
- 宗教的または哲学的な信念を明らかにする個人データ
- 労働組合のメンバーであることを示す個人データ
- 遺伝的データ
- バイオメトリックデータ（本人確認を目的とする場合）
- 健康に関するデータ
- 個人の性生活に関するデータ
- 人の性的指向に関するデータ

犯罪の被疑事実、手続または有罪判決に関する個人データには、別のルールが適用されるため、これらの個人データは特別カテゴリの個人データには含まれない。特別カテゴリの個人データには、上記のカテゴリのデータを明らかにする、またはそれに関する個人データが含まれる。したがって、上記のカテゴリのいずれかに該当する誰かの詳細を推測した場合、当該データは特別カテゴリの個人データとしてカウントされる可能性がある。た

[33] ICO, Guide to the General Data Protection Regulation (GDPR), Special category data (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/).

だし、その推測がどの程度確かなものであるか、また、意図的にその推測を行ったかどうかによって異なる。

(2) 特別カテゴリの個人データに関するルールとは何か

- 管理者は、自らの処理が全般的に適法で、公正かつ透明性があり、UK GDPR の他のすべての原則および要件に準拠していることを常に確認する必要がある[34]。管理者の処理が適法であることを確保するためには、(通常の) 個人データの処理のための UK GDPR6 条の法的根拠を特定する必要がある。
- さらに、UK GDPR9 条の特定の条件の一つを満たすことができる場合にのみ、特別カテゴリの個人データを処理することができる。処理の目的を検討し、これらの条件のどれが関連するかを特定する必要がある。
- 処理の条件のうち 5 つは、UK GDPR9 条に規定されている。他の 5 つは、許認可または英国の法律における根拠を必要とするため、DPA 2018 に定められた追加条件を満たす必要がある。
- また、DPA 2018 に基づく適切なポリシー文書が必要かどうかを確認する必要がある。管理者のテンプレートである適切なポリシー文書には、この文書に含まれるべき情報の種類が示されている。
- リスクが高いと思われる処理の種類については、データ保護影響評価 (DPIA: Data Protection Impact Assessment) を行う必要がある。これは、特別カテゴリの個人データを処理するために DPIA を行う必要がある可能性が高いことを意味する。
- 特別カテゴリの個人データを処理する場合、当該データのカテゴリを文書化することを含め、記録を残す必要がある。また、特別カテゴリの個人データに関連するリスクが、他の義務 (特に、データの最小化、セキュリティ、透明性、データ保護責任者 (DPO: Data Protection Officer)、自動化された意思決定に関連する権利に関する義務) にどのように影響するかを検討する必要がある。

(3) 特別カテゴリの個人データを処理するための条件は何か

特別カテゴリの個人データを処理するための要件は、以下の通りである[35]。

(a) 明示的な同意
(b) 雇用、社会保障、社会保護 (法律で認められている場合)
(c) 重要な利益
(d) 非営利団体
(e) データ主体によって公開されたもの
(f) 法的請求または司法行為
(g) 実質的な公共の利益の理由 (法律上の根拠がある場合)
(h) 健康または社会的ケア (法律上の根拠があるもの)
(i) 公衆衛生 (法律上の根拠があるもの)

[34] 前掲・注 31
[35] 前掲・注 31

(j)　アーカイブ、研究、統計（法律上の根拠があるもの）の 10 通りである。

上記要件(b)、(h)、(i)または(j)に依拠している場合、DPA 2018 の Schedule 1 のパート 1 に記載されている英国法の関連条件も満たす必要がある。UK GDPR9 条 2 項(g)の実質的な公共の利益の理由という要件に依拠する場合は、DPA 2018 の Schedule 1 のパート 2 に記載された 23 の実質的な公共の利益の理由の要件[36]のいずれかを満たす必要もある[37]。

5. データ主体の権利およびその行使の手順を尊重する義務（12-22 条）

データ主体は、UK GDPR 上の要件を満たす場合には、以下の表 7 に列記した権利を有する。データ主体が権利行使を行った場合、管理者は原則として権利行使の要請を受けてから 1 カ月以内に対応しなければならない[38]。また、管理者は、データ主体の権利を尊重する義務があるため、データ主体の権利行使のための管理者における連絡先を個人データ保護方針等で明らかにしておく必要がある。管理者が原則として 1 カ月の時間制限に迅速に対応できるようにするためには、組織内でデータ主体の権利行使があった場合に関する内部の苦情対応手続を策定する必要がある。

表 7：データ主体の権利の内容

データ主体の権利	内容
通知を受ける権利（13 条、14 条）	自己に関する個人データの処理に関する情報を取得する権利
アクセス権（15 条）	管理者が自己に関する個人データの処理を行っているかの確認、ならびに当該個人データおよび一定の関連情報の開示を受ける権利
訂正権（16 条）	自己に関する不正確、または不完全な個人データについて訂正を求める権利
削除権（17 条）	自己に関する個人データの削除を受ける権利
制限権（18 条）	自己に関する個人データの処理に制限を加える権利
データポータビリティ権（20 条）	自己に関する個人データを、一般的な機械で読取り可能な形式で受領し、または他の管理者に送信させる権利
異議権（21 条）	自己に関する個人データの処理に異議を唱える権利

[36] 23 の実質的な公共の利益の理由の要件は、DPA 2018 の Schedule 1 の 6 項から 28 項に記載されており、以下に列記する通りである。
6. 法定および政府の目的、7. 司法の管理および議会の目的、8. 機会または待遇の平等、9. 上級職における人種・民族的多様性、10. 不法行為の防止・発見、11. 一般市民の保護、12. 規制要件、13. ジャーナリズム、学界、芸術、文学、14. 不正行為の防止、15. テロリストへの資金提供やマネーロンダリングの疑い、16. 特定の障害や病状を持つ個人へのサポート、17. カウンセリング、18. 子どもや危険にさらされている人の保護、19. 特定の個人の経済的幸福の保護、20. 保険、21. 職業的年金、22. 政党、23. 要請に応じる選出された代表者、24. 選出された代表者への開示、25. 選出された代表者への囚人に関する情報提供、26. 判決文の公開、27. スポーツにおけるアンチ・ドーピング、28. スポーツにおける行動の基準

[37] 前掲・注 31

[38] 上記アクセス権について、DCMS のコンサルテーションにおいて、データ主体のアクセス要請規定を修正し、情報公開法をモデルとしたコスト制限を導入する旨の提案（DCMS コンサルテーション・パラグラフ 188）、プロファイリング等の自動化された意思決定に関する権利について、UK GDPR22 条を削除するか、その適用範囲を明確化する可能性についての提案（DCMS コンサルテーション・パラグラフ 100）がされている。上記コスト制限の導入につき、データ管理者としては、データ主体による濫用的なアクセス権の行使を合理的な理由がある場合に適法に拒否することができるため、肯定的な面のある改正提案であると考えられる。ICO としても反対しておらず、改正法の内容に含まれる可能性が高い提案であると考える。これに対して、UK GDPR 22 条の削除の提案については、ICO は DCMS の提案に懸念を表明しており、改正法に含まれるかどうかは不透明であると考えられる。

自動化された意思決定に関する権利（22 条）	完全に自動化された意思決定の対象から除外される権利

なお、DCMS は、DCMS コンサルテーションにおいて、管理者に苦情処理プロセスを設けることを義務付ける旨の提案を行っている[39]。ICO は DCMS の提案に概ね賛成しており、改正法に含まれる可能性が高いと考えられる。

6. 情報通知義務（13、14 条）

（1）通知を受ける権利と情報通知義務の位置づけ

通知を受ける権利は、UK GDPR の主要な透明性要件の一部をカバーしている。これは、個人データをどのように処理するかについて、データ主体に明確で簡潔な情報を提供することである。13 条および 14 条では、データ主体がどのような情報を得る権利があるのかを規定しており、この情報は「**プライバシー情報**」と呼ばれている。通知を受ける権利に対応する義務を、**情報通知義務**といい、当該義務の遵守について効果的なアプローチを用いることで、UK GDPR の他の側面を遵守し、データ主体との信頼関係を育み、データ主体からより有益な情報を得ることができる。反対に、当該義務の遵守に失敗すると、制裁金を課せられたり、風評被害につながったりする可能性がある[40]。

（2）提供すべきプライバシー情報とは

以下の表 8 は、提供しなければならないプライバシー情報をまとめたものである。提供しなければならないプライバシー情報は、個人データをデータ主体から収集するか、他の情報源から取得するかによって若干異なる[41]。

表 8：提供すべきプライバシー情報

どのような情報を提供する必要があるか	データ主体から収集する個人データ	他の情報源から取得する個人データ
組織の名称および連絡先	✓	✓
組織の代表者の名称および連絡先	✓	✓
組織のデータ保護責任者の連絡先	✓	✓
処理の目的	✓	✓
処理の法的根拠	✓	✓
処理の正当な利益	✓	✓
取得した個人データの種類		✓
個人データの受領者または受領者の種類	✓	✓

[39] DCMS コンサルテーション・パラグラフ 386
[40] ICO, Guide to the General Data Protection Regulation (GDPR), Right to be informed (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/).
[41] 前掲・注 38

第三国または国際組織への個人データの移転の詳細	✓	✓
個人データの保持期間	✓	✓
処理に関して個人が利用可能な権利	✓	✓
同意の撤回権	✓	✓
監督当局に苦情申立てを行う権利	✓	✓
個人データの情報源		✓
個人が個人データを提供する法律上または契約上の義務に服するか否かの詳細	✓	
プロファイリングを含む自動的意思決定の存在の詳細	✓	✓

(3) いつプライバシー情報を提供すべきか

個人データを関連するデータ主体から収集する場合は、個人データを取得する時点でプライバシー情報を提供する必要がある。データ主体に関連するデータ主体以外の情報源から個人データを取得する場合、原則として、個人データを取得してから合理的な期間内に、遅くとも１カ月以内に、当該データ主体にプライバシー情報を提供する必要があり[42]、(a)個人情報を利用してデータ主体と連絡を取る場合は、遅くとも最初の連絡が行われた時点で、(b)他人に開示することを想定している場合は、遅くともデータを開示した時点で、それぞれ当該データ主体にプライバシー情報を提供する必要がある。

管理者は、プライバシー情報をデータ主体に積極的に提供する必要がある。管理者は、自社のウェブサイトにプライバシー情報を掲載することで当該要件を満たすことができるが、データ主体に当該プライバシー情報を認識させ、簡単にアクセスできる方法を提供する必要がある。

(4) 情報通知義務の例外

データ主体から個人データを収集する場合、データ主体がすでに持っている情報を提供する必要はない。他の情報源から個人データを取得する際、以下の場合は、データ主体にプライバシー情報を提供する必要はない[43]。

- データ主体が既に情報を持っている場合
- データ主体に情報を提供することが不可能な場合
- **データ主体に情報を提供することが不相応な労力を要する場合**
- データ主体に情報を提供することで、処理の目的を達成することが不可能になるか、著しく損なわれる場合
- 個人データの取得または開示が法律で義務付けられている場合

[42] 前掲・注 38
[43] 前掲・注 38

■ 個人データを対象とする法律で規制された職業上の秘密保持義務を負っている場合

上記の**データ主体に情報を提供することが不相応な労力を要する場合**という例外要件は、原則としてデータ主体から個人データを収集する場合には適用されない。DCMS は、DCMS コンサルテーションにおいて、データ主体から直接個人データを収集した管理者が、さらなる処理を行う前に、データ主体にさらなる情報を提供するという現行の要件を、さらなる処理が研究目的であり、そのために不相応な労力を要する場合には例外的に免除するという提案を行っている[44]。ICO は DCMS の提案に概ね賛成しており、改正法に含まれる可能性が高いと考えられる。

(5) プライバシー情報はどのように作成すべきか

データマッピングを行うことで、どのような個人データを保有し、それをどのように処理しているかを知ることができる。プライバシー情報のデータ主体を想定し、当該データ主体の立場に立って、プライバシー情報の作成方法について検討する必要がある。例えば、子どもの個人データを収集または取得する場合は、子どもに提供する情報が適切に記述され、明確で平易な言葉を使用するように特に注意する必要がある。

すべてのデータ主体に対して、以下のような方法で情報を提供する必要がある[45]。

- 簡潔であること
- 透明であること
- わかりやすいこと
- 容易にアクセス可能であること
- 明確で平易な言葉を使用していること

プライバシー情報を確定した後は、定期的に見直しを行い、正確で最新の情報を維持する必要がある。新たな目的で個人データを処理する場合には、プライバシー情報を更新し、変更点を積極的にデータ主体に知らせる必要がある。

(6) プライバシー情報の提供にはどのような方法があるか

プライバシー情報をデータ主体に提供するために使用できる方法には、以下のようなものがある[46]。

- **層構造のアプローチ（A layered approach）**：主要なプライバシー情報を含む短い通知に、より詳細な情報を追加する層を設ける。
- **ダッシュボード**：個人データをどのように使用しているかをデータ主体に知らせ、個人データで何が起こるかをデータ主体が管理できるようにするプリファレンス管理ツール
- **ジャストインタイム通知**：データ主体に関する個々の情報を収集する際に、関連性の高い、焦点を絞ったプライバシー情報を提供するもの
- **アイコン**：特定の種類のデータ処理の存在を示す小さくて意味のある記号

[44] DCMS コンサルテーション・パラグラフ 50
[45] 前掲・注 38
[46] 前掲・注 38

- **モバイルおよびスマートデバイスの機能**：ポップアップ、音声警告、モバイルデバイスのジェスチャーを含む。

個人データを収集する際には、その背景を考慮する必要がある。個人データの収集に使用するのと同じ媒体を使用して、プライバシー情報を通知することは望ましい慣行であると考えられる。

7. 個人データの移転の条件に従う義務（44-49 条）

（1）個人データの国外移転規制の概要

UK GDPR では、英国国外の国や国際組織への個人データの移転を制限している。当該制限は移転の規模や頻度にかかわらず、すべての移転に適用される。2021 年 6 月 28 日、欧州委員会は、EU GDPR および法執行指令に基づく英国の十分性に関する決定を採択し、欧州委員会は英国の十分性が認められると判断した。これにより、ほとんどの個人データは、追加の保護措置を必要とすることなく、EU および EEA から引き続き英国へ移転することができる。英国から EEA を含む他の国への移転が制限されている場合は、英国の制度に基づく国外移転規制が適用される。当該英国の国外移転規制は、EU GDPR をほぼ反映しているが、英国はこの枠組みを見直す独立性を有する。また、ブレグジット後の英国の新体制への移行をスムーズにするための移行措置も用意されている[47]。

まず、英国政府は、第三国や国際機関に関する独自の「十分性認定」を行う権限を有している。英国の体制では、これらは「**十分性ルール規則**」と呼ばれている。また、2020 年 12 月 31 日時点で有効な EU の標準的契約条項（SCC: Standard Contractual Clauses）を、既存の制限付き移転と新規の制限付き移転の両方で継続して使用することを認める規定もある。最後に、EU の拘束的企業準則（BCR: Binding Corporate Rules）を英国の制度に移行させるための規定がある[48]。

すなわち、UK GDPR においては、個人データを英国および後述の十分性認定を受けている国以外の第三国に移転すること（「**制限付き移転**」）は原則として禁止されているが、適切な保護措置（例：SCC、BCR 等）（46 条）が提供され、または法令上の例外（49 条）に該当する場合には、例外的に個人データの移転が認められる。UK GDPR は 5 章の 44 条から 50 条において、制限付き移転の場合に関する規定を置いている。条文構造としては、EU GDPR 同様、個人データの英国国外への移転につき、原則禁止（44 条、前文 101）とした上で、以下の通り、45 条以降で当該国外移転が例外的に許される場合について規定している。

- 十分性認定による移転（45 条）
- 標準データ保護条項（SDPC: Standard Data Protection Clauses）による移転（46 条 2 項(c)）

---

[47] ICO, Guide to the General Data Protection Regulation (GDPR), International transfers after the UK exit from the EU Implementation Period (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/).

[48] 前掲・注 45

- 拘束的企業準則（BCR: Binding Corporate Rules）による移転（46 条 2 項(b)、47 条）
- 行動規範による移転（46 条 2 項(e)）
- 承認された認証メカニズムによる移転（46 条 2 項(f)）
- データ主体による同意による移転（49 条 1 項(a)）
- 同意以外の特定の状況における例外（49 条 1 項(b)-(g)）による移転

以下、各例外のうち十分性認定による移転、標準データ保護条項（SDPC）による移転、拘束的企業準則（BCR）による移転について解説する。

（2）十分性認定による移転（45 条）

十分性認定による移転とは、UK GDPR の十分性ルール規則に基づき認められた第三国または国際組織への移転（45 条 1 項）をいう。すなわち、個人データについて、英国法で十分性が認められた国・地域との関係では、英国国外への個人データの移転を自由に行えることとするものである。したがって、英国から EEA および 2020 年 12 月 31 日時点で欧州委員会の十分性認定の対象となっている、以下の表 9 に列記した国[49]への個人データの移転は、英国の国外移転規制の下でも十分性認定に基づいて適法に行うことができることが UK GDPR 上認められている。

表 9：十分性が認められている国

国名		
アンドラ	アルゼンチン	カナダ（連邦政府、地方政府および関連公的機関などを除く）
フェロー諸島	ガーンジー（英国領）	イスラエル
マン島（英国領）	日本（公的部門は対象外）	ジャージー（英国領）
ニュージーランド	スイス	ウルグアイ

英国政府のデータ戦略としては、ニュージーランドの十分性認定について造詣が深いジョン・エドワーズ氏を 2022 年 1 月 4 日に新しい情報コミッショナーとして迎え、EU による英国の十分性認定（4 年間の有効期限付き）の有効性の維持を目指しつつ、2021 年 8 月 26 日に DCMS が公表した「UK approach to international data transfers」[50]に示した通り、米国・インド・韓国・シンガポール・インドネシア・オーストラリア・ブラジル・コロンビア・ドバイ国際金融センター・ケニアを十分性認定の審査の優先順位のトップに位置付け、英国を中心としたデータ自由流通の戦略を描いているものと考えられる。

[49] European Commission, Adequacy decisions, (available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en).
[50] ICO, Guidance, UK approach to international data transfers (26 August 2021) (available at https://www.gov.uk/government/publications/uk-approach-to-international-data-transfers).

（3）標準データ保護条項（SDPC）による移転（46 条 2 項(c)）

① 概要

組織（データ輸出者）とデータ輸入者が、英国のデータ保護制度に従って認識または発行された標準データ保護条項（SDPC）を組み込んだ契約を締結している場合は、制限付き移転を行うことができる。

これらは EU GDPR との関係では、「標準的契約条項」（「**SCC**」または「**モデル条項**」）として知られている。EU SCC には、送信者（データ輸出者）および受信者（データ輸入者）の契約上の義務と、個人データが移転されたデータ主体の権利が規定されている。データ主体は、これらの権利を EU SCC 上のデータ輸入者およびデータ輸出者に対して直接行使することができることとなる。

移行期間の終了前に締結された EU SCC は、英国の制度下での制限付き移転に対して引き続き有効である。新規の制限付き移転については、（移行期間終了時に有効であった）EU SCC（後述の通り**旧 EU SCC** と呼ぶべきものである）を引き続き使用することができる。制限付き移転のための標準契約条項（旧 EU SCC）は、管理者と管理者の間では 2 セット、管理者と処理者の間では 1 セットある[51]。管理者から他の管理者への制限付き移転を行う場合、管理者は自身の事業上の取決めに最も適したものに応じて使用する条項のセットを選択することができる。

2021 年 6 月 4 日、欧州委員会が、「第三国への個人データ移転のための SCC に関する決定」[52]を公表し、当該 SCC に関する欧州委員会決定の一部である APPENDIX として SCC の改定版[53]（「**改定版 EU SCC**」）が添付されている[54]。したがって、改定版 EU SCC とは区別される標準データ保護条項として、**旧 EU SCC** が存在することに注意が必要である。

---

[51] ICO のウェブサイトでは、UK GDPR の下で引き続き使用可能な旧 EU SCC が列記されている。
- 2001 controller to controller
- 2004 controller to controller
- 2010 controller to processor

[52] European Commission, COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (available at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en)

[53] European Commission, Annex to the COMMISSION IMPLEMENTING DECISION on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (available at https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf)

[54] 従前は、管理者から管理者への移転について 2 種類の 旧 EU SCC、管理者から処理者への移転について 1 種類の 旧 EU SCC のみであったのに対して、改定版 EU SCC では、一般条項に加えて、具体的なデータ移転の状況に応じて、4 つのモジュールの契約条項のうち該当するものを選択することが求められる（モジュール 1「管理者から管理者への移転」、モジュール 2「管理者から処理者への移転」、モジュール 3「処理者から処理者への移転」、モジュール 4「処理者から管理者への移転」）。管理者からの移転に関するモジュール 1 および 2 の移転類型は、旧 EU SCC の枠組みにも対応するものであるが、処理者からの移転に関するモジュール 3 および 4 の移転類型は、改定版 EU SCC により初めて導入されたものである。締結済みの旧 EU SCC については 2022 年 12 月 27 日に廃止されるため、EU GDPR 対応としては、同日より前までに、改定版 EU SCC を締結するなどの対応をする必要がある。日本貿易振興機構（ジェトロ）「個人データの第三国への移転のための標準契約条項に関する 2021 年 6 月 4 日付欧州委員会実施決定（EU）2021/914（参考和訳）」（2021 年 10 月）（https://www.jetro.go.jp/ext_images/world/europe/eu/gdpr/pdf/scc_20210914.pdf）において参考和訳が公表されている。

ここで、改定版 EU SCC は、UK GDPR の下での標準データ保護条項（SDPC）として使用することはできないことに注意が必要である。

代わりに、旧 EU SCC の法的な意味を変えないことを条件に、旧 EU SCC を英国の文脈で意味をなすように変更することができる。例えば、EU GDPR から UK GDPR への変更、EU または EU 加盟国から英国への変更、監督当局から ICO への変更などが挙げられる[55]。それ以外の場合は、ビジネス関連の問題に関する保護条項や複数の条項を追加する場合を除き、旧 EU SCC に変更を加えてはならない。また、旧 EU SCC に拘束されることを条件に、当事者を追加すること（すなわち、データの輸入者またはデータ輸出者を追加すること）が可能である。

ICO は、2021 年 8 月、英国法上の SDPC に該当するものとして**国際データ移転契約書**（**IDTA**: International Data Transfer Agreement）のドラフトを公表し、また**移転リスク評価**（**TRA**: Transfer Risk Assessment）に関するガイダンスのドラフトも公表するとともに、両ドラフトについてパブリックコンサルテーションを行い、2021 年 10 月に終了した。

上記パブリックコンサルテーションに引き続き、英国国務長官は、2022 年 2 月 2 日、**国際データ移転契約書（IDTA）**[56]、**欧州委員会の国際データ移転に関する標準契約条項の補遺（Addendum）**[57]、および**経過措置を定めた文書**[58]の各文書を英国議会に提出した。当該各文書は DPA 2018 第 119 A 条に基づいて発行された[59]。

上記各文書に異議を述べる締切として設定された 2022 年 3 月 21 日までに英国議会から異議が出なかったため、上記各文書は、同日発効し、UK GDPR の適用を受けるデータ輸出者は、制限付き移転を行う際に、IDTA または補遺（Addendum）を、UK GDPR46 条を遵守するための移転ツールとして使用することができることとなった。IDTA および補遺（Addendum）は、今までの個人データの国外移転に関する旧 EU SCC に代わるものである。IDTA および補遺（Addendum）は一般に「Schrems II」と呼ばれている欧州連合司法裁判所の拘束力のある判決を考慮して作成されたものである。

---

[55] ICO による UK GDPR の下で制限付き移転を行う場合に、旧 EU SCC を使う際の改訂案も以下の通り ICO によって示されている。

- Controller to controller
- Controller to processor

[56] ICO が国際データ移転契約書（IDTA）として公表した文書のデータファイルは以下の通りである。

- International data transfer agreement (PDF)
- International data transfer agreement (Word document)

[57] ICO が欧州委員会の国際データ移転に関する標準契約条項の補遺（Addendum）として公表した文書のデータファイルは以下の通りである。

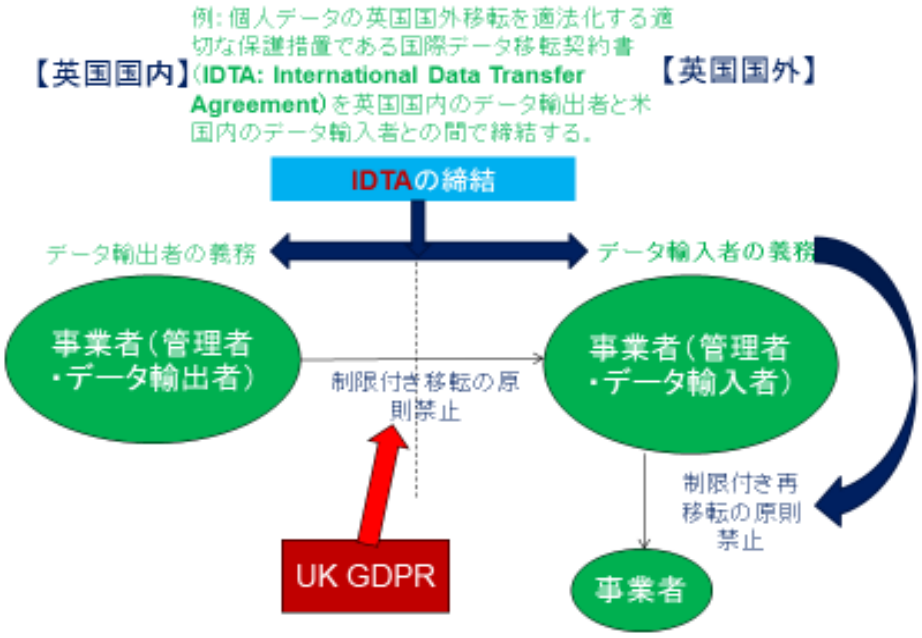
- International data transfer addendum to the European Commission's standard contractual clauses for international data transfers (PDF)
- International data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Word document)

[58] ICO が経過措置を定めた文書として公表した文書のデータファイルは以下の通りである。

- Transitional provisions

[59] ICO, International data transfer agreement and guidance (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/)

図 3：標準データ保護条項（SDPC）に該当する IDTA の締結に基づく個人データの英国国外への移転



IDTA は、英国において、旧 EU SCC に代わるものとして、個人データの英国国外への移転のために単体で用いることができるものである。これに対して、補遺（Addendum）は、改定版 EU SCC に修正を加えたうえで、実質的に IDTA を締結した場合と同じ効果を導くものである。具体的には、補遺（Addendum）において、改定版 EU SCC のモジュールおよび一部の条項（改定版 EU SCC の選択的条項であるドッキング条項等）を選択し、選択した改定版 EU SCC の各モジュールに対して、UK GDPR に合わせた修正（準拠法、監督当局等）を加えている。なお、選択した改定版 EU SCC と補遺（Addendum）の間に不整合がある場合には、改定版 EU SCC の方が強力なデータ主体に対する保護を与える場合を除いて、補遺（Addendum）の内容が優先する。

IDTA と補遺（Addendum）は、国際移転を支援するための英国の幅広いパッケージの一部を構成している。これには第三国の十分性評価に対する英国政府のアプローチを独自にサポートすることも含まれる。

ICO が公表した上記経過措置（Transitional provisions）に関する文書によれば、旧 EU SCC に基づいて 2021 年 9 月 21 日以前に締結された契約は、契約の主題である処理業務が変更されず、それらの条項に依拠することで個人データの移転が適切な保護措置の対象となることが保証されることを条件に、2024 年 3 月 21 日まで UK GDPR 46 条 1 項の目的のために適切な保護措置を提供し続けるものとするとされており、同日までに IDTA または補遺（Addendum）に基づく改定版 EU SCC を締結すればよいものと考えられる。

なお、EU GDPR の適用を受ける組織の多くは、EU GDPR の関係で、EU 域外である英国への個人データの国外移転の場合、十分性決定（2025 年 6 月 27 日まで有効[60]）に依拠して移転するか、改定版 EU SCC により対応することが想定される。念のため付言するが、上記補遺（Addendum）は、UK GDPR との関係で、英国国外への個人データの国外移転の場合のデータ輸出者が用いるツールであるため、EU GDPR 上の個人データの域外移転規制への対応のためには、使用することはできない。

また、UK GDPR の適用を受ける組織は UK GDPR との関係で、英国国外への個人データの国外移転の場合も、基本的には、IDTA で対応することが想定され、改定版 EU SCC および補遺（Addendum）が使用される場面は限られてくるとも考えられる。もっとも、EU GDPR および UK GDPR の適用を受ける組織（例えば、EU や英国のデータ主体に対してサービス提供を行っており、EU GDPR および UK GDPR の直接適用を受ける日本企業）が、データ輸出者として、EU 域外かつ英国国外の組織（例えば、米国や中国の子会社）に対して個人データを移転する場面において、EU GDPR との関係では、改定版 EU SCC の締結により対応するとともに、UK GDPR との関係では、別途 IDTA の締結をするのではなく補遺（Addendum）を使用することにより効率的に対応することが可能となり、このような場面では補遺（Addendum）を活用することが有益かつ便利であると考えられる。

なお、ICO によれば、以下の各文書を今後公表するとのことであるが、本レポートの基準日である 2022 年 3 月 27 日現在、これらはいずれも公表されていない[61]。

- IDTA および補遺に関する条項ごとのガイダンス（Clause by clause guidance to the IDTA and Addendum）
- IDTA の使用方法に関するガイダンス（Guidance on how to use the IDTA）
- 移転リスク評価に関するガイダンス（Guidance on transfer risk assessments）
- 国際移転に関するガイダンスの更なる明確化（Further clarifications on our international transfers guidance）

したがって、次の「②IDTA と TRA の概要」および「③IDTA の締結および TRA の実施の実務対応フロー」については、2022 年 3 月 21 日に発効した IDTA の内容（ただし、最終版の IDTA からは、ドラフト版にあったガイダンス・インストラクション部分は削除されている）を反映させたものであるものの、基本的には、2021 年 8 月に ICO が公表した文書の内容に基づくものである[62]。

---

[60] ICO, Overview – Data Protection and the EU (available at https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/overview-data-protection-and-the-eu/).

[61] 前掲・注 57

[62] 本稿執筆時点において、2022 年 3 月 21 日に発効した IDTA については ICO により公表されているものの（available at https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf）、IDTA および TRA のガイダンスの公表は未了である。そのため、IDTA に関する説明部分（表 11 および強制条項の具体的な条項に関する説明部分）を除き、「②　IDTA と TRA の概要」および「③　IDTA の締結および TRA の実施の実務対応フローについて」の説明は、2021 年 8 月から同年 10 月までの間、ICO によるパブリックコンサルテーションが実施された IDTA および TRA の各ドラフトの中に記載されていたガイダンス・インストラクション（使用方法の説明の記載）に基づいて記載している（ICO, ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of UK" (available at https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/)。そのため、今後、ICO が公表する上記各ガイダンスにより、内容がアップデートされる可能性があることに留意されたい。

② IDTA と TRA の概要

IDTA とは、UK GDPR の下で英国国内から英国国外の第三国への個人データの制限付き移転を適法化するものであり、特に IDTA の執行可能性および第三者のアクセスから生じるリスク（監視から生じる可能性のあるリスクを含む）の管理に関して、英国の法体系を支える主要な基準と十分に類似したあらゆる体制のための適切な保護措置の基準を提供するが、IDTA に依拠した移転の場合には、TRA が必要である。

TRA の目的は、制限された移転について、その制限された移転のすべての状況を考慮して、IDTA がデータ主体に対して、個人データが英国国内にあるときにデータ主体が有する関連する保護と十分に類似した保護を提供しているかどうかを確認することで、IDTA が単独で当該制限付き移転に対して適切な保護を提供しているのか、追加の措置や保護を講じる必要があるのか、別の移動手段を検討する必要があるかなどの判断を可能とすることである。

TRA における考慮事項は、①制限付き移転の具体的な事実、②移転先の国・地域に関する特定の事実、③移転によるデータ主体への潜在的な影響、およびデータ輸出者が特定するデータ主体への損害のリスクのグループに分けられる。

なお、英国による十分性認定を受けた国（EU、日本等）へ移転の場合、または 49 条の例外の一つに該当する場合には、TRA を実施する必要はない。

IDTA のドラフトに基づく IDTA の全体構造を表 10 に示す。

表 10：IDTA の全体構造

部	必要事項
第 1 部 表	表 1：当事者および署名、表 2：移転内容、表 3：移転されたデータ、表 4：セキュリティ要件 ■ 当事者の具体的な情報や移転制限についての詳細を記入する。 ■ テンプレートの表を用意しているが、必ずしも当該表を使う必要はない。 ■ IDTA に全ての関連情報が含まれていること、相互参照が正しいことを確認 ■ IDTA が効力を発するためには、両当事者が表 1 の契約書に署名または、署名に代替する手段により両当事者が拘束されることを確保する必要がある。
第 2 部 追加保護条項	■ データ輸出者が、移転データ保護のため必要と判断とした特別な保護措置についての条項（追加的保護条項）を追加する必要がある。 ■ 追加的保護条項の一部または全部を第 1 部表 4 のセキュリティ要件に記載することも可能
第 3 部 商業条項	■ 合意された商業条項を記載する。ひな型が用意されているが、リンク契約を締結する場合は当該ひな型を使用する必要なく、必ずしもひな型を使用する必要はない。 ■ 商業条項を使用しない場合、i)商業条項の欄に「商業条項は使用していない」と記載するか、ii)強制条項の中の商業条項への言及をすべて削除することで対応できる。
第 4 部 強制条項	■ 原則、全ての IDTA に、変更することなく完全な形で強制条項を記載する。 ■ ただし、以下のいずれかの場合は例外として、変更・削除等ができる。 ➢ 第 1 部ないし第 3 部で、同一のフォーマットを使用しない場合は、強制条項の文言を変更して、該当部分に関する情報に相互参照することができる。 ➢ データ輸出者が当事者間に適用されないことが明示されている条項を削除する。 ➢ IDTA に 2 以上の当事者がいる場合、複数当事者の契約として効力を有するように変更することができる。 ■ IDTA の保護レベルを不用意に下げてしまうと、制限付き移転が UK GDPR に違反する可能性があるため、強制条項の変更を行う際には、慎重に行う必要がある。

③　IDTA の締結および TRA の実施の実務対応フローについて

次に、UK GDPR の下で英国国内から英国国外の第三国への個人データの制限付き移転の適法化手段として、IDTA に依拠する場合、実際の IDTA の締結の実務対応フローについて解説する。

i）Step 1：英国国内所在者の個人データの移転フローを特定（IDTA 締結用データマッピングの実行）

英国の十分性認定によってカバーされない国・地域（EEA や日本以外の国々、例えば、米国や中国等）に所在する拠点との関係で IDTA の締結が必要となる。まずは、IDTA 第 1 部に対応する情報（表 11：IDTA 第 1 部表の記載の情報）の収集をする必要がある。

表 11：IDTA 第 1 部表の記載の情報

IDTA 第 1 部表	
表 1 当事者と署名	開始日、当事者の詳細、主な連絡先、データ輸入者のデータ主体の連絡先、署名
表 2 移転内容	■ IDTA の準拠法・管轄裁判所（イングランドおよびウェールズ、北アイルランド、スコットランドから選択） ■ 輸入者の属性（管理者、処理者、復処理者） ■ 輸入者への UK GDPR の適用の有無 ■ リンク契約（契約の名称・締結日・当事者） ■ 期間（IDTA、リンク契約）、期間終了前の IDTA の終了の可否、承認された IDTA に変更があった場合の IDTA 終了の権利 ■ 再移転の可否・制限事項 ■ IDTA のレビューの日程
表 3 移転されたデータ	■ 移転されたデータ、移転されたデータに含まれる特別カテゴリの個人データ ■ 移転されたデータのデータ主体、輸入者の処理目的
表 4 セキュリティ要件	■ 送信のセキュリティ、保管のセキュリティ、処理のセキュリティ ■ 組織的、技術的セキュリティ対策、セキュリティ要求事項の更新

ii）Step 2：TRA の実施

次に、TRA を実施する。具体的な TRA の実施手順については、表 12 に示す。

表 12：TRA の実施手順

Step	TRA の実施手順の概要
Step 2-1 移転の評価	■ 本 TRA のツールが対象となる制限付き移転に適していることを確認 ■ 制限付き移転が他の UK GDPR の義務を満たしていることを確認（移転がデータ主体の高いリスクを伴う場合は、他の UK GDPR の義務を満たしていない可能性がある） ■ 制限付き移転の性質の評価・記録
Step 2-2 移転先国における法的効力	■ IDTA が移転先国で強制力を持つかどうかを評価。執行可能である可能性が高いと判断した場合、Step 2-3 に進む。 ■ IDTA の執行可能性に懸念がある場合は、補足的なリスク評価を実施して、データ主体に危害が及ぶリスクがあるかどうか、また、追加的な措置や保護によってリスクを低減できるかどうかを評価 ✓ 危害のリスクがない、または、低いと評価した場合は、Step 2-3 に進む。 ✓ 危害のリスクが高まっていると評価した場合は、リスク評価のために TRA ツールの使用を止め、UK GDPR 第 46 条以外の手段による移転を検討するか、移転を断念
Step 2-3 第三者のアクセスからのデータの適切な保護の有無	■ 個人データへの第三者のアクセス（監視を含む）を規制するための移転先国の体制を評価。Step 2-3 が終了した時点で、次のいずれかの場合には移転を実行することが可能 ✓ 第三者のデータアクセス（監視を含む）を規制する移転先国の制度が、英国の制度を支える原則と十分に類似していること ✓ 送付先の国の体制に関わらず、第三者によるアクセス（監視を含む）の可能性が少ないこと

	✓ 第三者によるアクセス（監視を含む）が行われたとしても、データ主体に損害を与えるリスクが低いこと

iii）Step 3-1：TRA の結果に基づく追加保護条項の記載

上記 Step 2 の TRA の結果を踏まえて、追加の措置・保護を、追加保護条項（IDTA 第 2 部）または第 1 部の表 4 のセキュリティ要件として記載することが必要となる。すなわち、**追加保護条項**とは、移転データおよび TRA に利用可能な保護を検討した結果、IDTA における適切な保護レベルを維持するために追加の措置および保護が必要であると判断した場合、それらの追加の措置および保護として、IDTA の中で規定する条項のことであり、(i) 特別な技術的セキュリティ保護、(ii) 組織的な保護の強化、(iii) 契約上の特別な保護がある。(i) ないし (iii) のいずれも、第 1 部表 4 のセキュリティ要件に記載することができ、表 4 に記載した場合は、改めて追加保護条項として記載する必要はない。

iv）Step 3-2：商業条項・強制条項の追加・IDTA の締結

当事者が合意した追加の商業条項がある場合は、IDTA の中で、商業条項（IDTA 第 3 部）として、追加することができる。ICO では、テンプレート形式を提供しているが、使用を義務付けられているわけでは必要はなく、例えば、リンク契約（業務委託契約等）がある場合は、商業条項を追加する必要はなく、商業条項を使用しない場合、最も簡単な対応は、商業条項欄に「商業条項は使用していない」と記載することである。

商業条項が IDTA の保護レベルを不用意に下げてしまう場合、当該制限付き移転は UK GDPR に違反する可能性があるため、商業条項を追加する際には、慎重に行う必要がある。

強制条項（IDTA 第 4 部）とは、商業条項とは異なり、原則、全ての IDTA に、変更することなく完全な形で条項を記載することが求められる条項である。強制条項の主な条項としては、輸入者の義務として、目的の範囲内での処理、IDTA・リンク契約の遵守義務、ICO の要求への対応義務等（IDTA 第 12 条）、輸入者が UK GDPR の適用を受ける場合の義務として、UK GDPR の適用・ICO の管轄に属すること、UK GDPR の遵守につき合意する義務（IDTA 第 13 条）、データ保護の主要原則を遵守するためのデータ輸入者の義務として、目的との関係で必要最小限の処理、正確性等、保管期間が合理的期間内であることなどの保証（IDTA 第 14 条）（ただし、データ輸出者の処理者または復処理者の場合には本条の遵守義務なし。）、データ輸入者の個人データ侵害があった場合の対応についての義務として、有害な影響を最小限に抑えるなどの合理的な措置、適切なセキュリティレベルの提供の保証、（データ輸入者が処理者の場合）個人データ侵害が発生した場合のデータ輸出者に対する通知義務等、（データ輸入者が処理者の場合）データ主体の権利・自由へのリスクをもたらす可能性がある場合のデータ輸出者に対する通知義務・高リスクの場合のデータ主体に対する通知義務等（IDTA 第 15 条）、移転されたデータの再移転をする場合の規制（IDTA 第 16 条）、処理を再委託する場合のデータ輸入者自身の責任（IDTA 第 17 条）、データ主体による権利の行使方法に関する規定において、データ主体の要求に応じた移転データのコピーの提供、訂正、消去、ダイレクトマーケティング目的の使用中止、合理的要求に従うこと、プロファイリングを含む自動化された意思決定の原

則禁止等（IDTA 第 20 条）（ただし、データ輸出者の処理者または復処理者の場合には本条の遵守義務なし。）が規定されている。

以上の IDTA の締結の実務対応フローをまとめると、以下の表 13 のとおりである。

表 13：IDTA の締結の実務対応フロー（まとめ）

IDTA の締結の実務対応フロー	
Step 1：英国国内所在者の個人データの移転フローを特定（IDTA 締結用データマッピングの実行） ✓ 英国の十分性認定によってカバーされない国・地域（EEA や日本以外の国々、例えば、米国や中国等）に所在する拠点との関係で IDTA の締結が必要となる。 ✓ IDTA 第 1 部に対応する情報の収集	
Step 2：移転リスク評価（TRA：Transfer Risk Assessment）の実行	
Step2-1 移転の評価	■ 本 TRA のツールが対象となる制限付き移転に適していることを確認 ■ 制限付き移転が他の UK GDPR の義務を満たしていることを確認（移転がデータ主体の高いリスクを伴う場合は、他の UK GDPR の義務を満たしていない可能性がある） ■ 制限付き移転の性質の評価・記録
Step2-2 移転先国における法的効力	■ IDTA が移転先国で強制力を持つかどうかを評価。執行可能である可能性が高いと判断した場合、Step 2-3 に進む。 ■ IDTA の執行可能性に懸念がある場合は、補足的なリスク評価を実施して、データ主体に危害が及ぶリスクがあるかどうか、また、追加的な措置や保護によってリスクを低減できるかどうかを評価 ✓ 危害のリスクがない、または、低いと評価した場合は、Step 2-3 に進む。 ✓ 危害のリスクが高まっていると評価した場合は、リスク評価のために TRA ツールの使用を止め、UK GDPR 第 46 条以外の手段による移転を検討するか、移転を断念
Step2-3 第三者のアクセスからのデータの適切な保護の有無	■ 個人データへの第三者のアクセス（監視を含む）を規制するための移転先国の体制を評価。Step 2-3 が終了した時点で、次のいずれかの場合には移転を実行することが可能 ✓ 第三者のデータアクセス（監視を含む）を規制する移転先国の制度が、英国の制度を支える原則と十分に類似していること ✓ 送付先の国の体制に関わらず、第三者によるアクセス（監視を含む）の可能性が少ないこと ✓ 第三者によるアクセス（監視を含む）が行われたとしても、データ主体に損害を与えるリスクが低いこと
Step 3-1：TRA の結果に基づく追加保護条項の記載 ✓ TRA の結果を踏まえた追加の措置・保護を、追加保護条項または表 4 のセキュリティ要件として記載することが必要	
Step 3-2：商業条項・強制条項の追加・IDTA の締結	

（4）拘束的企業準則（BCR: Binding Corporate Rules）による移転（46 条 2 項(b)、47 条）

拘束的企業準則（BCR: Binding Corporate Rules）とは、事業体グループまたは共同経済活動に従事する事業体グループの構成企業同士で、英国国外への個人データの制限付き移転を適法に行うために ICO の承認を取得したうえで採用するものであり、契約の形態を採る IDTA とは、事業体グループの内部規則という形態で UK GDPR 上の義務を規定する点で異なる。BCR を使用して制限付き移転を行うための適切な保護手段を提供するという制度は、EU データ保護指令およびそれに基づく EU 加盟国法の下で開発され、UK GDPR（特に 47 条）の下で英国法の一部として継続されている。国際的な組織の中で制限付き移転を行うには、データ輸出者とデータ輸入者の両方が承認された BCR に含まれている必要がある。英国の BCR は ICO の情報コミッショナーによって承認される。BCR は、多国籍企業グループ、フランチャイズ、ジョイントベンチャー、および専門家パートナーシップなどの共同経済活動に従事する企業グループによる使用を意図したものであ

る。BCR には、管理者 BCR と処理者 BCR の 2 種類がある。BCR は十分性のない第三国へのデータ移転を促進するだけではなく、企業のグローバルなプライバシーコンプライアンスプログラムの構造を形成することに役立つ面もある[63]。

BCR を導入すると、グローバル組織にとって以下のような幅広いメリットがある。

- **企業グループ内でのデータ保護要件の調和を図ることができる。**
- **他のデータ移転メカニズムの交渉を排除することで、長期的なコスト効率を実現すること**：BCR を導入してしまえば、個別の IDTA 締結・改訂等の対応をする必要がなくなり、長期的なコスト削減につながると考えられる。
- **政府からのアクセス要求への対応に関するグループ内の透明性の向上させること**
- **制裁金リスクの軽減**：データ保護監督当局の承認した BCR に則った運用をすることで、制裁金を課されるリスクを軽減することができる。
- **BCR を導入した企業が市場における競争優位性を得ること**：監督当局による制裁により、国際的なデータ移転を伴うデータの利活用が阻害されることによるリスク（レピュテーションリスクを含む）の影響の大きさを考慮すると、BCR の導入によるリスク軽減は将来的な競争優位性をもたらし、また、顧客（データ主体）からの信頼を基盤として成り立つ企業（B to C 企業等）にとって、高いデータ保護水準を示すことができ、一層顧客からの信頼を得ることにつながると考えられる。

他方で、BCR の要件の大部分は、GDPR の原則と重なっているため、組織は、既存の GDPR コンプライアンスプログラムを活用して BCR を導入することができるため、グループ全体としてコンプライアンスを進める企業にとっては、導入コストはそれほど大きくないと考えられる。

BCR は、法的拘束力があり、データ主体に強制力のある権利を付与し、少なくとも以下の要素を含まなければならない。

- グループの構成や連絡先
- データ移転の詳細
- 社内外を問わず、法的拘束力があること
- 一般的なデータ保護原則（目的の制限、データの最小化、保存期間の制限、デザインによるプライバシー、透明性、法的根拠、データセキュリティ等）の適用、および移転に関する要件
- データ主体の権利と利用可能な救済措置
- BCR に違反した場合の責任の引き受け
- BCR がデータ主体にどのように伝達されるか
- データ保護責任者の任務（データ保護責任者を選任している場合）
- 苦情処理手続き
- BCR の遵守状況を確認するために利用可能な監査手順
- BCR の変更を ICO に報告する方法
- ICO への協力方法

[63] ICO, Binding Corporate Rules (available at https://ico.org.uk/for-organisations/binding-corporate-rules/)

- BCR によって提供される保証に実質的な悪影響を及ぼす可能性のある、グループのメンバーが第三国で受ける法的要求事項を ICO に報告するためのメカニズム
- 個人データにアクセスできる人員に提供されるデータ保護トレーニング

BCR を申請する組織は、**英国 BCR の申請書（UK BCR-C-Application または UK BCR-P-Application）をリファレンス表（UK BCR-C-Referential Table または UK BCR-P-Referential Table）**とともに ICO に提出し、審査を受けることになる。ICO が英国 BCR の承認の申請を審査し、全ての要件を満たしたと判断した場合、情報コミッショナーが英国 BCR を承認することになる。

英国 BCR には、以下の表 14 のように、BCR に基づいて移転する個人データの種類・移転の目的・データ主体等を記載することが必要である。

表 14：BCR に基づいて移転する個人データの種類・移転の目的・データ主体

BCR の種類	BCR に基づいて移転する個人データの種類・移転の目的・データ主体
管理者 BCR	■ 人事情報 ➢ 目的：雇用、保険、セキュリティ等のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：従業員、派遣労働者、訪問者、取締役会メンバー ■ 取引先情報 ➢ 目的：アクセス権限の付与、支払いの円滑化、セキュリティ等のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：取引先、サプライヤー、コンサルタント ■ 顧客情報 ➢ 目的：アクセス権限の付与、支払いの円滑化、サポートサービスの提供、取引上の連絡、サービスの監視・改善等の目的のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：事業者・個人の顧客 ■ コンテンツ情報 ➢ 目的：アクセス権限の付与、サポートサービスの提供、セキュリティ等のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：従業員、派遣労働者、その他 A 社のユーザー
処理者 BCR	■ 顧客情報 ➢ 目的：アクセス権限の付与、支払いの円滑化、サポートサービスの提供、取引上の連絡、サービスの監視・改善等の目的のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：事業者・個人の顧客 ■ コンテンツ情報 ➢ 目的：アクセス権限の付与、支払いの円滑化、サポートサービスの提供、サービスの監視・改善等の目的のため A 社が必要とする処理をする場合に限る。 ➢ データ主体：事業者を含む顧客

（5）DCMS の UK GDPR の改正案

DCMS のコンサルテーションでは、必要に応じて組織が独自のメカニズムを特定できるようにするなど、代替となる移転メカニズムを導入する旨の提案[64]、反復的な移転に対す

[64] DCMS コンサルテーション・パラグラフ 261

る 49 条の例外規定の使用を拡大する旨の提案[65]を行っている[66]。DCMS の必要に応じて組織が独自のメカニズムを特定できるようにするなど、代替となる移転メカニズムを導入する旨の提案については、従来、個人データの国外移転規制に対する適切な保護措置のうち、組織の個別のニーズに応じたものとしては、ICO が組織独自の契約条項を審査・承認するというメカニズムがあったが、この審査・承認には長い時間を要するという問題があった。組織が代替的な移転メカニズムを ICO の承認なしで作成・特定できることは、他のグローバルな制度との相互運用性を高めることにつながるため、改正法において実現する可能性が高い。これは、組織にとっては、制限付き移転規制への遵守について、追加的な選択肢が増えるということを意味するものと考えられる。

また、DCMS の反復的な移転に対する 49 条の例外規定の使用を拡大する旨の提案については、UK GDPR において 49 条は、個人データの国外移転において適切な保護措置が提供できない例外的な場合に限定して、適法な国外移転を認めるものという位置づけであったが、この例外的な場合を拡張する提案であり、改正法において実現する可能性は一定程度あると考えられる。もっとも、組織全体の UK GDPR へのコンプライアンス制度の構築・運用にあたっては、引き続き第 49 条の法令上の例外に依拠することに過度に依存することは望ましくないと ICO は考える可能性が高いといえる。

8. ICO の命令に従う義務（58 条(1)および(2)）

ICO は、管理者および処理者による個人データの処理行為に関して、調査や是正措置を講じる権限を有しており、企業はこれらに関する命令に従う必要がある。ICO による命令等に迅速に対応するためには、UK GDPR に関する一連のコンプライアンス対応を事前に講じておくことに加え、そのような命令等があった場合にどのように対応すべきかについて内部的なメカニズムを構築しておく必要があると考えられる。

9. 13 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理に、子どもの保護責任者による同意または許可を取得する義務（8 条）

13 歳未満の子どもに対する直接的な情報社会サービスの提供に関して同意に基づく処理を行う場合、当該処理は、子どもの保護責任者によって同意が与えられた場合、または承認された場合に限り、適法である。

---

[65] DCMS コンサルテーション・パラグラフ 270

[66] ①必要に応じて組織が独自のメカニズムを特定できるようにするなど、代替となる移転メカニズムを導入する：DCMS は、UK GDPR46 条に記載されているものに加えて、組織が独自の代替的な移転メカニズムを作成または特定できるようにするかどうかを検討している。このような変更は、複雑なデータ移転要件を持つ組織にとって有益であり、例えば、安全な国際移転を可能にするために特注の契約を設計・使用することができる。これは、UK GDPR46 条に記載されている移転に関する既存のオプションを補完するものであり、ICO からの事前承認を必要とする特注のデータ保護条項の開発を規定している現在の 46 条 3 項(a)のオプションに取って代わるものである（DCMS コンサルテーション・パラグラフ 261）。
②反復的な移転に対する 49 条の例外規定の使用を拡大する：DCMS は、例外規定の反復使用が許可されることを明示することで、例外規定の使用に関する柔軟性を比例的に高めることを確立することを提案している。この許可は、やむを得ない正当な利益のための例外規定を除くすべての例外規定に適用される。この許可は、やむを得ない正当な利益のための例外規定を除く、すべての例外規定に適用される（DCMS コンサルテーション・パラグラフ 270）。

10. 適切な技術的・組織的な対策を実施する処理者を利用する義務（28 条）

管理者が個人データの処理に際して処理者を利用する場合、管理者は、当該処理が UK GDPR に定める義務に適合するような態様で適切な技術的・組織的な対策を実施することについて十分な保証を提供する処理者のみを利用することができる（28 条 1 項）。管理者は処理者による UK GDPR 違反の責任を負う可能性があるため、処理者の選定および監督について UK GDPR 上のリスクに留意しておく必要がある。管理者は、処理者を利用する際に管理者および処理者の間で締結する処理契約において、UK GDPR が定める特定の事項を規定しておく必要がある（28 条 3 項各号）[67]。

11. 設計によるデータ保護・デフォルトとしてのデータ保護を確保するために、適切な技術的措置および組織的措置を実装する義務（25 条）

管理者は、UK GDPR の要件に適合するものとし、かつ、データ主体の権利を保護するため、処理の方法を決定する時点および処理それ自体の時点の両時点において、データの最小化のようなデータ保護の基本原則を効果的な態様で実装し、その処理の中に必要な保護措置を統合するために設計された、仮名化のような、適切な技術的措置および組織的措置を実装しなければならない。また、管理者は、その処理の個々の特定の目的のために必要な個人データのみが処理されることを、デフォルトで確保するための適切な技術的措置および組織的措置を実装しなければならない。

12. 該当する場合、英国代理人の選任義務（27 条）

英国代理人は、UK GDPR の地理的適用範囲に関する 3 条 2 項に基づく UK GDPR の適用がある場合に選任が義務付けられる。3 条 2 項は英国国内に拠点のない管理者、または処理者が英国国内に所在するデータ主体の個人データについて以下のいずれかに関する処理を行う場合に UK GDPR が適用される旨を規定する。

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

(b) 英国国内で行われるデータ主体の行動の監視に関する処理。

ただし、以下のいずれかに該当する場合は、英国代理人を選任する必要はない。

- 公的機関である場合
- 処理は、時折行われるだけで、個人のデータ保護権に対するリスクが低く、特別カテゴリの個人データまたは犯罪データの大規模な使用を伴わない場合

3 条 2 項の適用範囲については、日本企業が英国国内に拠点を有するとしても、上記(a)または(b)に関して日本本社が行う英国国内のデータ主体の個人データの処理が英国国内の拠点と関連しない場合、英国国内に拠点のない管理者による英国国内のデータ主体の処理行為であると解釈され、3 条 2 項に基づき UK GDPR が適用され、英国代理人の選任が義務付けられる場合がある。

---

[67] ICO, Guide to the General Data Protection Regulation (GDPR), Contracts and liabilities between controllers and processors (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/)

13. 責任に基づいて処理行為の記録を保持する義務（30 条）

管理者および処理者は、個人データの処理に関する記録を維持する義務を負う（30 条 1 項）。ICO からの要求がある場合には管理者および処理者は当該記録を提出しなければならないため（30 条 4 項）、当該記録は UK GDPR の所定の要件に従って作成され、かつ最新の内容にアップデートされている必要がある[68]。管理者および処理者の記録義務の内容につき、以下の表 15 に示す。

表 15：管理者および処理者の記録義務の内容

管理者の記録義務（30 条 1 項）	処理者の記録義務（30 条 2 項）
▪ 管理者の名前と連絡先（該当する場合、共同管理者、管理者の代理人およびDPOの名前と連絡先） ▪ 処理目的 ▪ データ主体の種類および個人データの種類 ▪ 個人データが開示されたまたは開示され得る受領者（第三国または国際機関における受領者を含む）の種類 ▪ 該当する場合、第三国または国際機関への個人データ移転（当該移転先の特定を含む）、および49条1項後段で定める移転の場合には適切な保護措置に関する文書 ▪ 可能であれば、各データの種類に関する削除が想定される期間 ▪ 可能であれば、32条1項で定める技術的・組織的な安全対策の概要	▪ 処理者および管理者の名前と連絡先（該当する場合、管理者または処理者の代理人およびDPOの名前と連絡先） ▪ 管理者の代わりに実施している処理の種類 ▪ 該当する場合、第三国または国際機関への個人データ移転（当該移転先の特定を含む）、49条1項後段で定める移転の場合には、適切な保護措置に関する文書 ▪ 可能であれば、32条1項で定める技術的・組織的な安全対策の概要

上記のような処理行為の記録の要件に関し、DCMS のコンサルテーションで、処理行為の記録を、プライバシー管理プログラムの一環として、個人データのインベントリに置き換えることで記録保持の要件をする旨の提案[69]がなされている。

UK GDPR を遵守するためには個人データの処理と移転の内容の詳細を把握した上で、必要なコンプライアンス対応のための文書の作成・準備を行う必要があるため、個人データの処理記録の作成・保持は、UK GDPR 上の記録保持の要件の廃止にかかわらず、実務上は引き続き必要になると考えられる。

14. ICO に協力する義務（31 条）

データ管理者および処理者は、ICO からの要請がある場合には、ICO に協力しなければならない。

---

[68] ICO, Guide to the General Data Protection Regulation (GDPR), Documentation (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/)

[69] DCMS は、30 条の記録保持義務を撤廃することを提案する（DCMS コンサルテーション・パラグラフ 177）。30 条に基づく記録保持要件は、組織がデータガバナンスを改善し、UK GDPR の他の側面を遵守し、規制執行を支援するのに役立つ可能性がある。30 条の要件を削除すると、効果的な執行が妨げられ、データ主体に対する規制上の保護が弱くなるリスクがある。しかし、DCMS はそのリスクを最小限に抑えることができると考えている。プライバシー管理プログラムの新たな要件では、一定の記録を保持することが求められるが、組織は、取り扱う個人情報の量や機密性、実施するデータ処理の種類を反映した方法で記録を保持する方法について、より柔軟に対応できるようになる。また、UK GDPR13 条および 14 条では、これまで通り、プライバシー通知に同じ情報を記録することが求められる。

15. 適切なセキュリティレベルを保証する適切な技術的・組織的対策を実施しない場合（32 条）

UK GDPR の主要な原則は、「適切な技術的および組織的措置」によって個人データを安全に処理することであり、これは「**セキュリティの原則**」と言われる。このためには、リスク分析、組織的ポリシー、物理的・技術的対策などを検討する必要がある。また、データ処理のセキュリティに関する追加の要件を検討する必要があるが、これらはデータ処理者にも適用される。

どのような対策を講じるかを決定する際には、最新の技術や導入コストを考慮することができるが、それらは管理者の状況と処理が引き起こすリスクの両方に適したものである必要がある。適切な場合には、仮名化や暗号化などの手段の使用を検討する必要がある。

上記対策は、システムとサービス、およびその中で処理される個人データの「機密性、完全性、可用性」を確保するものである必要がある。また、物理的または技術的な事故が発生した場合には、個人データへのアクセスと可用性を適時に回復できるようにしなければならない。また、対策の有効性をテストし、必要な改善を行うための適切なプロセスがあることを確認する必要がある。

ICO は、**英国国家サイバーセキュリティセンター（NCSC: National Cyber Security Centre）**と緊密に協力して、管理者に適した対策を評価する際に使用できるアプローチを開発した[70]。このアプローチでは、共通の期待事項を考慮し、既存のガイダンスに従うか、特定のサービスを利用するか、または適切な知識とリソースがあれば独自のプロセスを開発することができる。このアプローチは、4 つの目的に基づいている。

- セキュリティリスクの管理
- サイバー攻撃から個人データを保護する。
- セキュリティイベントの検知、および
- 影響の最小化

DCMS のコンサルテーションにおいて、コンプライアンス要件として「**プライバシー管理プログラム**」を導入することの提案[71]がされている。プライバシー管理プログラムという新たなリスクベースの説明責任の枠組みが導入されることにより、組織は追加的に UK GDPR の改正法へのコンプライアンス対応を取る必要が出てくる。こうした枠組みの導入を内容とする改正提案がビジネスフレンドリーなものであるかどうかという点には議論があり得るものの、新しい形のプライバシー管理プログラムを世に対して問うという意味合いのある改正提案となるものと考えられる。パブコメによって集まった回答の内容を踏まえて、具体的な提案の内容がさらに検討されることになるものと考えられる。

---

[70] ICO, Security outcomes (available at https://ico.org.uk/for-organisations/security-outcomes/).

[71] プライバシー管理プログラムに基づいた、より柔軟でリスクベースの説明責任の枠組みを導入する。この枠組みの下では、組織はその処理活動に合わせたプライバシー管理プログラムを実施し、データプライバシー管理を単なる「チェックリスト」としてではなく、全体的に受け入れることが求められる（DCMS コンサルテーション・パラグラフ 145）。

16. データ侵害通知義務がある場合、当局への通知義務およびデータ主体への通知義務（33/34 条）

データ侵害が発生した場合、管理者は、以下の表 16 に記載するデータ侵害通知の要件に従って、データ主体の権利および自由に対するリスクに応じて、ICO およびデータ主体に対して通知を行う義務を負う。

表 16：データ侵害通知の要件

通知先	要件
ICO	個人データの侵害が発生した場合、管理者は、不当に遅滞することなく、可能であれば侵害を認識してから 72 時間以内に個人データの侵害を ICO に通知しなければならない。ただし、個人データの侵害が、自然人の権利または自由に対してリスクを生じさせない場合を除く。
データ主体	個人データの侵害が自然人の権利および自由に対して高いリスクを生じさせる可能性がある場合、管理者は、不当に遅滞することなくデータ主体に通知しなければならない。

一般的にデータ侵害のリスク評価においては、データ主体の権利および自由に対するリスクの可能性および重大性について検討を行う必要がある（前文 75 項および 76 項）。リスク評価は、以下の要素に関する客観的な評価に基づいて行われるべきである。

- データ侵害の性質
- 個人データの性質、センシティビティおよび量
- 個人の識別に関する容易性
- 個人に対する結果の重大性
- 個人に関する特別な性質（例：子供または脆弱な個人）
- 影響を受ける個人の数
- 管理者の特別な性質（例：特別なカテゴリの個人データを処理する医療機関）

データ侵害から 72 時間以内に ICO に通知するという時間制限を伴う義務は、管理者にとって事前の準備なく遵守することは困難であるため、データ侵害が発生した場合における対応マニュアルを事前に準備しておくことが望ましい。DCMS は、管理者が個人データ侵害の報告をすべきか否か判断しにくい場合があり、リスクの低いインシデントが過剰に報告される傾向およびそれによる管理者・ICO への不必要な負担を減らすため、DCMS コンサルテーションにおいて、ICO への個人データ侵害報告の閾値を引き上げる旨の提案を行っている[72]。ICO は DCMS の提案に概ね賛成しており、改正法では、個人データ侵害通知義務に関する閾値が引き上げられる可能性が高いと考えられる。

17. 該当する場合、データ保護影響評価を実施する義務（35 条）

データ保護影響評価（DPIA: Data Protection Impact Assessment）とは、データ処理の前に実施される個人データ保護に関する影響評価を意味し、処理が個人の権利および自由対して高度のリスクをもたらす可能性がある場合に、管理者が実施することが義務付けられるものである。DPIA は、プロジェクトのデータ保護リスクを特定し、最小化するためのプロセスである。個人に高いリスクをもたらす可能性のある処理については、DPIA を行う必要がある。

[72] DCMS コンサルテーション・パラグラフ 386

ICO が UK GDPR の下でも引き続き参考になると明言している欧州データ保護会議（EDPB）の DPIA に関するガイドラインによれば、以下の表 17 に列記した 9 つの基準のうち 2 つ以上に該当する処理行為については、DPIA を実施する義務があると考えられる（ただし、1 つの基準にのみ該当する処理行為について DPIA が義務付けられる場合もあり得る）。

表 17：DPIA の実施基準

EDPB の DPIA に関するガイドラインにおける高リスクの処理行為の基準
(1) 評価またはスコアリング
(2) 法的効果または類似の重大な影響を伴う自動的な意思決定
(3) 体系的な監視
(4) センシティブなデータまたは非常に個人的な性質を有するデータ
(5) 大規模なデータ処理
(6) データのセットのマッチングまたは結合
(7) 脆弱なデータ主体に関するデータ（例：従業員データ）
(8) 新しい技術的もしくは組織的な解決方法の革新的な利用または適用
(9) データ主体による権利の行使、またはサービス、利用や契約を行うことを妨げること

例えば、職場における防犯用の CCTV の導入は、従業員の監視行為に該当し得るため、上記(3)(7)に該当して DPIA が必要となり得る。DPIA の実施においては、DPIA に関するガイドラインの方針に従って、一定の方法論を踏襲する必要があり、例えば、以下のものを含む必要がある。

- 処理の性質、範囲、状況、目的を説明する。
- 必要性、比例性、コンプライアンス対策を評価する。
- データ主体に対するリスクを特定および評価する。
- これらのリスクを軽減するための追加措置を特定する。

リスクのレベルを評価するには、個人への影響の可能性と重大性の両方を考慮する必要がある。**高リスク**とは、何らかの危害が発生する可能性が高いこと、または重大な危害が発生する可能性が低いことのいずれかである。

データ保護責任者を選任している場合には、データ保護責任者に対して相談することに加え、場合によってはデータ主体や関連する専門家に相談することが必要である。また、処理者がいる場合には、当該処理者にも DPIA の実行に協力してもらう必要がある場合がある

上記のような DPIA に関して、事業者ごとにより柔軟なデータ保護影響評価を実施できるように、DCMS のコンサルテーションにおいて、DCMS は DPIA の実施のための要件の撤廃を提案しており[73]、これに対して ICO は廃止に反対している。世界中のデータ保護法の立法の動向を見ても、米国カリフォルニア州のカリフォルニアプライバシー権利法（CPRA）や中国の個人情報保護法においても、データ保護影響評価が一定の場合に義務付けられている。なお、ICO は、DPIA の形式に柔軟性を持たせる余地があることには同意しており、リスクに関する評価の堅牢性や質を確保できる形での新たな評価形式等に関する議論がなされる可能性はある。

[73] DCMS コンサルテーション・パラグラフ 167

18. 影響評価において緩和できないリスクがあった場合の当局への事前相談義務（36条）

管理者が DPIA の結果、軽減できない高いリスクを確認した場合は、処理を開始する前に ICO に相談する必要がある。例えば、データ主体が重大または不可逆的な結果を被り、それを克服することができないおそれがある場合（例：データ主体の生命の脅威、一時解雇、財政的危機につながるデータへの違法なアクセス）、またはリスクの発生が明白と考えられる場合（例：データの共有、使用または配布がなされているため、または周知の脆弱性に手当てがされていないため、データにアクセスする人数を減少させることができない）が挙げられる。ICO は、8 週間以内（複雑なケースでは 14 週間以内）に書面による助言を行う。適切であれば、データ処理を行わないよう正式な警告を発し、または処理を全面的に禁止することもある。

19. データ保護責任者（DPO）の選任義務、およびその職や役務を尊重する義務（37～39 条）

UK GDPR では、管理者または処理者が公的機関や団体である場合、または特定の種類の処理活動を行う場合に、**データ保護責任者（DPO：Data Protection Officer）**を選任する義務がある。DPO は、社内での UK GDPR コンプライアンスの監視、データ保護義務に関する情報提供と助言、データ保護影響評価（DPIA）に関する助言、データ主体と ICO との連絡窓口としての役割を果たす。DPO は、独立したデータ保護の専門家であり、十分なリソースを持ち、最高レベルの経営陣に報告する必要がある。DPO は、既存の従業員でも、外部から選任された者でもいずれでも問題ない。場合によっては、複数の組織が 1 人の DPO を選任することも可能である。DPO は、UK GDPR のコンプライアンスを証明するのに役立ち、説明責任の強化の一環となる[74]。

上記のような DPO の選任義務が課せられる場合、一律に DPO の資格・地位要件を有する専門家を選任することは、選任コストとそれによる効果の観点から、必ずしも、効果的なデータ保護につながるわけではない場面もあると考えられ、そのため、DCMS のコンサルテーションにおいて、DPO の選任要件を、プライバシー管理プログラムに責任を持つ適切な個人の選任要件に変更することの提案[75]がなされている。

ICO は、DCMS の提案に概ね賛成しており、改正法に含まれる可能性が高いと考えられる。この点、データ保護責任者は、UK GDPR コンプライアンスにおいて中心的な役割を果たす役割であり、EU GDPR を皮切りに、今日では中国の個人情報保護法における個人情報保護責任者（Personal Information Protection Officer）の役割の創設にまで至っている。UK GDPR においてデータ保護責任者の選任義務が廃止されるとすれば、衝撃的なニ

---

[74] ICO, Guide to the General Data Protection Regulation (GDPR), Data protection officers (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers/).

[75] データ保護責任者を選任する現行の要件を削除することを提案する（DCMS コンサルテーション・パラグラフ 163）。新たに提案されている要件は、プライバシー管理プログラムに責任を持ち、組織のデータ保護コンプライアンスを監督するための適切な個人を指定することであり、組織に異なる義務を課すことで、より効果的なデータ保護の成果を促す可能性がある。

ュースとなると考えられる。もっとも、DCMS 案においてもデータ保護コンプライアンスを監督する指定された個人を選任するという要件は含まれており、こうした個人の役割を、現在のデータ保護責任者が務めることも否定されていないため、実務的に一定の影響はあるものの、混乱は限定的なものにとどまるものと考えられる。

III. UK GDPR のコンプライアンス対応

以下では、UK GDPR の適用のある子会社を有する日本企業を念頭に、コンプライアンス対応実務について概説する。

1. データマッピング

データマッピングとは、UK GDPR の適用の有無を判断し、また、適用される場合に、UK GDPR の要求事項と現状とのズレ（ギャップ）を認識することを目的として行う社内調査のことをいう。データマッピングの作業は、色々な方法論があるところであるが、例えば、以下の 3 つの工程で行う。

1. データマッピング質問票の送付
2. 質問票への回答に対する追加質問・インタビュー
3. データマッピングアセスメントレポート作成

まず、主にデータマッピング質問票への回答を求めることによって、事実調査を行うが、質問票の送付後に、その趣旨を説明し、担当者の疑問に回答する機会を設けることも有用である。質問票の質問に対する回答の内容に対して、追加質問やインタビューを実施することにより、データマッピングアセスメントレポートでの法的判断に必要な事実を漏れなく収集する。最後に、各部署から収集した事実をもとに、GDPR の適用の有無等の法的判断を行い、データマッピングアセスメントレポートを作成する。

このようにデータマッピングにおいては、処理したデータ等に関する質問票への回答やインタビューを併用して、事実調査を進めることになる。具体的には、UK GDPR の適用がある個人データの処理、英国国外への国外移転の内容の目的毎の網羅的なリストアップを行うこと、自社の UK GDPR 上の位置づけの整理（「管理者」「共同管理者」、または「処理者」）することで自社の UK GDPR 上の義務の内容を特定するための事実調査を行う。

また、自社の個人データの処理において、UK GDPR 上の諸原則の遵守ができているのかの確認や処理の法的根拠（保持期間等を含む）を確認し、自社の個人データのフローを把握した上で、個人データの処理の法的根拠の分析をすることにより、自社の個人データの処理の UK GDPR 上の適法性を判断することができるようになる。

データマッピングによる事実調査では、個人データの処理業務をリストアップする際、取得すべき情報の粒度について、例えば人事情報の処理といった粒度ではなく、以下のようにより詳細な粒度で、個人データの処理業務を処理の目的ごとにリストアップする。

例：

- 人事関連（人事関連業務）
- 一般的な従業員情報（一般的な従業員情報管理業務）
- 採用/ CV （採用申込者および採用者の履歴書取り扱い業務）
- VISA 管理（VISA 管理業務）
- 給与（給与支払業務）
- 納税（所得税支払業務）
- 評価（人事評価業務）
- 年金（年金関連業務）

- グローバルタレントマネジメント（グローバルタレントマネジメントプログラム）
- 緊急連絡先（緊急連絡先情報管理）
- 監視 CCTV （監視カメラ）

上記のようなデータマッピングを行うことにより、自らの組織の個人データの処理の中で、データ主体の同意、データ主体に対する情報通知、処理契約、国外移転のための IDTA および TRA が必要な場面を特定し、対応漏れがないかの確認をすることが可能となる。また、DPIA の実行義務の特定、DPO および/または英国国内の代理人の選任義務の有無の検討をすることが可能となる。

2. UK GDPR 対応コンプライアンス文書の作成

上記のデータマッピングにより、事実調査が完了した後、自社のデータ処理の中で、一定の文書が UK GDPR 対応コンプライアンス文書として必要となり、多くの企業では、以下の文書を作成または改訂することが必要になる。

（1）データ処理に関する内部規則

UK GDPR の適用のある個人データの処理に関するルールを社内規程として整備・明確化し、これを従業員等に周知徹底することが重要となる。データ処理に関する内部規則に記載すべき大まかな内容としては、社内規程の目的、適用範囲、個人データ処理の基本原則、説明責任、個人データの処理時の具体的な留意事項や手続、個人データの移転時の具体的な留意事項や手続、データ処理記録の記載とデータ処理との関係、データ主体からの権利行使への対応手続・フロー、データ侵害発生時の対応、罰則、社内規程の責任者などが挙げられる。

（2）データ主体権利行使対応マニュアル

データ主体権利行使対応マニュアルは、データ主体から権利行使があった場合の社内での対応窓口を含む体制、および、実際にデータ主体から権利行使があった場合に、権利行使への対応を判断し、当該判断をデータ主体に連絡するまでのフローを整理する形で作成する。実際にデータ主体から権利行使を受ける可能性のある従業員等にデータ主体権利行使対応マニュアルを周知することが望ましい。

（3）データ侵害通知マニュアル（データ保護監督当局への通知、データ主体への個人データ侵害通知）

個人データ侵害が発生した場合、管理者は、原則、データ保護監督当局への通知義務を負っており、また、一定の場合には、データ主体に対する通知義務を負う。そのため、データ侵害への対応方法を説明するマニュアルを作成し、個人データ侵害に対する適切な対応について、データ保護マネージャーまたはデータ保護担当者に周知することが有用である。データ侵害通知マニュアルの内容としては、個人データ侵害発生時における手続きの概要、初期段階の対応、データ保護監督当局への通知、データ主体への通知、個人データ侵害の文書記録、社内体制の評価、書式例等が挙げられる。

（4）処理契約

管理者は、個人データの処理委託にあたり、UK GDPR28 条 3 項所定の事項（処理行為の対象事項および期間、処理行為の性質および目的、データ主体の個人データの種類およ

びカテゴリ、管理者の義務および権利、ならびに、28 条 3 項各号に定められた事項（管理者の文書による指示に基づくデータ処理、守秘義務の確保、適切な技術的および組織的措置、復処理者への委託、管理者のデータ主体の権利行使に関する義務履行の支援、管理者の 32 条ないし 36 条に規定される義務履行の支援、サービス提供終了後の個人データの削除または返却、ならびに情報提供および監査への協力)）を定める処理契約を締結する必要がある。

(5) プライバシーポリシー・個別の情報通知

UK GDPR 上、データ主体に提供すべき情報として、管理者の身元および連絡先、DPO の連絡先、意図された個人データの処理の目的および法的根拠、管理者または第三者によって追求される正当な利益、管理者に対する個人データへのアクセス権、訂正権、制限権、異議権、データポータビリティ権の存在等が規定されており、これらの事項につき、プライバシーポリシーまたは個別の情報通知に記載する必要がある。プライバシーポリシー・個別の情報通知を使って情報通知義務を遵守する要件については、上記 II.「6. 情報通知義務（13、14 条)」に詳述した通りである。

(6) データ主体の同意書

データ主体に対して同意の撤回を許しても不都合でない場合、同意を個人データ処理の適法化根拠とすることが適切な場合がある。UK GDPR 上、有効な同意を取得するためには、EU GDPR 同様、任意になされ、特定されており、情報提供を受けた上でなされ、かつあいまいでないものである必要がある。有効な同意の要件は、上記 II.「3. 同意の条件を遵守する義務（7 条)」に詳述した通りである。

(7) 国外移転のための IDTA および TRA

英国国外への個人データの国外移転の適法化根拠として、UK GDPR 上の適切な保護措置を備える必要があるが、IDTA の締結と TRA の実施により適切な保護措置を備えることが、実務上、合理的な対応といえることが多いと考えられる。IDTA の締結および TRA の実施については上記 II.「7. 個人データの移転の条件に従う義務（44-49 条）（3）標準データ保護条項（SDPC）による移転（46 条 2 項(c))」①から③において詳述した通りである。

(8) 適切な技術的・組織的措置の実施（プライバシープログラムの策定を含む）

上記 II.「15. 適切なセキュリティレベルを保証する適切な技術的・組織的対策を実施しない場合（32 条)」に記載の通り、処理するデータの規模・性質等に応じて、適切な技術的・組織的措置を実施する必要がある。

(9) DPIA テンプレートの作成

上記 II.「17. 該当する場合、データ保護影響評価を実施する義務（35 条)」に詳説した通り、高リスクの処理行為に関しては処理行為の実行前の DPIA の実施が必要になるため、DPIA のテンプレートを準備する必要がある。ICO が作成した DPIA のテンプレート（https://ico.org.uk/media/for-organisations/documents/2553993/dpia-template.docx）が公表されており[76]、これに従うのが ICO の見解を踏襲することができるため最も安全で

[76] ICO, Guide to the General Data Protection Regulation (GDPR), Data protection impact assessments (available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-

あるが、EU GDPR に対応して作成された DPIA のテンプレートであっても引き続き利用可能であると考えられる。

3. UK GDPR 対応コンプライアンス文書の使用とトレーニング

UK GDPR 対応社内体制を整備した後、各部署の担当者自身の UK GDPR 対応の知見を深めることにより、実務対応を可能とすることができる。そのため、UK GDPR 対応の主導的な立場にある DPO、英国国内の各拠点におけるデータ保護マネージャーを含む UK GDPR 対応チームに対して、プライバシープログラムの運用の観点からの専門的なトレーニングを実施する必要がある。また、実際に、データ主体の権利行使への対応等を行う、英国国内の各拠点の一般従業員に対して、UK GDPR の内容と UK GDPR 対応において協力を求める事項に関するトレーニングを実施する必要がある。また、プライバシーポリシーのウェブサイトへの掲載、必要に応じて情報通知の実行、処理契約の締結、国外移転のための IDTA の締結および TRA の実施、DPIA を実施する必要がある。

general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).

Ⅳ. おわりに

本レポートでは、UK GDPR の改正案に関する検討の動向を踏まえつつも、現行の UK GDPR の基本的な内容を解説するとともに、コンプライアンス対応のために必要となる対応を概説した。

DCMS“Data: A new direction”による提案は、ICO による一部の内容に関する反対・抵抗があるものの、大筋において UK GDPR 改正法に織り込まれる可能性が高い。最終的な UK GDPR 改正法が EU GDPR から大きく乖離しデータ保護に対する権利を弱めるものとなった場合には、欧州委員会は、UK GDPR が改正され次第、英国のデータ保護の十分性決定を取り消す検討を開始する可能性がある。もともと欧州委員会による英国の十分性決定には、4 年間のサンセット条項（4 年間経過すると更新がない限りは無効とする条項）が含まれており、2025 年 6 月 27 日が有効期限とされている。

前述の通り、英国のデータ戦略としては、ニュージーランドの十分性認定について造詣が深いジョン・エドワーズ氏を新しい情報コミッショナーとして迎えて、EU からの十分性認定の有効性維持を目指しつつ、2021 年 8 月 26 日に DCMS が公表した” UK approach to international data transfers”に示した通り、米国・インド・韓国・シンガポール・インドネシア・オーストラリア・ブラジル・コロンビア・ドバイ国際金融センター・ケニアを十分性審査の優先順位のトップに位置付け、英国を中心としたデータ自由流通の戦略を描いている。すなわち、英国としては、EU の十分性認定の有効性維持は目指すものの、自国を中心としたデータ自由流通の枠組みを形成することを通じて、自国独自のデータ保護制度を構築するための備えを行っていると評価できよう。

したがって、英国が UK GDPR を大改正し、独自のデータ保護制度を構築し、EU GDPR から逸脱する可能性は否定できない。UK GDPR の大改正は、ビジネスフレンドリーな側面は大きいものの、日本企業にとっては EU GDPR とは別の独自のデータ保護制度へのコンプライアンス対応が追加で必要となり、また ICO の独自のガイドラインの動向を追う必要も出てくるため、全体としてはコンプライアンスの負担が重くなる恐れがある。UK GDPR の基本的な内容を踏まえたコンプライアンス対応を推進するとともに、UK GDPR の改正の動向を注視することも重要である。

以　上

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20220001

本レポートに関するお問い合わせ先：
日本貿易振興機構（ジェトロ）
海外調査部 欧州ロシア CIS 課
〒107-6006 東京都港区赤坂 1－12－32
TEL：03-3582-5569
E-mail：ORD@jetro.go.jp