G - ユーロプライバシー・GDPRコア基準

参照文書を含む「推奨される検証手段」は、本基準を充足するか否かを判断するために十分な証拠が収集されるまで、本基準に基づき評価されなければならない。
一般的な注意事項として、適用可能な各基準は個別に評価され、充足しなければならない。いずれかの基準を充足しない場合、たとえ他の基準を充足する場合であっても、正式な不遵守の引き金となる。
本基準の評価は、評価対象に適用される。当該評価は、ユーロプライバシー・コミュニティウェブサイトで利用可能なユーロプライバシー認証制度 一般仕様及び要件、並びに、本基準、確認項目及び管理項目の使用に関するユーロプライバシーガイドラインの両文書に従い、実施されなければならない。
GDPRの下では、認証は次の3つのケースに分けられる。
(1) EEA域内に所在し、GDPRの直接適用を受ける申請者（GDPR第3条1項）
(2) EEA域外に所在し、GDPR第3条2項に基づき直接適用を受ける申請者
(3) EEA域外に所在し、GDPR第3条第2項に基づき直接適用を受けない申請者であるものの、データ輸入者として欧州の個人データを取り扱っている者
いずれのケースも、認証はGDPR第42条を遵守する必要がある一方で、GDPR第46条は第3のケース（EEA域外に所在するデータ輸入者）にのみ適用される。第3のケースでは、GDPR第46条の義務も遵守しなければならない。これには、GDPR第46条が言及する「データ主体の権利に関するものを含め、適切な保護措置を適用するための拘束力があり執行可能な第三国の管理者又は処理者の約定を伴った、第42 条による承認された認証方法」を要求している。
EU法の下では、第三国からのデータのリモートアクセスは、第三国へのデータ移転と同等とみなされる。
本基準が既存の規則、方針、手順又は仕組みを参照する場合、申請者はこれらを効果的に実装する必要がある。同様に、監査人はそれらの実際かつ効果的な実装をレビューしなければならない。
申請者の法域と法の抵触がデータ主体にとってのリスクを構成し、かつ、当該リスクを効果的に低減できない場合、認証機関は認証を進めてはならない。認証後に規制変更により法の抵触が生じ、かつ、これを効果的に低減できない場合、認証機関は認証書の一時停止又は取消しを行わなければならない。
本基準で使用される用語の定義及び明確化は、次のとおりである。
「EU又はEEA加盟国法」とは、EEA域外に所在する申請者との関係では、GDPR第3条第2項a及びbに基づき、個人データが取扱われるデータ主体が所在するEU又は加盟国の法をいう
「第三国」とは、EEA域外の国及び国際機関をいう。
「第三国法」とは、非EEAの法域から申請する申請者の法であって、当該法が、民主主義の社会において必要かつ比例的な範囲を超えるデータ保護の権利に対する制限を課すものでない限りにおいて、求められる対象と比例的であり、データ保護の権利の本質的部分を尊重し、また、データ主体の基本的な権利及び利益の安全性を確保するための個別の措置を定めるものをいう。
「データ輸出者」とは、EEA域外の国に所在する別の管理者、共同管理者又は処理者（「データ輸入者」）に対して、個人データを開示、移転又はその他の方法で利用可能にするデータ管理者又は処理者をいう。
「データ輸入者」とは、EEA域外に所在するデータ管理者又は処理者であって、別のデータ管理者又は処理者（「データ輸出者」）からデータを取得する者をいう。
「所轄データ保護機関」とは、EEAにおけるデータ保護機関をいう。全体としては、評価対象によって取り扱われる個人データのコンプライアンスを執行する職務権限を有する各国データ保護機関をいう。GDPR第46条に基づきデータ輸入者に対してGDPR認証が付与される場合、所轄データ保護機関は、EEA域内のデータ輸出者のデータ保護機関のいずれかである。ただし、苦情の申立てについては、EEA域内のいずれの機関も職務権限を有するものとする。
「高いリスクのデータ取扱い」とは、特別な種類の個人データ若しくは有罪判決に関するデータを取り扱うデータ取扱い、子どもの個人データを特に対象とするデータ取扱い、又は、自然人の権利及び自由に対して高いリスクをもたらす可能性のあるデータ取扱いをいう。
「SME」とは、労働者数が250人未満の企業をいう。
その他の定義は、ユーロプライバシー認証制度一般仕様及び要件の第4節を参照されたい。

参照ID「G」（第3条）	申請者	固有／一般	レベル	タイトル	GDPR第3条1項及び2項の文脈における第42条のための基準（規定条項）	実装ガイダンス GDPR第3条1項及び2項の文脈における第42条のための基準（更新の対象となる参考条項）	推奨される検証手段（監査人向け）	GDPR条項	
G.1				**データ取扱いの適法性** 目的　評価対象におけるデータ取扱いが適法かつ比例的であるのを確保すること。 条件　【IF】申請者が評価対象で取り扱われる個人データのデータ管理者である場合、【THEN】次のとおりとする。					
G.1.1				**取扱いの適法性**					
G.1.1.1	C	S	A	取扱いの適法性評価	A) 評価対象におけるデータ取扱いが、申請者によって適法であると評価されたことを示す報告書又は文書がなければならない。 【AND】 B) 申請者は、DPO又は法律専門家と協議し、その所見を当該報告書又は文書に含めなければならない。 【AND】 C) 適法性が是正措置を条件とする場合、申請者は当該是正措置を実施しなければならない。 【AND】 D) 適法性に関する評価（又は再評価）報告書は、次のとおりでなければならない。 d.1) 評価対象で特定された全ての個人データの取扱いを対象とすること d.2) 【AND】データ取扱いの適法性の根拠を示すこと d.3) 【AND】該当する場合、正当化する書類又は参考資料を含めること d.4) 【AND】初回評価以前の12か月以内に実施されたものであること	申請者は、データ取扱いを実施する前に、データ取扱いの適法性を評価するための規則又は正式な手順を確立することができる。 申請者のDPO又は法律専門家は、データ取扱いの適法性について意見を提供することが期待される。 適法性を評価する際には、データ取扱いがその正当な利益を超えないよう、比例性を考慮するのが望ましい。 同意は明確であるべきであり、データ主体が同意を表明する不明瞭ではない行為が必要である。例えば、事前にチェックされたチェックボックスは認められない。 専門家の資格又は評価の結論に疑念がある場合、監査人は報告書に異議を唱え、補足評価を要求することが期待される。 同一の報告書は、本要件及び基準G.1.1.5の要件の双方に対応することができる。	適法性評価及び確認の記録及び文書 DPO又は法律専門家との面談 DPO又は法律事務所の書面による声明	6.1	1 7
G.1.1.2	C	S	A	適法性の正当化	データの取扱いは、次のいずれかの正当化根拠のうち少なくとも1つを遵守しなければならない。	申請者は、その個人データの取扱いについて、次のいずれかの適法性の法的根拠に準拠していることを文書化し、これを証明するのが望ましい。取扱活動を実施する前に、全ての個人データの取扱活動が少なくとも次のいずれかの法的根拠に対応していることを確保し、これを証明するための規則、方針、手続又は仕組みを整備することが推奨される。		6.1	
				同意	A) データ取扱いは、次の条件を充足する、データ主体の事前の情報に基づく同意に基づくものでなければならない。 a.1) 当該個人データを取り扱う前に、収集されなければならない。 a.2) 【AND】データ主体によって、明確かつ明示的な方法（明確な積極的行為）で与えられなければならない。	本基準は、詳細基準G.1.2.1を考慮して評価されなければならない。同意が有効であるためには、データ主体は、自身の個人データの取扱いについて、1つ以上の特定の目的のために同意を与えなければならない。申請者は、同意の仕組みを枠付け、かつ、同意が次の要件を充足することを確保するための内部方針、手順若しくは仕組み、又は、その複数を定義及び実施することができる。 - 自由に与えられること - 特定の目的のためであること - 事前に説明を受けていること - 不明瞭でないこと - 陳述又は明確な積極的行動に基づいていること - データを取扱う前に要求されること 該当する場合、申請者は、収集された同意について、同意が与えられた日時を含む電子レジストリを確立するのが望ましい。同意がデータ取扱いの根拠である場合、同意が取得されていない場合又は撤回された場合に個人データの取扱いを防止するための適切な規則、手順又は仕組みが実施されるのが望ましい。	データ主体による同意の記録 ユーザーインターフェース 合意書又は契約条項	6.1.a	1
				契約上の必要性	【OR】 B) データ取扱いは、契約で特定されたサービスの履行に必要でなければならない。	申請者は、データの取扱いが契約の履行又は要求の対応のために比例的かつ必要であることを文書化し、これを証明することができるのが望ましい。申請者は、本法的根拠の利用の基盤となる契約上の必要性を証明及び文書化するための規則、方針、手続又は仕組みを整備するのが望ましい。本手続へのDPOの関与が推奨される。	契約上の根拠 DPO又は法律事務所による契約上の必要性の評価 DPOとの面談	6.1.b	2 1
				法的義務	【OR】 C) データの取扱いは、EU法又はEEA加盟国の国内法に基づく法的義務に基づいて行われなければならない。	申請者は、次の事項を証明できるのが望ましい。 - 取扱いが法的義務の遵守に必要であること（より侵襲的でない利用可能な方法が存在しないこと） - 取扱いが法的義務と比例的であること（取扱いの目的に対して適切かつ関連する個人データのみが収集及び取り扱われていること） GDPR第3条第2項の適用対象となる申請者の法的義務は、EU法又はEEA加盟国の国内法に基づくものであることが期待される	法的根拠 適法性評価の記録又は文書 DPOとの面談	6.1. c	1
				生命に関する利益	【OR】 D) データ取扱いは、データ主体の生命に関する利益（生命、健康）を保護するために必要でなければならない。	申請者は、データ取扱いについて、次の事項を証明できるようにするのが望ましい。 - 主張された生命に関する利益を保護するために必要かつ比例的であること（同一の結果を達成するため、より侵襲的でない利用可能な方法が存在しないこと） - 主張される生命に関する利益を保護するために比例的であること（取扱いの目的に対して適切かつ関連性のある	適法性評価の記録又は文書 DPOとの面談	6.1.d	1

				公益又は公的権限	【OR】 E) データの取扱いは、次の要件を充足しなければならない。 e.1) EU法又はEEA加盟国の国内法により認められた公共の利益に基づくこと e.2) 【AND】当該公共の利益のための法的根拠に関する文書が付されていること	申請者は、次の職務又は機能を証明する記録を保持するのが望ましい。 - 関連するデータ取扱いを実施する明確な権限を提供していること - 【AND】取扱いが職務の遂行に必要かつ適切であること（同一結果をもたらすためのより侵襲的でない方法が存在しないこと）	法的根拠又は行政決定 適法性評価の記録又は文書 DPOとの面談	6.1.e. 6.3			
				正当な利益	【OR】 F) データ取扱いは正当な利益に基づくものでなければならず、その場合、申請者は次の事項を証明しなければならない。 f.1) 主張された正当な利益の書面による記述 f.2) 【AND】申請者は、データ取扱いがデータ主体の権利及び自由に与える影響を文書で評価したこと f.3) 【AND】申請者は、当該正当な利益よりも、データ主体の権利及び自由に優先のほうが優先しないと文書で結論付けたこと f.4) 【AND】DPO又は法律専門家に相談し、その見解が評価に含まれていること	申請者は、次の措置を実施するための手続を整備するのが望ましい。 - データ主体の利益を評価及び文書化すること - 未成年者の個人データの取扱いを特定及び文書化すること 記録には、次の事項を文書化するのが望ましい。 - データ取扱いによって求められる具体的かつ正当な利益 - 取扱活動を実施するために主張される正当な利益の適用可能性の評価 - データ主体の利益及び自由の評価 - 個人データの追加的取扱いに関するデータ主体の合理的期待の評価 - 正当な利益に関するDPOのレビュー - 取扱いが、主張される正当な利益に関連する目的に対して必要かつ比例的であること（同一の結果を達成するために利用可能なより侵襲的でない方法が存在しないこと） 欧州連合司法裁判所は、データ保護指令95/46/ECの文脈において、Rigas事件（C-13/16, 2017年5月4日）における正当な利益に関する三段階テスト（目的、必要性、バランシング）アプローチを確認し	正当な利益に関連する文書 適法性評価の記録又は文書 DPOとの面談	6.1.f		2	
G.1.1.3	CP	S	A	国家固有義務の遵守状況評価	A) 法律専門家は、申請者に適用可能な個人データ保護に関するEEA加盟国の補完的国家固有義務へのデータ取扱いの遵守状況を評価し、その評価を国家固有義務遵守状況評価報告書（NOCAR）に提供しなければならない。 【AND】 B) NOCARには、次の事項が含まれなければならない。 b.1) 評価対象の明確な特定 b.2) 【AND】法律専門家の資格の記述 b.3) 【AND】評価対象に適用可能なEEA加盟国の補完的国家固有データ保護義務の一覧 b.4) 【AND】評価対象のEEA加盟国の国家固有義務への遵守状況の評価 b.5) 【AND】データが保存、研究又は統計目的で取り扱われる場合、データ主体の基本的な権利及び利益を尊重するための技術的措置及び組織的措置（特にデータ最小化措置） b.6) 【AND】評価が、EEA加盟国の国家固有義務にを遵守するために対応が必要と結論付けた場合、当該対応は文書化されなければならない。 【AND】 C) 法律専門家は、次の措置を実施しなければならない。 c.1) ECCPが提供する国家固有データ保護義務プロファイルに一覧化された、適用可能な全てのEEA加盟国の補完的国家固有義務を考慮に入れること c.2) 【AND】他の分野固有のEEA加盟国の国内法及び規制が適用されるか否かを確認すること c.3) 【AND】データ取扱いがEEA加盟国の承認を必要とするか否かを確認し、必要となる承認の有効性を確認すること 【AND】 D) NOCARは、次の要件を充足しなければならない。 d.1) 完全かつ一貫性があること d.2) 【AND】評価対象がEEA加盟国の国家固有義務を遵守していると結論付けること 【AND】 E) 申請者は、次の措置を実施しなければならない。 e.1) NOCAR報告書に文書化された措置を時間をかけて適用することを誓約すること e.2) 【AND】該当する場合、NOCARが推奨する措置を遵守するための詳細な行動計画を策定すること e.3) 【AND】該当する場合、EEA加盟国の国家固有義務を遵守するために必要な行動計画に含まれる措置を適用及び文書化すること	GDPRは、個人データ取扱いに関して「法令の一貫性のある均質な適用」を各加盟国に求めている（前文第10項）。前文第100項及びGDPR第42条において定められているとおり、GDPR認証の目的は、GDPRの遵守状況を評価することである。GDPR前文第10項は、GDPRの均質な適用を要求している。もっとも、GDPRは、加盟国が特定の分野において独自の個人データ保護規制を有することができることを言及している。例えば、特別な種類のデータ（第9条、前文第149項）、犯罪行為（第10条、前文第149項）、未成年者の個人データの取扱い（第8条）及び国家識別番号の取扱い（第87条）である。認証がGDPRと「関連する製品及びサービスのデータ保護水準を即座に評価できる」ことを目的とする一方（前文第100項）、各国のデータ保護関連規制に違反するデータ取扱いに対して認証を付与しないようにするため、申請者は、自らの取扱活動が評価対象に適用可能なEEA各国の各国規制を遵守しているか否かを確認することが期待される。NOCARで考慮された法域は認証書に記載され、公式の認証レジストリを通じてオンラインで公開される。 各国規制は、尊重すべき補完的データ保護義務が含まれる。適用可能な各国規制に関する十分な専門知識を有する法律専門家が、認証を受けるデータ取扱活動が適用可能な補完的各国法令及び規制（分野固有のものを含む）を遵守しているか否かを評価しなければならない。本評価は、内部又は外部の専門家によって実施することができ、これには、申請者のDPOが適用可能な各国規制に関する必要な法的専門知識を有し、かつ、独立性の要件と矛盾しない場合には、DPOも含まれる。 ECCPは「国家固有義務遵守状況評価報告書（NOCAR）に関するユーロプライバシーガイドライン」を提供しており、作成すべき報告書の内容及び構造を詳細に定めている。監査人はNOCARをレビューし、その内容に基づいて、NOCARが完全、適切かつ整合的であるかを判断しなければならず、事実に基づき報告書及びその結論に信頼性が認められないと判断する場合は、これを拒否しなければならない。また、ECCPは、評価及びNOCARのレビューを実施する際に重要な国家固有義務の見落としがないように、全てのユーロプライバシー申請者及び監査人に提供される特定された補完的国家固有要件の一覧（国家固有データ保護義務プロファイル）も提供している。評価は、データ取扱いが国家当局による承認の対象であるか否かを考慮し、当該承認が付与されていることを確認するのが望ましい。特別な種類のデータ、ビデオ監視、公共空間におけるIoT展、又はウェブサイトのクッキーを含むデータ取扱いは、特定の国家固有義務及び潜在的承認の対象となる可能性があり、これらは確認されなければならない。 国家固有義務は、セキュリティ要件、データ保護影響評価、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など、いくつかの基準に影響を与える可能性がある。NOCAR報告書が申請者によって採用されるべき是正措置を特定している場合、申請者は詳細な是正措置計画を作成しなければならない。認証機関は、法律専門家によって定義された推奨措置の実施に対する評価に限定することはない。認証機関は、（法律専門家の独自の評価前に実施されたか否かに関わらず、）申請者がNOCARに記載された措置を実施したか否かを確認する責任がある。 データが公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために取り扱われる場合、（GDPR第89条が要求するとおり、）データ主体の基本的な権利及び利益を尊重するため、仮名化又は匿名化などのデータ最小化のための特定の措置を講じる義務がある。本要件の効果的な実施は、基準G.6.1.1によって確認される。b5) て要求される措置の適切性は、基準G.6.1.1「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」を通じて	国家固有義務遵守状況評価報告書（NOCAR）のレビュー	6.2, 6.3, 89		4	
G.1.1.4	CP	S	A	NOCAR専門家の十分な資格	【IF】NOCARが必要となる場合、【THEN】次のとおりとする。 A) NOCARを作成又は取りまとめた法律専門家は、EUの法域においてデータ保護オフィサーとして行動するために必要な資格を有さなければならない。	法律専門家は、国家固有義務遵守状況評価報告書において評価される国内法及び規制に関する十分な専門知識を有さなければならない。当該法律専門家は、適用可能な各国規制に関する専門知識の水準を証明することが不可欠である。期待される専門知識の水準は、EDPBガイドラインに従い、又は、適用可能な各国規制に従い、GDPR第42条及び第43条に基づく監査及び認証活動に参加する法律専門家に必要な資格と少なくとも同等であるのが望ましい。	NOCAR及び専門家の資格の文書レビュー	6.2, 6.3	1	1	
G.1.1.5	CP	S	A	EEA域外に所在する申請者に関する法の抵触の可能性	【IF】申請者が評価対象を包含する十分性認定のない第三国に所在する場合、【THEN】次のとおりとする。 A) 申請者のために作成された申請者の国の法及び慣行に関する書面による報告書が存在し、少なくとも次の事項を記述しなければならない。 a.1) 評価対象 a.2) 【AND】政府による個人データへのアクセス（ガバメントアクセス）に関する当該国の法律及び慣行（取扱いデータへのガバメントアクセスを制限するための保護措置、ガバメントアクセスに対する独立した監督、及び、データ主体に対する救済手段を含む） a.3) 【AND】当該国の法及び慣行がデータ主体の権利及び自由の保護のレベルに与えるリスク及び影響のマッピング及び評価 a.4) 【AND】影響を受けるGDPR要件のマッピング及び評価 a.5) 【AND】該当する場合、取り扱われるデータ並びにデータ主体の権利及び自由を保護するための補完的措置に関する推奨 【AND】 B) 報告書は、次の要件を充足しなければならない。 b.1) 当該国の法及び慣行に関する専門的知識を有することが証明された法律専門家によって作成されていること b.2) 【AND】当該法律専門家の独立性のレベルが含まれていること 【AND】 C) 報告書は、申請者の国の法及び慣行について、次の事項を結論付けていなければならない。 c.1) 申請者がGDPRに基づく適用可能なデータ保護義務を履行するのを妨げないこと c.2) 【AND】申請者がユーロプライバシー認証に関連する契約上の義務を履行するのを妨げないこと c.3) 【AND】データ主体の基本的権利及び自由の本質的部分を尊重すること c.4) 【AND】GDPR第23条第1項に定める対象のいずれかを保護するために民主主義の社会において必要かつ比例的な範囲を超えないこと c.5) 【AND】データ主体の権利及び自由を保護するための適切な保護措置を提供すること 【AND】 D) 申請者は、次の措置を実施しなければならない	申請者がEEA域外に所在し、GDPR第3条第2項の適用を受ける場合、移転を伴わない場合（したがって、G.10基準では対処できなかった場合）であっても、法の抵触が生じるリスクがある。EDPBガイドラインに従い、法的根拠が取り扱われたデータ並びにデータ主体の権利及び自由の保護を損なわないのを確保することが重要である。 第三国法が次の要件を充足することを確保するため、当該法はGDPR第23条に従い評価されるのが望ましい。 - データ保護権に対して、民主主義の社会において必要かつ比例的な範囲を超える制限を課さないこと - 求められる目的に適合するものであること - データ保護の権利の本質的部分を尊重すること - データ主体の基本的権利及び利益を保護するための具体的な措置を提供すること 同一の報告書は、基準G.1.1.1の要件に対応することができる。 第三国法が上記の条件を充足しないと評価された場合、申請者は、当該第三国の法及び慣行が、c1からc4に詳細に定められた要件の遵守を妨げないこと確保するため、必要な補完的措置を採用することが期待される。第三国法が上記要件を充足せず、補完的措置を特定及び実施できない場合、第三国法との不適合が生じ、申請者は認証を進めることができない。 法律専門家は、第三国の法令、国内法及び欧州のデータ保護法（GDPRに関する深い理解を含む）についての専門知識、並びに、申請者の規則、手続及び手順に関する理解を証明するのが望ましい。報告が独立した専門家によって実施されない場合、認証機関はより詳細なレビューを実施するのが望ましい。 申請者が複数の拠点を有する場合でも、申請はそのうち1つの拠点についてのみ申請を行うことができる。 また、EDPBの補完的措置に関する必須保証についてのEDPB勧告01/2020、監視措置に関する欧州保証についてのEDPB 02/2020及びGDPR第23条の制限に関するEDPBガイダンスも参照されたい。 申請者がEEA域外に設立され、評価対象において実施される取扱いに関連する十分性認定の利益を享受している場合、本要件の遵守は簡略化された報告書をよって示すことができる。当該報告書は、評価対象が十分性認定の適用範囲に含まれる理由を文書化するのが望ましい。	規制環境評価又は移転影響評価の文書レビュー	6.1, 10	1	15	

G.1.1.6	C	G	A	一般的目的制限	A) 申請者は、データの追加的取扱いが次の条件を充足することを確保するための方針、手順、規則又は仕組みを整備しなければならない。 a.1) データが収集された目的と適合すること a.2) 【OR】公共の利益に資する保存目的、科学的若しくは歴史的研究目的、又は、統計目的のために行われること a.3)【OR】（G.1.1.2に規定される）別の適法根拠に基づくものであること 【AND】 B) 当該目的が適合するか否かを判断するため、申請者は、次の事項を評価しなければならない。 b.1) 個人データが収集された目的と意図される追加的取扱いの目的との関連性 b.2)【AND】個人データが収集された文脈 b.3)【AND】個人データの性質 b.4)【AND】データ主体に与え得る意図する追加的取扱いの結果	申請者は、特定され、明確であり、かつ、正当な目的のためにのみデータを取扱い、これらの目的と両立しない方法で追加的に取扱ってはならない。いかなる追加的取扱いについても、別途、その適法性が評価されるべきである。	文書レビュー 面談	5.1.b , 6.4					
G.1.2				**（該当する場合、）同意が有効であるための補完的要件** 条件	【IF】データ取扱いの適法性が同意に基づく場合、【THEN】次のとおりとする。			**7**			
G.1.2.1	C	S	A	同意の 形式的要件	A) データ主体の同意は、次の事項を確保することにより、事前に与えられ、かつ、事前に説明を受けた上でのものでなければならない。 a.1) データ取扱いの目的及び管理者の身元に関する情報は、同意前又は同意時にデータ主体に連絡されなければならない。 a.2)【AND】同意は特定の目的のために要請されなければならない。 a.3)【AND】同意の要請は、容易に理解可能な方法で表現されなければならない。 a.4) 【AND】書面で作成される場合、同意の要請は、他の事項とは区別できる別の段落で提示されなければならない。 a.5)【AND】同意は、申請者が個人データを取り扱う前に収集されなければならない。 a.6) 【AND】データ主体の同意は、明確かつ明示的な方法で（明確な積極的行為により）で与えられなければならない。 a.7)【AND】同意は、取扱いが行われる各目的を対象としていなければならない。 【AND】 B) データ主体の同意は、次の事項を確保することを含め、自由に与えられなければならない。 b.1) データ主体は、不利益を被ることなく、同意を制限又は放棄することができる。 b.2) 【AND】評価対象がデータ取扱いの複数の目的を含む場合、申請者は、データ主体がどの目的に同意するかを自由に選択できるように、きめ細かな同意の仕組みを提供しなければならない。	申請者は、事前にチェックされたボックスはGDPR（第5条～第6条、第7条）に照らして有効な同意として認められないことを留意するのが望ましい。 同意は、データ主体のデータ取扱いに対する同意の意思の不明確ではない「表示」を必要とする。データ主体が同意を与えるために行う積極的な行動のみが、本要件を充足することができる。GDPRは「沈黙、予めチェック済みのボックス又は不作為」が同意を構成することを排除している。 オンラインサービス、アプリケーション又はユーザーインターフェースのためにプラグイン及びマイクロサービスを使用する場合、申請者は、当該プラグイン及びマイクロサービスがGDPRを遵守していること、これがデータ主体に明確に通知されていることを確保するのが望ましい。 本宣言のいかなる部分であっても、本規則に違反するものは拘束力を有さない。 同意手順は、データ管理者が積極的に同意を収集しようとする地域の様々な国語で利用可能とすることが推奨される。	同意を収集するために使用される手順、ユーザーインターフェース又は仕組み DPOとの面談 手順の試験	7.2					
G.1.2.2	C	S	A	同意を撤回する権利	A) 申請者は、データ主体の同意を撤回する権利を遵守するための手順又は仕組みが要求の効果的な実施を可能にすることを証明しなければならない。 【AND】 B) 同意の撤回手続は、次の要件を充足しなければならない。 b.1) 同意の収集のために用いられるものと同じように、簡単なものであること b.2)【AND】同意を収集するために使用されるユーザーインターフェースを通じて利用できること b.3)【AND】データ主体に不利益を与えないこと	申請者は、DPOに対し、内部の同意撤回管理方針、手順、運用指針及び仕組みを検討し、意見を提供するよう依頼するのが望ましい。なお、同意の撤回は、撤回前の同意に基づく取扱いの適法性に影響を及ぼさない。同意を与える前に、データ主体に対してその旨が通知されるのが望ましい。	同意撤回のために使用される手順、ユーザーインターフェース又は仕組み DPOとの面談 同意撤回のための手順の試験	7.3					
G.1.3				**（該当する場合、）情報社会サービスに関して子どもの同意に適用可能な条件** 条件	【IF】評価対象が、16歳未満の子どもに直接提供される情報社会サービスを含む場合、【THEN】次のとおりとする。			**8**			
G.1.3.1	C	S	A	子どものデータ取扱いの適法性及び親権者の同意の検証	A) 同意に適用される年齢の制限は、データ取扱いに関連する潜在的な新規のデータ主体に明確に連絡されなければならない。 【AND】 B) 次の措置を講じるための手順若しくは仕組み、又は、その両方がなければならない。 b.1) 未成年者であるデータ主体の年齢を要求すること b.2) 【AND】同意年齢に満たない未成年者の個人データの収集を阻止すること、又は、同意年齢に満たない未成年者の親権者の同意を求めること	未成年者にサービスを提供する際、申請者は、収集した同意について、同意が与えられた日時を含む電子レジストリを整備することが推奨される。 同意は明確であり、親権者による不明瞭でない確認を必要とするのが望ましい。オンライン登録手続において、申請者は親権者からの確認メールを求めることができる。 申請者は、適用可能な各国規制（年齢制限が異なる場合がある）を考慮すべきである。当該規制には、対象となる子どもが所在するEEA加盟国の国内法が含まれる。加盟国は、その目的のために、13歳を下回らない範囲で、より低い年齢を国内法により定めることができる。	同意撤回のために使用される手順、ユーザーインターフェース又は仕組み DPOとの面談 同意撤回のための手順の試験	8.1, 8.2					
G.2				**特別なデータ取扱い** 目的	評価対象において取り扱われる特別な種類のデータが、規制要件を遵守するのを確保すること。						
G.2.1				**特別な種類のデータの取扱いの遵守** 条件	【IF】評価対象が特別な種類の個人データを取り扱う場合、【THEN】次のとおりとする。			**9**			
G.2.1.1	C	S	A	特別な種類のデータ ーDPOの関与	A) 申請者は、次の措置を実施しなければならない。 a.1) データ主体の権利、自由及び正当な利益に対する特別な種類のデータの取扱いのリスク及び影響を評価すること a.2)【AND】特別な種類のデータの取扱いの適法性を確認すること 【AND】 B) 申請者は、DPO又は法律専門家と協議し、その所見を当該評価に含めなければならない。	申請者は評価対象において取扱われるデータの種類について、体系的な棚卸しを行うのが望ましい。 特別な種類のデータの取扱いは、DPO又は法律専門家によって慎重に分析されるのが望ましい。特に、データ主体の権利及び自由に対するリスク分析に注意が払われるのが望ましい。申請者がEEA域外に所在し、GDPR第3条第2項の適用対象となる場合、たとえ移転が伴わない場合であっても（したがって、G.10基準では対応できなかった場合であっても）、法の抵触が生じるリスクがある。EDPBガイドラインに従い、法的根拠が取る扱われるデータ並びにデータ主体の権利及び自由の保護のレベルが低下しないことを確保することが重要である。 特別な種類のデータが同意に基づいて取り扱われる場合、適用可能なEU法又は加盟国の国内法によって同意が禁止されていないことを確認及び確保することが期待される。	リスクアセスメント及び適法性評価報告書（DPO又は法律専門家の意見を含む） NOCAR報告書	9					
G.2.1.2	C	S	A	特殊な種類のデータの取扱いに関する例外	評価対象における特別な種類の個人データの取扱いは、次の正当化根拠のいずれか1つに基づき適法である。	申請者は、DPO又は法律専門家に対し、特殊な種類のデータの取扱いが次の要件をいずれも充足することを確保するため、特に確認し、意見を提供するよう依頼するのが望ましい。 - GDPRの要件及び適用可能な各国規制を遵守していること - 必要な場合、承認されていること	適法性評価報告書 NOCAR報告書 DPOとの面談	9					
				明確な同意	A) 特別な種類のデータ取扱いは、EU法又はEEA加盟国の国内法により禁止されている場合を除き、データ主体の明確な同意に基づかなければならない。	申請者は、DPOに対し、内部の同意管理方針、手順、運用指針及び仕組みを検討し、意見を提供するよう依頼することができる。	同意の収集及び撤回のために使用される手順、ユーザーインターフェース又は仕組みの試験	9.2.a					
				雇用、社会保障、保護（一般）	【OR】 B) 特別な種類のデータの取扱いは、次の要件を充足しなければならない。 b.1) 雇用及び社会的必要性に基づくものであること b.2) 【AND】EU法若しくはEEA加盟国の国内法により認められ、又は、データ主体のための保護措置を定めるEU法若しくはEEA加盟国の国内法による団体協約によって認められること	申請者は、データの取扱いが次の要件を充足することを証明する記録を保持するのが望ましい。 - 雇用、社会保障又は社会保護の法律の分野に関連していること - 管理者又はデータ主体の義務の履行又は権利の行使を目的としていること - 職務の遂行に必要かつ比例的であること（同一の結果を達成するために利用可能なより侵襲的でない方法が存在しないこと） - データ主体の基本的権利及び利益に対して適切な保護措置を提供していること 該当する場合、GDPR第3条第2項に基づきGDPRの適用対象となる申請者は、基準G.1.1.5を適用する際に、雇用、社会保障及び社会保護のためのデータ取扱いの法的根拠として、EU法又はEEA加盟国の国内法に基づく法的根拠を含めることが期待される。	文書レビュー DPOとの面談	9.2.b					
				生命に関する利益	【OR】 C) 申請者は、特別な種類のデータの取扱いが生命に関する利益に基づくものであることを証明しなければならず、その場合には次の条件を充足しなければならない。 c.1) データ主体の生命に関する利益（生命、健康）が危険にさらされていた場合 c.2)【AND】関連するデータ主体又は保護される自然人が、物理的又は法的に同意を与えることができない場合	申請者は、次の事項を証明する記録を保持するのが望ましい。 - データ主体の生命に関する利益が危険にさらされたこと（生命、健康） - 取扱いが職務の遂行に必要かつ比例的であること（同一の結果を達成するために利用可能なより侵襲的でない方法が存在しないこと） - データ主体又は保護された自然人が同意を提供することが物理的又は法的に不可能であること - DPO又は法律専門家が、かかる生命に関する利益に基づく取扱いの手続きについて意見を提供したこと	生命に関する利益の評価及び決定プロセスの記録及び文書 DPOとの面談	9.2.c					

				正当な利益を持つ非営利団体	【OR】 D) 特別な種類のデータ取扱いは、非営利組織の正当な活動の過程で行われなければならず、その場合には次の条件を充足しなければならない。 d.1) 申請者が非営利組織であること d.2) 【AND】取り扱われるデータが、申請者のメンバー及び元メンバー、若しくは、申請者の目的に関連して申請者と継続的に接触を持つ者、又は、その両方のみに関連すること d.3) 【AND】当該取扱いが非営利組織の目的と適合すること d.4)	申請者は、データ取扱いが、データ主体が申請者に合理的に期待し得る目的に対して比例的であることを確保するのが望ましい。GDPR第9条第2項d は、「政治、思想、宗教又は労働組合の目的による団体、協会その他の非営利組織による適切な保護措置を具備する正当な活動の過程において、当該取扱いが、その組織の構成員若しくは元構成員、又は、その組織の目的と関係してその組織と継続的に接触をもつ者のみに関するものであることを条件とし、かつ、データ主体の同意なくその個人データが当該組織の外部に開示されないことを条件として、取扱いが行われる場合」と述べている。	組織の内規 取扱活動の目録 労働者及びDPOとの面談 内部規則及びガイドライン	9.2.d	4
				公開データ	E) 特別な種類のデータの取扱いは、データ主体によって公開のものとされたデータに基づかなければならない。	申請者は、データがデータ主体によって明白に公開のものとされたことを証明できるようにするのが望ましい。	データ収集に関する文書 データ取扱活動の記録 データサンプル分析 労働者及びDPOとの面談	9.2.e	1
				法的主張	特別な種類のデータの取扱いは、訴えの提起若しくは攻撃防御のため、又は、裁判所がその司法上の権能を行使するために必要でなければならない。	申請者は、差し迫った又は進行中の法的措置に関する文書化された証拠を有するのが望ましい。	法的主張及び裁判に関する文書 労働者及びDPOとの面談	9.2.f	1
				公共の利益	G) 特別な種類のデータの取扱いは、公共の利益の理由のために必要でなければならず、その場合には次の条件を充足しなければならない。 g.1) 公共の利益はEU法又はEEA加盟国の国内法に基づくものであること g.2) 【AND】データ主体の権利を保護するための措置が採用されていること	申請者は、次の事項を証明するための記録又は証拠を保持するのが望ましい。 - DPO又は上級管理職が、データ主体の権利、自由及び正当な利益に対するリスクの評価に貢献したこと - データの取扱いが、職務の遂行に必要かつ比例的であること	法的根拠又は行政上の根拠を含む、公共の利益に関する文書 DPOとの面談 DPOによる適法性評価の文書	9.2.g	2
				健康及び業務遂行能力	H) 特別な種類のデータの取扱いは、医療又は社会福祉の目的のために必要でなければならず、その場合には次の条件を充足しなければならない。 h.1) 取扱いが、予防医学又は産業医学、労働者の業務遂行能力の評価、医療上の診断、医療若しくは社会福祉又は治療の提供、又は、医療制度若しくは社会福祉制度及びそのサービス提供の管理のいずれかの活動に関連するものであること h.2) 【AND】当該データが、職業上の守秘義務に服する職にある者によって、又は、そのような者の責任の下で取扱われること h.3) 【AND】当該データが、EU法又はEEA加盟国の国内法に基づいて取扱われること	申請者は、次の事項を証明する記録又は証拠を保持するのが望ましい。 - 取扱いが、法的根拠又は医療専門家との契約に基づいていること - 取扱いが、職務の遂行に必要かつ比例的であること（同一の結果を達成するために利用可能なより侵襲的でない方法が存在しないこと） - 当該専門家は処理者の守秘義務の対象であること 健康及び業務遂行能力の必要性に基づいて行われる取扱い（GDPR第9条第2項h)については、次の事項が求められる。 - 必要性の原則を充足すること - EU法又はEEA加盟国の国内法により規定された法的義務に基づくこと 該当する場合、GDPR	適法性評価の記録及び文書 DPOとの面談 労働者の契約条項 内部規則	9.2.h	4
				公衆衛生	I) 特別な種類のデータの取扱いは、公衆衛生の分野における公共の利益の理由のために必要でなければならず、その場合には次の条件を充足しなければならない。 i.1) 公衆衛生の分野における公共の利益は、EU法又はEEA加盟国の国内法により定められた法的根拠に基づくものであること i.2) 【AND】データ主体の権利及び自由を保護するための措置が講じられていること i.3)	データ主体の権利及び利益を保護するための措置には、次の事項を確保するための方針、手続又は仕組みが含まれ得る。 - 申請者がリスクを評価し、特別な種類のデータの取扱いに関する決定をデータ主体の権利、自由並及び正当な利益とのバランスを考慮していること - 特別な種類のデータにアクセスする申請者の要員が職業上の守秘義務に拘束されていること	公共の利益に関する文書 DPOとの面談 法的根拠又は行政上の根拠 適法性評価の記録及び文書	9.2.i	3
				保管、研究、統計の目的	J) 特別な種類のデータの取扱いは、公共の利益における保管の目的、科学的研究若しくは歴史的研究の目的又は統計の目的のために必要でなければならず、その場合には次の条件を充足しなければならない。 j.1) 申請者が、取り扱われるデータが宣言された目的のために有用かつ比例的であることを評価及び確認していること j.2) 【AND】仮名化及び匿名化の技術などの具体的な措置が、データ主体の権利及び利益を保護するために採用されていること。	データ主体の権利及び利益を保護するための措置には、次の事項を確保にするための方針、手続又は仕組みが含まれる。 - トップマネジメントがデータ主体の権利、自由及び正当な利益に対するリスクを評価していること - 取扱いの目的に関連する要件と整合する場合、特別なデータの種類が仮名化又は匿名化されていること - 評価及び実施された保護措置がDPOによってレビューされていること	オンライン情報を含むプロジェクト文書 DPOによる適法性評価の文書	9.2.j	3
G.2.1.3	C	S	A	特殊な種類のデータ取扱いに関する追加的な	申請者は、データの性質及びそれに伴うリスクに応じて、特別な種類のデータを保護するための追加の制限及び保護措置を講じなければならない。	追加的な制限及び保護措置には、個人データにアクセスすることが許可される要員の制限、追加的なセキュリティ対策（仮名化など）、若しくは、データのさらなる開示に関する追加的な制限、又は、その複数が含まれ得る。	規則、方針又は仕組み 制限及び保護措置	9	1 1
G.2.2				**（該当する場合、）有罪判決及び犯罪行為に関するデータの取扱い**				**10**	
				条件	【IF】評価対象が有罪判決若しくは犯罪行為、又は、その両方に関連するデータの取扱いを目的とする場合、【THEN】次のとおりとする。				
G.2.2.1	C	S	A	有罪判決及び犯罪行為に関連するデータ	A) 有罪判決及び犯罪行為に関する個人データの取扱いは、次のとおりとする。 a.1) 公的機関の管理の下にあるか、又は、EU法若しくはEEA加盟国の国内法によって認められなければならない。 a.2) 【AND】公的機関の管理の下にある場合を除き、有罪判決の包括的な記録を構成してはならない。 【AND】 B) 有罪判決若しくは犯罪行為、又は、その両方に関連するデータの取扱いは、次のとおりでなければならない。 b.1) 管理され、かつ、遵守していると評価されること b.2) 【AND】申請者の経営陣によって承認されていること	申請者は、有罪判決及び犯罪行為に関するデータの取扱いを認める法的根拠を文書化するのが望ましい。当該文書は、適用可能な各国規制を明確に特定するのが望ましい。	文書レビュー（G.1.1.1参照） DPOとの面談	10	1 4
G.3				**データ主体の権利**					
				目的	評価対象におけるデータの取扱いがデータ主体の権利の実効的行使を尊重し、可能にするのを確保すること。				
G.3.1				**データ主体の権利行使のための透明性のある情報提供、連絡及び書式**				**12**	
G.3.1.1	C	S	A	明確な文言による通知義務	A) 申請者がデータ主体及び利害関係者に提供するデータ取扱いに関する情報は、次の要件を充足しなければならない。 a.1) 簡潔で、透明性があること a.2) 【AND】理解しやすく、容易にアクセスできる方式であること a.3) 【AND】明確かつ平易な文言であること a.4) 【AND】書面又はその他の方法（電子的な方法など）により提供されること a.5) 【AND】申請者の公用語で利用可能であること a.6) 【AND】対象となるデータ主体の言語で利用可能であること 【AND】 B) 【IF】評価対象において子どもの個人データの取扱いが含まれる場合、【THEN】その情報は評価され、子どもにとって適切かつ理解可能であると評価され、そのように認められなければならない。	申請者は、次の要件を充足する情報を簡潔で、透明性があり、理解しやすく、容易にアクセスできる方式により、明確かつ平易な文言を用いて、書面で提供するのが望ましい（参照：WP29 ガイドライン WP260 Rev.01）。 - 簡潔で、透明性があること（情報過多を避けるため、情報は構造化され、効率的かつ簡潔であるのが望ましい） - 理解可能であること（情報は、対象となる対象読者の平均的なメンバーによって理解されるのが望ましい） - 容易にアクセスできること（データ主体は情報を探し求める必要がなく、情報は当該データ主体にとって直ちに明らかであるのが望ましい） - 明確かつ平易な文言を用いること（解釈の余地を避けるため、情報は可能な限り平易かつ簡潔な方法で提供されるのが望ましい） 書面以外の手段も使用することができる。ウェブサイト訪問者が関連する特定の事項にアクセスできるようにする階層型のプライバシーステートメント／プライバシーノーティスの活用が推奨される。情報提供の方法は、状況及び提供される情報に応じて適切であるのが望ましい。データ主体の本人確認がなされている場合、口頭で情	データ主体に提供されるユーザーインターフェース及び情報資料 （該当する場合）契約条項	12.1	1 7
G.3.1.2	C	G	A	データ主体の権利行使を容易にする義務	A) 申請者は、次の事項を証明しなければならない。 a.1) データ主体に対し、申請者の公にアクセス可能な手段（ウェブサイトなど）を通じて、権利を行使する方法を通知すること a.2) 【AND】データ主体の要求の取扱方法について、教育、訓練を受けた要員を有すること	申請者は、データ主体の権利行使を容易にしなければならない。管理者は、データ主体を特定することができないことを証明する場合を除き、第15条から第22条に基づくデータ主体の権利を行使するための要求への対応を拒否しないことが期待される。	ウェブサイトを含むデータ主体に提供される情報	12.2	1 2

G.3.1.3	C	G	A	適切なデータ主体の権利管理及び記録の確保	A) 申請者は、次の措置を実施するための手順又は仕組みを整備しなければならない。 a.1) データ主体からの全ての要求を受領及び記録すること a.2) 【AND】当該要求の受領をデータ主体に確認すること a.3) 【AND】データ主体の身元を識別又は認証すること a.4) 【AND】要求に応じるために全ての条件を充足しているかを評価及び確認すること a.5) 【AND】当該要求に応じるか、又は、拒否すること a.6) 【AND】データ主体からの要求の受領から、申請者による回答若しくは対応、又は、その両方までの遅延を管理すること 【AND】 B) 申請者は、次の記録を保持しなければならない。 b.1) データ主体の識別又は認証 b.2) データ主体の要求及びその受領日 b.3) 【AND】データ主体との連絡及びその日付 b.4) 【AND】フォローアップ措置及びその日付 b.5) 【AND】該当する場合、受領した要求に応じない理由	明確な文書による手順又は技術的解決策は、データ主体が申請者に要求を行うたびに、当該要求が記録され、不当な遅延なく取り扱われることを確保するのが望ましい。監査人は、データ主体であるかのように試験を実施できるのが望ましい。要求の提出方法に関する情報を見つけることができ、模擬的な要求を行い、当該要求がどのように記録され、フォローアップされるかを確認できるのが望ましい。 当該記録には、データ移転の仕組みとしての利用の利用に関連する苦情を含めることができるのが望ましい。	データ主体の要求管理のための手順又は仕組み 可能な場合、過去のデータ主体の要求の記録	12.2		1	11
G.3.1.4	C	G	A	不当な遅延のない情報	A) 申請者は、整備されている手順又は仕組みが、次の措置のために有効かつ適切であることを証明しなければならない。 a.1) データ主体から受領した要求を記録すること a.2) 【AND】受領した要求に対し、1か月以内かつ不当な遅延なく対処及び回答すること	申請者は、次の事項について体系的な記録を保持するのが望ましい。 - データ主体から受けた要求（日付を含む） - データ主体とのフォローアップに関する連絡（日付を含む） - 受けた要求に対応するために講じた措置（日付を含む） - 該当する場合、受領した要求に応じなかった理由 a.2に記載された1か月の期間は、要求の複雑さ及び件数を考慮し、必要に応じてさらに2か月延長できる。管理者は、データ主体に対し、当該要求の受けた時から1か月以内に、その遅延の理由とともに、当該延長をて通知することが期待される。	データ主体の要求管理のための手順又は仕組み 可能な場合、データ主体の要求の記録のサンプル分析	12.3		1	2
G.3.1.5	C	G	A	電子的応答	A) 申請者は、データ主体が電子的な手段により要求を行った場合、原則として、情報も電子的な手段により提供されることを確保するための規則、手順又は仕組みを整備しなければならない。	申請者は、次を実施するための手順又は仕組みを整備しているのが望ましい。 - データ主体が電子的な手段によりデータ主体からの要求を提出できるようにすること - データ主体が要求に対して電子的な手段で返信し、これに応じること - データ主体が要求した形式でデータ主体からの要求に返信し、これに応じること	ユーザーインターフェース データ主体の要求管理のための手順又は仕組み	12.3		1	1
G.3.1.6	C	G	A	不作為を正当化する通知義務	A) 申請者は、データ主体からの要求に応じない場合について、その旨を通知し、かかる不作為を正当化するための規則、手順又は仕組みを整備しなければならない。 【AND】 B) 申請者は、データ主体からの情報要求に対応しないことを決定した場合、データ主体に対し、当該要求の受領から1か月以内に次の事項を通知しなければならない。 b.1) 対応しない理由 b.2) 【AND】所轄データ保護機関に対する苦情申立ての権利 b.3) 【AND】司法救済を求める可能性	第15条から第22条に定める要求を行う自然人の身元に関して管理者が合理的な疑いをもつ場合、当該管理者は、当該データ主体の身元を確認するために必要な追加的な情報の提供を求めるのが望ましい。 管理者は、データ主体が個人データの取扱いがGDPRに違反していると考える場合はいつでもEEA域内のデータ保護機関に苦情を申し立てる権利を有することを、明確かつ透明性のある方法で、データ主体に通知するのが望ましい（GDPR第77条参照）。 管理者は、データ主体が苦情を申し立てることができるデータ保護機関と、苦情を主監督機関として調査することができる所轄データ保護機関を区別するのが望ましい。しかし、本基準は透明性の要件に関連しているため、本文脈において、いかなる場合でも、所轄データ保護機関は、データ主体がGDPR第77条に従って苦情を申し立てることができるデータ保護機関である。 さらに、個人データを取り扱う管理者に対して苦情を申し立てるため、データ主体は苦情を申し立てるためにEEAに「所在」する必要はない。所轄データ保護機関を本基準において直接特定するため、GDPR第77条の文言を適用するのが望ましい。	データ主体の要求管理のための手順又は仕組み 可能な場合、データ主体の要求の記録のサンプル分析	12.4. 12.6		1	4
G.3.1.7	C	G	A	無償	A) 原則として、申請者は、データ主体の権利行使の要求に関連して、データ主体に対していかなる費用も請求してはならない。 【AND】 B) 【IF】申請者が、正当化されない要求又は過剰な要求に対してデータ主体に課金する意図がある場合、【THEN】申請者は次の事項を文書化した手順を整備しなければならない。 b.1) 要求が明らかに根拠がないか否かを事実に基づき評価すること b.2) 無償の情報提供を行わない決定には、事実に基づく正当化を文書化すること b.3) 明らかに根拠がないと認められる場合、関連する要求の業務運営費用を評価すること b.4)	データ主体からの要求が、特に反復して行われることからして、明らかに根拠がない場合又は過剰な性質のものである場合、管理者は、次のいずれかの措置を講じることができる。 （a）情報若しくは連絡を提供すること、又は、業務運営費用を考慮に入れ、合理的な手数料を課金すること （b）要求された行行為を拒むこと いかなる場合でも、データ主体から要求された最初の複製物は、その分量及び必要な労力に関わらず、無償で提供される。	データ主体の要求管理のための手順又は仕組み 可能な場合、データ主体の要求の記録のサンプル分析	12.5		1	6
G.3.1.8	C	G	A	アイコンの機械可読性	【IF】申請者が、電子的な手段により、データ主体にデータ保護ポリシーを通知するため、アイコンを使用する場合、【THEN】次のとおりとする。 A) 申請者は、データ主体にデータ保護ポリシーを通知するために使用されるアイコンが、機械可読であることを証明しなければならない。	申請者が、データ主体に対し、電子的な手段により、データ保護ポリシーを通知するためにアイコンを使用する場合、機械可読なアイコンを使用することが期待される。例えば、盲目などの障害を持つデータ主体が、テキスト読み上げアプリケーションを通じてユーザーインターフェース上で提供される情報にアクセスできることが重要である。	ユーザーインターフェース上で連絡されるデータ保護ポリシー 該当する場合、アイコンの読みやすさの技術的試	12.7		1	1
G.3.2				**データ主体から個人データが収集される場合に提供すべき情報** 条件	【IF】評価対象がデータ主体から直接取得したデータを取り扱う場合、【THEN】次のとおりとする。 ［ただし、G.3.2.3に従って免除が証明できる場合を除く。］			**13**			
G.3.2.1	C	S	A	通知義務	データ収集時にデータ主体に提供される情報には、少なくとも、次の情報が含まれなければならない。	申請者は、個人データを収集する際に、データ主体に対して明確な情報を提供する義務がある。データ輸出者として行動する申請者は、GDPR 第46条の範囲内で特定された移転、そのデータ輸入者、並びに、データ主体の権利及び第三国法に関連する義務についての情報を提供する義務がある。 a.22) に関して、GDPR 第77条は「他の行政上の救済又は司法上の救済を妨げることなく、全てのデータ主体は、そのデータ主体が、自己と関係する個人データの取扱いが本規則に違反すると判断するときは、特に、データ主体の居住地の加盟国、就業場所の加盟国又は違反行為があると主張する場所の加盟国において、監督機関に異議を申立てる権利を有する。」と明確にしている。 データ主体は、EEA域内のデータ保護機関を選択する権利を有する。	ユーザーインターフェース又はデータ主体との契約条項 可能な場合、データ主体に送信された情報の記録			1	
				管理者の詳細	A) 管理者及びDPOの詳細。すなわち、次の情報。 a.1) 管理者の身元、及び、該当する場合にはその代表者の身元 a.2) 【AND】管理者の連絡先、及び、該当する場合にはその権限を与えられた代表者の連絡先			13.1.a		2	
				DPOの連絡先	a.3) 【AND】データ保護オフィサーの連絡先（又は連絡方法）			13.1.b		1	
				目的	【AND】 B) データの取扱いに関する情報。すなわち、次の情報。 b.1) 取扱目的			13.1.c		1	
				法的根拠	b.2) 【AND】取扱いの法的根拠			13.1.c		1	
				正当な利益	b.3) 【AND】該当する場合、管理者又は第三者によって求められる正当な利益			13.1.d		1	
				保持期間	b.4) 【AND】保持期間、又は、それが不可能な場合には保持期間を決定するための基準			13.2.a		1	
				要件の性質	b.5) 【AND】当該個人データの提供が制定法上若しくは契約上の要件であるか否か、契約を締結する際に必要な要件であるか否か、並びに、データ主体がその個人データの提供の義務を負うか否か、及び、そのデータ提供をしない場合に生じ得る結果			13.2.e		1	
				取得者	b.6) 【AND】個人データの取得者又は取得者の類型					1	
				データ主体の権利	【AND】 C) データ主体の権利。すなわち、次の情報。 c.1) データ主体の個人データにアクセスする権利に関する情報 c.2) 【AND】データ主体の個人データの訂正の権利に関する情報 c.3) 【AND】データ主体の個人データの消去の権利に関する情報 c.4) 【AND】データ主体のデータ取扱いの制限の権利に関する情報 c.5) 【AND】データ主体のデータ取扱いに対し異議を述べる権利に関する情報 c.6) 【AND】データ主体のデータポータビリティの権利に関する情報			13.2.b		6	
				同意を撤回する権利	c.7) 【AND】取扱いが同意に基づく場合、撤回前の取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利			13.2.c		1	
				異議を申し立てる権利	c.8) 【AND】EEA域内の所轄データ保護機関に異議を申立てる権利			13.2.d		1	

				EEA 域外への移転	【AND】 D) 【IF】個人データのEEA域外又は国際機関への移転を意図している場合、【THEN】次の情報 d.1) データが移転される非欧州諸国の一覧 d.2) 【AND】データ移転に有効な十分性認定が適用されるか否か d.3) 【AND】EEA域内のデータに提供される保護のレベルが低下しないことを確保するため、管理者が採用する保護措置に関する情報 d.4) 【AND】データ主体が当該保護措置の複製物を取得できる場所又は利用可能な場所			13.1.f		4
				自動的な決定	【AND】 E) 【IF】自動的な決定若しくはプロファイリング、又は、その両方が実施される場合、【THEN】次の情報 e.1) 取扱活動に含まれている論理に関する意味のある情報 e.2) 【AND】取扱活動の重要性 e.3) 【AND】データ主体に生ずると想定される取扱活動の結果			13.2.f		3
G.3.2.2	C	S	A	追加的取扱い	A) 申請者は、データ主体に対し、追加的取扱いに関する情報（追加的取扱いの目的及びデータ主体の権利を含む）を通知するための規則、手順又は仕組みを整備しなければならない。 【AND】 B) 申請者は、次の記録を保持しなければならない。 b.1) データ取扱いのかかる拡張の一切（その理由を含む） b.2) 【AND】当該追加的取扱いの適法性の評価 b.3) 【AND】データ主体との連絡（及びその日付）	申請者は、データ取扱いが次の要件を充足することを証明できなければならない。 - 主張される生命に関する利益を保護するために必要かつ比例的であること（同一の結果を達成するために利用可能なより侵襲的でない方法が存在しないこと） - 主張される生命に関する利益を保護するために比例的であること（取扱いの目的に対して適切かつ関連性のある個人データのみが収集され、取り扱われること）	追加的取扱いについてデータ主体に通知するための規則、手順又は仕組み	13.3	1	4
G.3.2.3	C	S	E	許容される例外	基準G.3.2.1及びG.3.2.2の例外を認めるため、申請者は、データ主体が既に通知を受けていることを証明しなければならない。	いかなる例外も、明確に正当化され、文書化されるのが望ましい。	文書レビュー サンプル試験分析	13.4	1	1
G.3.3				**個人データをデータ主体から取得していない場合に提供すべき情報** 条件	【IF】評価対象がデータ主体から収集していないデータを取り扱う場合、【THEN】次のとおりとする。 ［例外として、G.3.3.4に従って免除を証明できる場合を除く。］			**14**		
G.3.3.1	C	S	A	通知義務	データ主体に提供される情報には、次の情報が含まれなければならない。	申請者は、データ主体から取得した情報の記録を保持し、当該基準の例外とするために、データ主体が当該情報に既にアクセスしていることを証明できるようにするのが望ましい。これらの項目は、データ主体が既に当該情報を有している範囲においては適用されない。 データ主体は、GDPR 第77条に従い、EEA域内の所轄データ保護機関に対して輸入者に関する苦情を申し立てることができる。a.23)に関して、GDPR 第77条は「他の行政上の救済又は司法上の救済を妨げることなく、全てのデータ主体は、そのデータ主体が、自己と関係する個人データの取扱いが本規則に違反すると判断するときは、特に、データ主体の居住地の加盟国、就業場所の加盟国又は違反行為があると主張する場所の加盟国において、監督機関に異議を申立てる権利を有する。」と明確化している。 データ主体は、EEA域内のデータ保護機関（又は監督機関）を選択する権利を有する。 データ主体は、EEA域内の所轄データ保護機関に苦情を申し立てる権利について通知されるのが望ましい。	データ主体に提供されるユーザーインターフェース及び情報資料 （該当する場合）契約条項	14.1	1	2
				管理者の詳細	A) 管理者及びDPOの詳細、すなわち、次の情報。 a.1) 管理者の身元、及び、該当する場合はその代表者の身元 a.2) 【AND】管理者の連絡先、及び、該当する場合はその権限を与えられた代表者の連絡先			14.1.a		
				DPO の連絡先	a.3) 【AND】データ保護オフィサーの連絡先（又は連絡方法）			14.1.		1
				目的	【AND】 B) データの取扱いに関する情報、すなわち、次の情報。 b.1) 取扱目的			14.1.c		1
				法的根拠	b.2) 【AND】取扱いの法的根拠			14.1.c		1
				正当な利益	b.3) 【AND】該当する場合、管理者又は第三者によって求められる正当な利益			14.2.b		1
				データの種類	b.4) 【AND】関連する個人データの種類			14.1.d		1
				保持期間	b.5) 【AND】保持期間、又は、それが不可能な場合には保持期間を決定するための基準			14.2.a		1
				データの出所	b.6) 【AND】個人データの出所 b.7) 【AND】該当する場合、当該情報が一般に公開されている情報源から取得されたかものか否か			14.2.f		2
				取得者	b.8) 【AND】個人データの取得者又は取得者の類型			14.1.e		1
				データ主体の権利	【AND】 C) データ主体の権利。すなわち、次の情報。 c.1) データ主体の個人データにアクセスする権利に関する情報 c.2) 【AND】データ主体の個人データの訂正の権利に関する情報 c.3) 【AND】データ主体の個人データの消去の権利に関する情報 c.4) 【AND】データ主体のデータ取扱いの制限の権利に関する情報 c.5) 【AND】データ主体のデータ取扱いに対し異議を述べる権利に関する情報 c.6) 【AND】データ主体のデータポータビリティの権利に関する情報			14.2.c		6
				同意を撤回する権利	c.7) 【AND】取扱いが同意に基づく場合、撤回前の取扱いの適法性に影響を与えることなく、いつでも同意を撤回する権利			14.2.d		1
				異議を申し立てる権利	c.8) 【AND】EEA域内の所轄データ保護機関に異議を申立てる権利			14.2.e		1
				EEA 域外への移転	【AND】 D) 【IF】個人データのEEA域外又は国際機関への移転を意図している場合、【THEN】次の情報 d.1) データが移転される非欧州諸国の一覧 d.2) 【AND】データ移転に有効な十分性認定が適用されるか否か d.3) 【AND】EEA域内のデータに提供される保護のレベルが低下しないことを確保するため、管理者が採用する保護措置に関する情報 d.4) 【AND】データ主体が当該保護措置の複製物を取得できる場所又は利用可能な場所			14.1.f		4
				自動的な決定	【AND】 E) 【IF】自動的な決定若しくはプロファイリング、又は、その両方が実施される場合、【THEN】次の情報 e.1) 取扱活動に含まれている論理に関する意味のある情報 e.2) 【AND】取扱活動の重要性 e.3) 【AND】データ主体に生ずると想定される取扱活動の結果			14.2.g		3
G.3.3.2	C	S	A	通知義務	A) 申請者は、データ主体に対して、彼らのデータの間接的な収集について通知する手続を整備しなければならない。 【AND】 B) 申請者は、次の記録を保持しなければならない。 b.1) 個人データが間接的に取得された日付 b.2) 【AND】データ主体とのコミュニケーション及びその日付 b.3) 【AND】データ主体に提供された情報 【AND】 C) 記録は、管理者がデータ主体に情報を提供したことを示さなければならない。 c.1) 個人データを取得した後、1か月以内 c.2) 【AND】個人データがデータ主体との連絡に使用される場合、データ主体との最初の連絡の時点まで c.3) 【AND】他の取得者への開示が予定されている場合、個人データが最初に開示される時点まで	明確な文書による手順又は技術的解決策は、データ主体が申請者に要求を行うたび、当該要求が記録され、不当な遅延なく取り扱われることを確保するのが望ましい。監査人は、データ主体であるかのように試験を実施できるのが望ましい。要求の提出方法に関する情報を見つけることができ、模擬的な要求を行い、当該要求がどのように記録され、フォローアップされるかを確認できるのが望ましい。 データ主体に対して、個人データの間接的取得について情報を提供するための期間は、個人データを取得した後、合理的な期間であって、特定の状況に応じて遅くとも1か月以内（個人データが取り扱われる具体的な状況を考慮する）、個人データがデータ主体との連絡に使用される場合、遅くともそのデータ主体への最初の連絡の時点まで、又は、他の取得者への開示が予定されている場合、遅くとも個人データが最初に開示される時点までである。	データ主体に連絡するための規則、手順又は仕組み 可能な場合、データ主体との過去の連絡の記録 データ主体向け情報テンプレート	14.3	1	7

G.3.3.3	C	S	A	目的延長に関する通知義務	A) 申請者は、データ主体に対して、データが最初に収集された目的とは異なる目的のために予定されている個人データの追加的取扱いについて通知する手続きを整備しなければならない。 【AND】 B) 申請者は、その手続きの効果を示さなければならない。	申請者は、提供される情報が追加的取扱いの前に提供されることを確保し、**かつ**、特にGDPR第14条第2項に規定される情報を含むのが望ましい。	データ主体に連絡するための規則、手順又は仕組み 可能な場合、目的拡張に関するデータ主体との過去の連絡の記録 データ主体向け情報テンプレート	14.4						
G.3.3.4	C	S	E	許容される免除	次のいずれかに該当する場合、G.3.3.1はスキップできる。	いかなる例外も、明確に正当化され、かつ、文書化されるのが望ましい。GDPRが一定の例外を認める場合でも、ユーロプライバシーは、申請者に対し、通常の義務を遵守することを奨励する。	DPO、ユーザーインターフェース、データ主体との連絡、関連法	14.5		1				
				事前の情報	ケース 1 - データ主体が既に次の事項を通知されている場合 A) 申請者は、データ主体がG.3.3.1に列挙された情報を既に保有していることを証明しなければならない。			14.5.a			1			
				過大な努力	【OR】 ケース 2 - 不可能又は過大である場合 A) 申請者は、情報の提供が次のいずれかに該当することを証明しなければならない。 a.1) 不可能である こと a.2) 【OR】過大な負担が伴うこと a.3) 【OR】当該取扱いの目的を達成できないようにしてしまうおそれ、又は、それを深刻に阻害するおそれがあること 【AND】 B)			14.5.b				4		
				法的義務	【OR】 ケース 3 - 法的義務 A) 申請者は、個人データの収集又は開示を明示的に義務付ける特定の法的義務に拘束されなければならず、当該義務はEU法又はEEA加盟国の国内法に基づくものでなければならない。			14.5.c				1		
				規制された職業上の秘密	【OR】 ケース4 - 規制された職業上の秘密 A) 申請者は、法によって規律される職務上の守秘義務（EU法又はEEA加盟国の国内法に基づく制定法上の守秘義務を含む）に服さなければならない。			14.5.d				1		
G.3.4				**データ主体によるアクセスの権利**				**15**						
G.3.4.1	C	S	A	データ主体によるアクセスの権利	申請者は、データ主体が次の情報を要求し、アクセスできるようにするための効果的な仕組み又は手順を整備しなければならない。		データ主体の要求管理のための手順又は仕組み 可能な場合、アクセス権に関する過去の要求及びフォローアップ措置の記録	15.1						
				目的	A) データ取扱いに関する情報、すなわち、次の情報。 a.1) 個人データが取扱われているか否か、及び、その取扱目的			15.1.a		1				
				データの種類	a.2) 【AND】取扱われる個人データの種類			15.1.b			1			
				取得者	a.3) 【AND】第三国又は国際機関の取得者を含む、個人データの取得者又は取得者の類型、			15.1.b				1		
				保持期間	a.4) 【AND】保持期間、又は、それが不可能な場合には保持期間を決定するための基準			15.1.d			1			
				データの出所	a.5) 【AND】個人データが取得された情報源、及び、該当する場合には個人データが一般に公開されている情報源から取得されたものか否か			15.1.g			1			
				データ主体の権利	【AND】 B) データ主体の権利。すなわち、次の情報。 b.1) データ主体の個人データにアクセスする権利に関する情報 b.2) 【AND】データ主体の個人データの訂正の権利に関する情報 b.3) 【AND】データ主体の個人データの消去の権利に関する情報 b.4) 【AND】データ主体のデータ取扱いの制限の権利に関する情報 b.5) 【AND】データ主体のデータ取扱いに対し異議を述べる権利に関する情報 b.6) 【AND】データ主体のデータポータビリティの権利に関する情報			15.1.e				6		
				異議を申し立てる権利	b.7) 【AND】EEA域内の所轄データ保護機関に異議を申立てる権利			15.1.f			1			
				自動的な決定	【AND】 C) プロファイリングを含む自動的な決定の実施に関する情報。すなわち、次の情報。 c.1) 管理者が、プロファイリングを含む自動的な決定を実施したか否か c.2) 【AND】取扱活動に含まれる論理に関する意味のある情報 c.3) 【AND】取扱活動の重要性 c.4) 【AND】データ主体に生ずると想定される取扱活動の結果			15.1.h				4		
				EEA 域外への移転	【AND】 D) EEA域外へのデータ移転に関する情報。すなわち、次の情報。 d.1) 個人データが第三国又は国際機関に移転されるか否か d.2) 【AND】データが移転される第三国又は国際機関の一覧 d.3) 【AND】データ移転に有効な十分性認定が適用されるか否か d.4) 【AND】移転に関連して用いられる保護措置に関する情報、及び、必要な場合は個人データの保護のレベルを確保するための適切な措置に関する情報			15.2				4		
G.3.4.2	C	S	A	コピー提供義務	A) 申請者は、次の措置を実施するための規則、方針又は手順を整備しなければならない。 a.1) データ主体の取り扱われた個人データの複製物を抽出すること a.2) 【AND】かかる要求に応じて、データ主体に対し、当該個人データの複製物を提供すること 【AND】 B) 【IF】データ主体が電子的な手段による情報の受領を要求した場合、【THEN】当該複製物は一般的に使用される電子フォーマットで提供されなければならない。	データ主体は、自らの個人データの複製物を受領する権利を有し、データ主体が要求するフォーマットで提供されることが確保されるのが望ましい。手続を容易にするために、申請者は、データ主体が自らの個人データにアクセスし、ダウンロードできるようにすることを決定することができる。 データ主体から要求された追加の複製物については、管理者は業務運営費用に基づく合理的な手数料を徴収することができる。	データ主体にデータのコピーを移転するための手順又は仕組み 可能な場合、データ主体との過去の連絡の記録	15.3						
G.3.4.3	C	S	A	他人の権利を尊重する義務	A) 申請者は、データ主体からの個人データの複製物の受領要求に応じる際に、他のデータ主体の権利及び自由に対する悪影響を防止するため手順又は仕組みを整備しなければならない。	該当する場合、申請者は、権利の行使によって影響を受ける可能性のある他のデータ主体の個人データを削除するか、又は、複製物を提供する前に当該データ主体の同意を求めるのが望ましい。	データ主体にデータのコピーを移転するための規則、手順又は仕組み 可能な場合、データ主体	15.4		1	3			
G.3.5				**訂正の権利**				**16**		1	1			
G.3.5.1	C	S	A	訂正の権利	A) 申請者は、データ主体の個人データを訂正し、又は、完全なものとさせる権利に応じるために整備した手順又は仕組みが、当該要求を効果的に処理できることを証明しなければならない。	申請者は次の記録を保持するのが望ましい。 - データ主体の識別又は認証 - データ主体からの要求及びその日付 - データ主体との連絡及びその日付 - フォローアップ措置及びその日付 - 該当する場合、当該要求に応じなかった理由 本要件の効果的な実施には、整備された手順又は仕組みが監査人によって試験されるか、又は、データ主体からの要求のサンプル分析を通じて評価されることが必要である。	データ訂正に関する規則、手順又は仕組み もし入手可能であれば、訂正の権利に関する過去の要求とフォローアップ措置の記録	16						
G.3.6				**消去の権利（「忘れられる権利」）**				**17**		1	1			

G.3.6.1	C	S	A	消去の権利	A) 申請者は、G.3.6.3の条件のいずれかが適用可能な場合を除き、データ主体の要求に応じて個人データを効果的に消去するための規則、手順又は仕組みを整備しなければならない。	申請者は、次の措置を講じるための手順を整備するのが望ましい。 - データ主体の要求の記録 - データ主体の識別及び認証 - 個人データの全ての複製物を含む、要求された個人データの消去の実施 申請者は、次の記録を保持するのが望ましい。 - データ主体の要求及びその日付 - データ主体との連絡及びその日付 - フォローアップ措置及びその日付 - 当該要求に対する関連する理由の評価（すなわち、データがもはや必要でないこと、同意の撤回、データ主体の異議、違法な取扱い、法的義務の遵守、又は、関連するEU法若しくはEEA加盟国の国内法の意味における子どもに対する情報社会サービスの提供） - 該当する場合、当該要求に応じなかった理由 有効性は、手順の試験又はデータ主体からの以前の要求の分析を封じて証明され、かつ、データが効果的に消去されていることを確認することが確認されるのが望ましい。 消去は、個人データのリンク、コピー、バックアップ又は複製を含むのが望ましい。	データ消去のための規則、手順又は仕組み 可能な場合、消去権に関する過去の要求及びフォローアップ措置の記録	17.1			
G.3.6.2	C	S	A	要求を他のデータ管理者に伝える義務	【IF】申請者が評価対象の個人データを公衆に利用可能にしている場合、【THEN】次のとおりとする。 A) 申請者は、データ主体による消去の要求について、他の管理者に通知するための規則、手順又は仕組みを整備しなければならない。ただし、当該申請者が他のデータ管理者に通知するための潜在的な措置を評価し、特定された措置が過大であることを証明した場合には、この限りではない。	管理者は、利用可能な技術及び実施コストを考慮し、合理的な措置（技術的措置を含む）を講じ、当該個人データを取り扱う他の管理者に対して、データ主体が個人データへのリンク、コピー又は複製の消去を要求していることを通知するのが望ましい。	他の管理者にデータを移転するための規則、手順又は仕組み 可能な場合、データ移転に関する過去の要求及び	*17.2*	1	1	
G.3.6.3	C	S	E	許容される免除	消去する権利は、次の場合には制限される。 表現及び情報伝達の自由の権利の行使 A) 申請者は、個人データが表現及び情報伝達の自由の権利の行使のために利用されていることを証明しなければならな 【OR】法的義務の遵守 B) 申請者は、EU法又はEEA加盟国の国内法に基づく法的義務を遵守する義務があることを証明しなければならない。 C) 申請者は、EU法又はEEA加盟国の国内法に基づく公衆衛生の分野に公共の利益があることを証明しなければならない。 【OR】保管、研究又は統計 D) 申請者は、次の事項を証明しなければならない。 d.1) 取扱いが公共の利益における保管の目的に必要であること d.2) 【OR】取扱いが科学的目的に必要であること d.3) 【OR】取扱いが歴史的研究の目的に必要であること d.4) 【OR】取扱いが統計の目的に必要であること d.5) 【AND】削除が取扱いの目的の達成を不可能としてしまうおそれ、又は、それを深刻に阻害するおそれがあること d.6) 【AND】データ主体のため、適切な保護措置が講じられていること 【OR】法的手続 E) 申請者は、データの保持が訴えの提起又は攻撃防御に関連することを証明しなければならない。	消去権からのいかなる例外も、明示的に正当化及び文書化されるのが望ましい。 法的義務又は公共の利益を根拠とする場合、それらはEEA域内でEU法若しくはEEA加盟国の国内法、又は、その両方により正式に認められるのが望ましい。	DPOの記録及びDPOとの面談、プライバシーポリシー、整理した証拠	17.3 17.3.a 17.3.b 17.3.c 17.3.d 17.3.e	1 1 1 6 1	1 1 1	
G.3.7				**取扱いの制限の権利**				**18**				
G.3.7.1	C	S	A	取扱いの制限の権利	A) 申請者は、次の措置を講じるための規則、手順又は仕組みを整備しなければならない。 a.1) 次の場合において、データ主体による個人データの取扱制限の要求に効果的に応じること - 個人データの正確性についてデータ主体から疑義が提示されている場合 - 【OR】個人データが違法に取扱われ、又は、取扱いが付与された認証に含まれる要件に違反する場合であって、かつ、データ主体が個人データの消去に反対し、その代わりに、その制限を求めている場合 - 【OR】取扱いが収集された目的のためにもはや必要としない場合 - 【OR】データ主体が、管理者の正当性の根拠又は管理者に付与された公共の利益に基づく取扱い（プロファイリングを含む）に異議を唱えた場合 a.2) 【AND】取扱いが次の場合にのみ継続されることを確保すること - データ主体が同意した場合 - 【OR】訴えの提起又は攻撃防御のため - 【OR】EU法又はEEA加盟国の国内法に基づく重要な公共の利益の理由のため a.3) 【AND】データ取扱いの制限を解除する決定を文書化すること	データ制限について、申請者は、データ主体の要求により制限された取扱いが、データ主体が同意を与え、かつ、制限の解除について通知された後にのみ完全に有効になることを確保するのが望ましい。データ主体が上記の適法性に関する条件に基づいて同意を与えたことを確保する必要があり、また、管理者はその文書及び証拠を保持する必要がある。 取扱いの制限は、次のいずれかの場合に可能である。 (1) データの正確性についてデータ主体から疑義が提示されている場合、当該個人データの正確性を管理者が確認できるようにする期間において (2) 取扱いが違法である場合 (3) 管理者がその取扱いの目的のためにはその個人データを必要としないが、データ主体から、訴えの提起又は攻撃防御のために当該データが求められている場合 (4) データ主体が、第21条第1項に基づき、取扱いに異議を申し立てている場合	データ取扱いの制限のための規則、手順又は仕組み 可能な場合、制限に関する過去の要求及びフォローアップ措置の記録	18.1	1	4	
G.3.8				**個人データの訂正、消去又は取扱いの制限に関する通知義務**				**19**				
G.3.8.1	C	S	A	取得者への通知義務	A) 申請者は、個人データが開示された各取得者に対し、個人データの訂正又は消去又は取扱いの制限を連絡するための手順又は仕組みを整備しなければならない。 【OR】 B) 申請者は、取得者に通知する義務の遵守が不可能であること、又は、過大な労力を伴うことを証明しなければならない	申請者は、次の記録を保持するのが望ましい。 - データの取得者に通知するために行われた連絡及び日時 - 該当する場合、取得者に通知されなかった正当化理由、特に申請者が取得者に通知することが不可能である、又は、過大な普段を要すると申請者が判断した理由	訂正及び消去を通知するための規則、手順又は仕組み可能な場合、過去の通知の 記録	19	1	2	
G.3.8.2	C	S	A	要求された場合、データ主体に取得者を通知する義務	A) 申請者は、データ主体からの個人データの取得者の通知要求に効果的に応じるための規則、手順又は仕組みを整備しなければならない。 【AND】 B) 【IF】データ主体が取扱いの制限を受けていた場合、【THEN】申請者は取扱いの制限を解除する前にデータ主体に通知しなければならない。	申請者は、次の措置を実施するための手順又は仕組みを整備するのが望ましい。 - データ主体の要求の記録 - 本人確認に疑義がある場合、データ主体の識別及び認証 - 要求に応じるための全ての条件を充足しているかの評価及び検証 - 要求に応じ、データ主体に対する取得者に関する情報の通知 申請者は、次の記録を保持するのが望ましい。 - データ主体の要求及びその日付 - データ主体との連絡及びその日付 - 要求の評価及びフォローアップ措置並びにその日付 - 該当する場合、当該要求に応じなかった理由 申請者は、取扱いの制限が解除される場合、当該制限を解除する場合に、制限解除の理由を含む情報をデータ主体に提供するのが望ましい。	データ主体の要求を対処するための規則、手順又は仕組み 可能な場合、データ主体に提供された過去の情報の記録	19	1	1	
G.3.9				**データポータビリティの権利**				**20**				
				条件	【IF】個人データがデータ主体の同意又は契約をによって収集されたものである場合、【THEN】次のとおりとする。							
G.3.9.1	C	S	A	データポータビリティの権利	A) 申請者は、データポータビリティのため、次の措置を講じる手順又は仕組みを整備しなければならない。 a.1) データ主体が提供した個人データの複製物を電子形式で取得可能にすること a.2) 【AND】他のデータ主体の権利及び自由に悪影響を及ぼすおそれがある場合、当該他のデータ主体に関する個人データを除去しなければならない。 【AND】 B) データ主体への個人データの移転に使用されるデータ形式は、次の要件を充足しなければならない。 b.1) 構造化されていること b.2) 【AND】一般的に利用されていること b.3) 【AND】機械可読であること	技術的に可能な場合、申請者は、データ主体が取り扱われた自己のデータに直接アクセスできるようにするのが望ましい。 申請者は、次の措置を実施するための手順又は仕組みを整備することができる。 - データ主体の要求の記録 - 本人確認に疑義がある場合、データ主体の識別及び認証 - 要求に応じるための全ての条件を充足しているかの評価及び検証 - 要求されたデータのデータ主体への送信 申請者は、次の記録を保持するのが望ましい: - データ主体の要求及びその日付 - データ主体との連絡及びその日付 - 要求の評価及びフォローアップ措置並びにその日付 - 該当する場合、当該要求に応じなかった理由 申請者は、手順がデータ主体の要求に効果的に応じるために十分であることを証明（過去の記録のサンプル又は技術的実証）しなければならない。 本権利の適用は、取扱いが同意若しくは契約に基づく場合、又は、取扱いが自動的な手段によって行われる場合	データポータビリティのための規則、手順又は仕組みデータポータビリティの技 術的試験又は証明	20.1	1	5	
G.3.10				**異議を述べる権利**				**21**				

G.3.10.1	C	S	A	異議を述べる権利の有効性	A) 申請者は、データ主体による特定の状況に関連する理由に基づいて自己の個人データの取扱いに異議を述べる要求に対し、効果的に応じるための規則、手順又は仕組みを整備しなければならない。 【AND】 B) 【IF】データがダイレクトマーケティングの目的で取り扱われている場合（ダイレクトマーケティングに関連するプロファイリングを含む）、【THEN】規則、手順又は仕組みは、次の事項を確保しなければならない。 b.1) データ主体が、いつでも異議を述べることができること b.2) 異議を述べたデータ主体の個人データが、もはやマーケティング目的のために取り扱われないこと 【AND】 C) 【IF】データが科学的若しくは歴史的研究目的又は統計目的のために取り扱われている場合、【THEN】規則、手順又は仕組みは、データ主体が自己の個人データの取扱いに異議を述べることができるのを確保しなければならない。ただし、当該取扱いが、EEA法又は加盟国の国内法において認められた公共の利益において行われる職務の遂行のために必要である場合はこの限りではない。	申請者は、次の措置を実施するための手順を整備するのが望ましい。 - データ主体の要求の記録 - 本人確認に疑義がある場合、データ主体の識別及び認証 - 要求に応じるための全ての条件を充足しているかの評価及び検証 - データ主体の要求に従った不当な遅滞のなく取扱いの停止 申請者は、次の記録を保持するのが望ましい。 - データ主体の要求及びその日付 - データ主体との連絡及びその日付 - 要求の評価及びフォローアップ措置並びにその日付 - 該当する場合、当該要求に応じなかった理由 GDPRによれば、異議を述べる権利はいつでも行使できる。異議を述べる権利を行使した後、次の場合を除き、データはもはや取り扱われない。 - データ主体の利益、権利及び自由よりも優先する取扱いについて、やむを得ない正当な根拠がある場合 - 【OR】訴えの提起又は攻撃防御のために取扱いが必要な場合 マーケティング目的のための取扱いに関連して異議を述べる権利が行使された場合、個人データはかかる目的のためにはもはや取り扱われないのが望ましい。 GDPR第89条第1項に基づく科学的研究若しくは歴史的研究の目的又は統計の目的の取扱いに関連して異議を述べる権利が行使された場合、個人データはかかる目的のためにはもはや取り扱われないのが望ましい。ただし、取扱いがEU法又はEEA加盟国の国内法により定められた公共の利益の理由に基づいて行われる職務の遂行に必要な場合はこの限りではない。	異議を述べる権利に対処するための規則、手順又は仕組み 可能な場合、異議を述べる権利に関する過去の要求及びフォローアップ措置の記録	21			
G.3.10.2	C	S	A	異議を述べる権利に関する明確な情報	A) 申請者は、データ主体に対し、個人データの取扱いに異議を述べる権利について、次のとおり通知しなければならない。 a.1) データ取扱いの前に通知すること a.2)【AND】他の情報とは別の段落において、又は、他の情報から分けて通知すること 【AND】 B) 申請者は、当該情報がデータ主体によって明確かつ理解可能であることを検証しなければならない	申請者は、データ主体に提供された情報の記録を保持し、異議を述べる権利がどのようにデータ主体に明示的に通知されたかを示さなければならない。	データ主体に提供されるユーザーインターフェース及び情報資料 （該当する場合）契約条項	21.4	1	4		
G.3.11				**プロファイリングを含む個人に対する自動化された意思決定の対象とされない権利**				**22**			
G.3.11.1	C	S	A	プロファイリングを含む個人に対する自動化された意思決定	A) 評価対象におけるデータ取扱いは、データ主体に影響を及ぼし得る、自動的な決定のみに基づく決定から免れなければならない。ただし、当該自動化された決定のプロセスが、次のいずれかに該当する場合を除く。 a.1) データ主体とデータ管理者との間の契約の締結又は履行のために必要であり、同等の結果を得るためにより侵襲性の低い代替手段がないと結論付けられた書面による分析に基づくものである場合 a.2) 【OR】データ主体の権利及び正当な利益を保護するための適切な措置を提供するEU法又はEEA加盟国の国内法により認められている場合 a.3) 【OR】データ輸入者の第三国法により認められ、当該法がデータ主体の権利及び正当な利益を保護するための適切な措置を提供するものとして評価されている場合 a.4)【OR】データ主体の明確な同意に基づく場合 【AND】 B) 申請者は、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専用の措置を講じなければならない。	自動的な取扱いが行われる場合、申請者は、次の事項を文書化及び証明するのが望ましい。 - 申請者が、プロファイリングを含む意図された自動的なデータ取扱いについて、データ主体の自由及び権利、並びに、その正当な利益に対するリスクを評価していること - DPOが、プロファイリングを含む個人に対する自動化された意思決定の対象とならない権利に関連して、データ取扱いの適法性及び遵守状況を評価及び検証したこと - 正当な根拠、並びに、該当する場合、データ主体の自由、権利及び正当な利益を保護するために実施されるべき補完的な適切な技術的及び組織的措置 申請者は、外部監査人が、検査、試験若しくは文書レビュー、又は、その複数を通じて、上記の権利に対する本データ取扱いの遵守状況を評価できるようにするのが望ましい。 プロファイリングを含む自動化された意思決定の必要性及び比例性は、同等の結果に達するための自動化された意思決定の代替案を考慮しながら、プロセスの分析を通じて証明される必要がある。プロファイリングを含む自動的なデータ取扱いを必要とせず、同一の結果をもたらす同等の解決策が存在する場合、自動化された意思決定は不必要とみなされるのが望ましい。 全体として、プロファイリングを含む個人に対する自動化された意思決定は、子どもの個人データ又は特別な種類の個人データを含めないのが望ましい。ただし、GDPR第9条2項a又はgが適用可能な場合はこの限りではない。後者に関しては、データ主体の権利、自由及び正当な利益を保護するために適切な措置が講じられている限り、取扱いは許可される。 基本的な権利を確保するための保護措置は、主に透明性、説明責任を促進し、パイアスを緩和するための必要な	内部規則、方針及び手順 データ主体との連絡の記録 労働者との面談 データ取扱いの調査及び分析	22.1	1	5		
G.3.11.2	C	S	A	人間の関与を得る権利及び疑義を提示する権利	【IF】自動的な決定（プロファイリングを含む）が個人データの取扱いに基づく場合、【THEN】次のとおりとする。 A) 申請者は、当該自動的な決定（プロファイリングを含む）について、データ主体に対し、その個人データに関連する特定の情報を提供しなければならない。 【AND】 B) 申請者は、データ主体が次の措置を講じることを可能にする手順又は仕組みを整備しなければならない。 - 人的管理者の側での人間の関与を得ること	自動的な意思決定を用いた個人データのいかなる取扱いも、明確に正当化され、かつ、文書化されるのが望ましい。これは、整備された手順又は仕組みが、監査人によって試験されるか、又は、データ主体の要求のサンプル分析を通じて評価されることが必要である。	手順の文書レビュー 調査 手順の試験 DPOとの面談	22.3	1	3		
G.4				**データ管理者の責任** 目的　データ管理者が評価対象におけるデータ取扱いの責任を遵守するのを確保すること。 条件　【IF】申請者がデータ管理者である場合、【THEN】次のとおりとする。							
G.4.1				**管理者の責任**				**24**			
G.4.1.1	C	S	A	技術的措置及び組織的措置に関する文書	A) 申請者は、取り扱うデータを保護するために実施した技術的措置及び組織的措置に関する文書を有さなければならない。	申請者は、輸入された個人データを保護するために実施している技術的及び組織的措置に関する最新の文書を維持するのが望ましい。技術的及び組織的措置は、最先端の技術（すなわち、技術、セキュリティ等の分野における最新の発展）、並びに、個人データの取扱いの性質、範囲、文脈及び目的を考慮に入れるのが望ましい。申請者は、個人データの取扱いに関連して、データ主体の権利及び自由に対するリスクの異なる蓋然性及び深刻度に適した安全性の水準を確保するため、適切な技術的及び組織的措置を実施していることを証明するのが望ましい	技術的措置及び組織的措置に関する文書	24.1	1	1		
G.4.1.2	C	S	A	見直し及び更新の義務	A) 申請者は、定期的に（少なくとも年に1回）、次の事項の適切性を見直すための手順を整備しなければならない。 a.1) 個人データを保護するために講じられている技術的措置及び組織的措置 a.2)【AND】個人データを保護するために講じられている方針、手続及び仕組み 【AND】 B) 申請者は、次の文書化された記録を保持しなければならない。 b.1) 技術的措置及び組織的措置、並びに、方針、手順及び仕組みの見直し b.2) 特定された脆弱性及び当該脆弱性に対処するために講じられた措置	申請者は、個人データを保護するために講じられている技術的及び組織的措置、並びに、方針、手順及び仕組みの適切性について、定期的に、少なくとも年1回は見直しを行うことが期待される。申請者は、当該見直しの文書を保持し、特に、当該技術的及び組織的措置、並びに、方針、手順及び仕組みが、個人データの取扱いの性質、範囲、文脈及び目的に関連して適切であるとみなされるか否かを明記するのが望ましい。 評価対象におけるデータ取扱いが特別な種類のデータ若しくは子どもの個人データを含む場合、又は、データ主体の権利及び自由に対して様々な蓋然性及び深刻度のリスクをもたらす可能性がある場合、次のとおりとする。 - 申請者は、データのセキュリティに関する内部監査若しくは外部監査又はその両方を実施することが期待される。特に、監査の範囲は、少なくとも12か月ごとに、取り扱われる個人データの性質、範囲、文脈及び目的、並びに、自然人の権利及び自由に対する様々な蓋然性及び深刻度のリスクを含むのが望ましい。 - 申請者の上級管理職は、少なくとも12か月ごとにデータ保護ポリシーを見直すことが期待される。	内部規則、方針及び手順 技術的措置及び組織的措置 の最終レビューの文書 労働者及びDPOとの面談	24.1	1	4		
G.4.1.3	C	S	A	データ保護ポリシー	A) 申請者は、少なくとも次の事項を含む、書面によるデータ保護規則若しくはポリシー、又は、その両方を有さなければならない。 a.1) セキュリティ及びアクセス制御 a.2)【AND】個人データ侵害管理 a.3)【AND】リスクアセスメント、及び、該当する場合にはデータ保護影響評価（DPIA） a.4)【AND】データ処理者の要件及び遵守状況評価 a.5)【AND】所轄データ保護機関への報告及び協力の手順 a.6)	申請者は、書面によるデータ保護に関する規則若しくは方針又はその両方を有さなければならない。	データ保護に関する規則及びポリシー	24.2	1	7		
G.4.1.4	CP	G	A	EEAの代理人	【IF】申請者がEEA域外に所在し、EEA域内における個人データの収集を積極的に対象としている場合、【THEN】次のとおりとする。 A) 申請者は、EEA加盟国に所在するオフィス又は代理人を有し、その連絡先が申請者のウェブサイト上で利用可能とな	申請者がEEAに所在しないが、GDPR第3条第2項に基づきGDPRの適用対象となる場合、EU域内に代理人を持つことが期待される。GDPR第3条第2項によれば、GDPRは、EEA市場に物品若しくはサービスを提供し、又は、EEA域内のデータ主体の行動を監視する管理者に適用される。	文書レビュー（商業登記など） ウェブサイト調査	27	1	1		
G.5				**データ処理者（又は復処理者）** 目的　評価対象の取扱いに参加するデータ処理者が規制要件を遵守するのを確保すること。 条件　【IF】評価対象にデータ処理者又は復処理者が関与する場合、【THEN】次のとおりとする。							

G.5.1				処理者				28		
G.5.1.1	C	S	A	処理者の従事	【IF】申請者が処理者を従事させるデータ管理者として行動する場合、【THEN】次のとおりとする。 A) 次の措置によって、十分な保証を提供する処理者及び復処理者のみを従事させるための規則、手順又は仕組みが整備されていなければならない。 a.1) 個人データを保護するための技術的措置及び組織的措置に関する情報について、データ処理者及び復処理者に要求し、これを記録すること a.2) 【AND】個人データ保護のために処理者及び復処理者が講じている技術的措置及び組織的措置の適切性を評価すること a.3)【AND】当該評価を文書化し、当該データ処理者のサービスを採用する決定を記録すること 【AND】 B) 申請者は、次の事項について文書化された記録を保持しなければならない。 b.1) 技術的措置及び組織的措置に関し、処理者及び復処理者が提供した情報及び保証 b.2) 【AND】評価対象に係るデータ取扱いに関与するデータ処理者及び復処理者を関与させるための決定プロセス	申請者は、処理者及び該当する場合は復処理者が、データ保護要件の遵守を確保するための十分な保証を提供するために講じた技術的及び組織的措置を評価、見直し及び文書化するための規則、手順又は仕組みが整備されていることを証明しなければならない。 申請者は、技術的及び組織的措置の適切性を証明するため、処理者及び復処理者との契約及び提供された保証の定期的な見直しを実施することが期待される。 適切性とは、取扱いがデータ主体の権利及び自由を損なわないことを確保する技術的及び組織的措置の能力を意味する。 個人データを保護するためのデータ処理者及び復処理者の技術的及び組織的措置に関する情報は、有効なGDPR認証を通じて提供されることができる。	処理者及び復処理者の遵守状況評価のための規則、手順又は仕組み 処理者及び復処理者の過去の評価の記録及び文書 処理者及び復処理者に提供されたGDPR認証	28.1		
G.5.1.2	P	S	A	復処理者の従事	申請者が評価対象のために復処理者を使用してデータ処理者として行動している場合、【THEN】次のとおりとする。 A) 次の措置により、十分な保証を提供する復処理者のみを使用するための規則、手順又は仕組みが整備されなければならない。 a.1) 個人データを保護するための技術的及び組織的措置に関する情報について、復処理者に要求し、これを記録すること a.2) 【AND】個人データを保護するために復処理者によって講じられている技術的及び組織的措置の適切性を評価すること a.3)【AND】復処理者を従事させるため、管理者の事前承認を取得し、これを文書化すること a.4) 【AND】復処理者が、評価対象に係るデータ取扱いに関して、処理者に課せられる義務と同等の義務に契約上拘束されるのを確保すること 【AND】 B) 申請者は、次の事項について文書化された記録を保持しなければならない。 b.1) 復処理者が提供する情報及び保証（技術的及び組織的措置を含む） b.2) 【AND】評価対象に係るデータ取扱いに関与するデータ処理者の従事及び復処理者の事前承認に関する評価及び決定プロセス 【AND】 C) 事前承認が包括的なものである場合、申請者の文書には、次の事項が含まれなければならない。 c.1) 復処理者を選定及び任命のために管理者が承認した基準の一覧 c.2)【AND】選定された復処理者が管理者によって設定された基準をどのように充足しているか c.3) 【AND】復処理者の変更予定について、管理者に通知し、当該変更前に合理的な異議申立ての機会を付与するための手順、仕組み又は方針 【AND】	復処理者が関与する場合、申請者は、管理者が一般的又は特定の事前承認を提供したことを証明するのが望ましい。当該承認が一般的なものである場合、申請者は、事前承認された潜在的な復処理者の一覧又は復処理者を選択及び関与させるために使用される基準の一覧を提供し、選択された復処理者がその基準をどのように充足しているかを証明するのが望ましい。 申請者は、復処理者がデータ保護要件を遵守するための十分な保証を提供するために講じた技術的及び組織的措置を評価、見直し及び文書化するための規則、手順又は仕組みを整備していることを証明するのが望ましい。 申請者は、技術的及び組織手措置の適切性を証明するため、復処理者との契約及び提供された保証の定期的な見直しを実施することが期待される。 適切性は、取扱いがデータ主体の権利及び自由を損なわないことを確保する技術的及び組織的措置の能力を意味する。 個人データを保護するためのデータ処理者及び復処理者の技術的及び組織的措置に関する情報は、有効なGDPR認証を通じて提供されることができる。	処理者及び復処理者の遵守状況評価のための規則、手順又は仕組み 処理者及び復処理者の過去の評価の記録及び文書 事前承認の記録 処理者及び復処理者に提供されたGDPR認証	28.2 28.4	1	6
G.5.1.3	C	S	A	データ管理者として行動し、処理者と契約を締結する申請者に関する契約上の要件	【IF】申請者が管理者として行動し、処理者を使用する場合、【THEN】次のとおりとする。 A) 申請者は、評価対象における個人データの取扱いに関して、全てのデータ処理者との間で書面による契約を締結していなければならず、当該契約は次の要件を充足しなければならない。 a.1) 欧州連合加盟国の裁判所の管轄に服すること a.2)【AND】取扱いの対象及び期間を特定すること a.3)【AND】取扱いの性質及び目的を特定すること a.4)【AND】個人データの種類を特定すること a.5)【AND】データ主体の種類を特定すること a.6)【AND】管理者の権利及び義務を特定すること a.7)【AND】第三国又は国際機関への移転に関する要件を特定すること a.8) 【AND】データ処理者及び復処理者による個人データの移転は、管理者の書面による指示に基づき実施されるのを要求すること	管理者及び処理者は、GDPR第28条を遵守する書面による契約関係を有さなければならない。 データ処理者は、データ管理者からの文書による指示に基づいてのみ、管理者から受領した個人データを移転することができる。再移転は、移転のための補完的要件に関し、基準G.10.1において評価される補完的要件の対象となる。 a.1) の要件は、申請者が、EU加盟国の裁判所に出廷できることを意味する。	管理者と処理者との契約書	28.3	1	10
G.5.1.4	P	S	A	処理者の契上の約要件	【IF】申請者が処理者として行動する場合、【THEN】次のとおりとすること。 A) 申請者は、評価対象におけるデータの取扱いを担当する全てのデータ管理者及びデータ復処理者との間で、書面による契約を締結しなければならない。 【AND】 B) 評価対象に関与する処理者とデータ管理者及びデータ復処理者との各契約関係は、次の条件を充足しなければならない。 b.1) 欧州連合加盟国の裁判所の管轄に服すること b.2)【AND】取扱いの対象及び期間を特定すること b.3)【AND】取扱いの性質及び目的を特定すること b.4)【AND】個人データの種類を特定すること b.5)【AND】データ主体の種類を特定すること b.6)【AND】管理者の権利及び義務を特定すること b.7)【AND】第三国又は国際機関への移転に関する要件を特定すること b.8) 【AND】データ処理者及び復処理者による個人データの移転は、管理者の書面による指示に基づき実施されるのを要	管理者及び処理者は、GDPR第28条を遵守した書面による契約関係を持たなければならない。	処理者と管理者及び復処理者との契約書	28.3 28.4	1	9
G.5.1.5	CP	S	A	処理者及び復処理者の契約上の義務	A) 評価対象に関与する全てのデータ処理者との契約関係は、当該処理者が、次の措置を実施することを明記しなければならない。 a.1) 管理者の文書による指示に基づいてのみ個人データを取り扱うこと a.2) 【AND】評価対象における個人データの取扱いを許可された全ての者が機密保持義務に服するのを確保すること a.3)【AND】取扱いの安全性に関して必要となる全ての措置を実施すること a.4)【AND】管理者の同意なく他の処理者（又は復処理者）を従事させないのを誓約すること a.5)【AND】データ主体からの要求に応じる義務を果たすこと a.6) 【AND】データ主体の権利行使に関する要求に応じる管理者の義務を果たすために、可能な範囲において、適切な技術的及び組織的措置により管理者を支援すること a.7) 【AND】リスクアセスメント、個人データ侵害の管理及び通知、データ保護影響評価、並びに、機関との事前協議など、データ取扱いの安全性に関する義務の遵守を確保するために管理者を支援すること a.8) 【AND】管理者の選択により、取扱いに関するサービスの提供終了後、全ての個人データを管理者に削除又は返還し、かつ、EU又はEEA加盟国の国内法によりデータの保存が要求されない限り、既存の複写物を削除すること	管理者及び処理者は、GDPR第28条に定める要件を遵守する書面による契約関係を持たなければならない。 処理者は、GDPR第32条から第36条に従い、取り扱われるデータの十分な安全性及び保護を確保しなければならない。 処理者は、復処理者によって行われるいかなる取扱いに対しても責任を負い、復処理者が管理者との契約関係において定められた条件を遵守するのを確保することが期待される。	契約条項	28.3 28.4	1	11

G.5.1.6	CP	S	A	処理者によるコンプライアンスの補完的証明	A) 申請者は、各データ処理者について、認証、承認された行動規範、及び、適用可能なデータ保護規制を尊重するための拘束力がある約束に関する情報を取得し、その記録を保持しなければならない。	データ処理者が認証を受けておらず、かつ、認められた行動規範に拘束されていない場合、少なくとも、契約上拘束力のある手段（すなわち、プライバシーパクト又は同等のもの）を通じて、GDPRに含まれるデータ保護義務及び原則を尊重することを公に約束するのが望ましい。 該当する場合、申請者は、そのデータ処理者の認証ステータス、行動規範、及び、GDPRを尊重するための公的な契約上の拘束力ある約束を記録したレジストリを保持するのが望ましい。	データ処理者との連絡 認証、行動規範又は拘束力 がある約束ツールを有する処理者のレジストリ（	24.3, 28.5, 25.3, 32.2	1	1
G.5.2				**管理者のために処理者又は復処理者によって行われる取扱い**				**29**		
G.5.2.1	P	S	A	管理者からの指示のみに基づく取扱い	【IF】申請者が処理者として行動する場合、【THEN】次のとおりとする。 A) 申請者は、次の措置を実施するための規則、手順又は仕組みを整備しなければならない。 a.1) 管理者からの指示のないデータ取扱いを防止すること a.2)【AND】管理者からの指示を受け、記録すること 【AND】 B) 申請者は、次の記録を有さなければならない。 b.1) 管理者から受けた取扱いの指示 b.2)【AND】取扱活動 【AND】 C) 取扱活動は、管理者から受けた指示を遵守しなければならない。	処理者として、申請者は、管理者から受領した指示に基づき、かつ、当該指示に従ってのみデータを取扱うことを証明しなければならない。	指示に基づいてのみ取り扱うための規則、手順又は仕組み データ取扱いに関して受領した指示の記録	29	1	5
G.5.3				**取扱活動の記録**				**30**		
G.5.3.1	C	G	A	管理者によるデータ取扱いの記録	【IF】申請者が管理者として行動する場合、【THEN】次のとおりとする。 A) 申請者は、ToEに適用可能な取扱活動の書面（電子形式を含む）による記録を維持しなければならず、当該記録は次の情報を含まなければならない。 a.1) 管理者の名称及び連絡先 a.2) 該当する場合、共同管理者の名称及び連絡先 a.3) 該当する場合、管理者の代理人の名称及び連絡先 a.4) データ保護オフィサーの名称及び連絡先 a.5) 取扱いの目的 a.6) データ主体及び個人データの種類の記述 a.7) 個人データが開示され、又は、開示される予定の取得者の種類（第三国又は国際機関の取得者を含む） a.8) データの種類ごとの消去までの予定期間を明記したデータ保持方針 a.9) 技術的及び組織的安全管理措置の一般的記述 【AND】 B)【IF】個人データが第三国に移転される場合、【THEN】次のとおりとする。 b.1) 第三国又は国際機関への個人データの移転に関する情報 b.2) データ移転先の第三国又は国際機関の一覧 b.3)	ToEの一部である最新の取扱活動の記録の存在は、ユーロプライバシー認証に必要である。当該記録は、データベースなどの電子形式を含む書面の形式で作成されなければならない。技術的及び組織的措置の記述は、GDPR第32条の範囲を考慮に入れるのが望ましい。G.10.5.2を参照されたい。 取扱活動の一部として移転が含まれる場合、管理者は、第三国及び国際機関への移転に関する情報（それらの特定を含む）を提供するのが望ましい。さらに、必要に応じて、勧告01/2020に従い、個人データのEUにおける保護水準の遵守を確保するため、補完的措置を含む適切な保護措置が移転ツールを補完するのが望ましい。	取扱活動の記録	30	1	12
G.5.3.2	P	G	A	処理者によるデータ取扱いの記録	【IF】申請者が処理者として行動する場合、【THEN】次のとおりとする。 A) 申請者は、管理者に代わって評価対象において実施される全ての種類の取扱活動について、次の情報を含む記録を保持しなければならない。 a.1) 処理者の名称及び連絡先 a.2) 該当する場合、処理者がそのために行動する管理者（共同管理者を含む）の名称及び連絡先 a.3) 該当する場合、管理者又は処理者の代理人の名称及び連絡先 a.4) データ保護オフィサーの名称及び連絡先 a.5) 実施されている技術的及び組織的安全管理措置の一般的記述 a.6) 各管理者のために実施される取扱活動の種類 【AND】 B)【IF】個人データが第三国に移転される場合、【THEN】次の情報が提供されなければならない。 b.1) 第三国又は国際機関への個人データの移転に関する情報 b.2) データ移転先の第三国又は国際機関の一覧（識別情報を含む） b.3) 当該移転により保護のレベルが低下しないのを確保するための適切な保護措置（補完的措置を含む）に関する文書（	取扱活動の記録の存在は、ユーロプライバシー認証に必要である。当該記録は、データベースなどの電子形式を含む書面形式で作成されなければならない。 技術的及び組織的措置の記述は、GDPR第32条の全ての要素を考慮に入れるのが望ましい。 取扱活動に移転が含まれる場合、処理者は、第三国及び国際機関への移転に関する情報（それらの特定を含む）を提供するのが望ましい。さらに、必要に応じて、勧告01/2020に従い、個人データのEUにおける保護水準の遵守を確保するため、補完的措置を含む適切な保護措置が移転ツールを補完するのが望ましい。	取扱活動の記録	30.2	1	9
G.5.3.3	CP	S	A	データ取扱指示の記録	A) 管理者から処理者（、又は、該当する場合、管理者に代わって処理者から復処理者）に連絡された書面による指示のレジストリ若しくは文書、又は、その両方が存在しなければならない。 【AND】 B) 管理者が処理者に対して復処理者を従事させるのを許可するために提供した書面による承認及び条件のについてのレ	申請者は、データがデータ処理者によって指示に基づいてのみ取扱われたことを証明できるのが望ましい。 処理者は、管理者から当該復処理者についての承認を得ている場合に限り、他の処理者（すなわち復処理者）を関与させるのが望ましい。 処理者は、他の処理者を関与させている場合、当該復処理者が管理者の指示に基づいてのみ取扱いを行うことを証明するのが望ましい。これには、処理者が管理者に代わって伝達した指示が含まれ得る。	調査 データ取扱いに関する指示の記録 CISO又はDPOとの面談		1	2
G.5.3.4	CP	S	A	取扱活動の記録の完全性	評価対象の範囲内における全ての取扱活動は、取扱活動の記録に記載されなければならない。	取扱活動の記録は、全てのデータ取扱活動に関して完全かつ包括的でなければならない。申請者は、当該記録が最新であることを確保し、定期的に更新及びレビューされていることを証明するための手順又は仕組みを整備するのが望ましい。	DPOとの面談 手順又は仕組みの記録 取扱活動の記録		1	1
G.5.3.5	CP	S	A	EEAの所轄データ保護機関との協力義務	【IF】申請者がEEA域外の第三国に所在する場合、【THEN】次のとおりとする。 A) 申請者は、次の措置を実施するための規則、方針又は手順を整備しなければならない。 a.1) EEAにおける所轄データ保護機関からの要求に協力すること a.2)【AND】要求に応じて、取扱活動の記録を利用可能にすること	申請者は、ToEにおける取扱いに関し、EEA域内の所轄データ保護機関と協力するのが望ましい。これには、要請に応じて、不当な遅滞なく、取扱活動の記録を提供することが含まれる。 申請者は、EEA域内の所轄データ保護機関から取扱活動の記録を提供するように求められた場合、その要請を文書で記録するのが望ましい。当該記録には、特に次の事項が含まれるのが望ましい。 - 要請を行ったEEA域内の所轄データ保護機関 - 要請の日時 - 要請を受け取ってから記録が提供されるまでの対応期間 - EEA域内の所轄データ保護機関に提供された情報	EEA域内の所轄データ保護機関からの要求の文書記録 EEA域内の所轄データ保護機関に提供された情報	30.4	1	2
G.6				**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、並びに、取扱いの安全性** 目的　評価対象において取扱われるデータが、十分な安全性、並びに、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の恩恵を受けるのを確保すること。						
G.6.1				**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**				**25**		

G.6.1.1	C	S	A	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	A) 申請者は、次の事項の最小化を含む、データ取扱いに対して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を適用し維持することを求める方針、規則又は手順を整備しなければならない。 a.1) 個人データの収集及び取扱い a.2)【AND】個人データの保存及び保持 a.3)【AND】取り扱う個人データへのアクセス 【AND】 B) 申請者は、次の事項を含め、評価対象のデータ取扱いが、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の要件を遵守していることを文書で正式に評価しなければならない。 b.1) 蓋然性及び深刻度の観点から、データ主体の自由及び権利に対するリスクを分析すること b.2) 【AND】個人データの収集がその目的及び適法性の根拠を達成するために限定されているか否かを評価し、限定されていない場合は推奨を行うこと b.3) 【AND】個人データの取扱いがその目的及び適法性の根拠を達成するために限定されているか否かを評価し、限定されていない場合は推奨を行うこと b.4) 【AND】個人データの保持期間がその目的及び適法性の根拠を達成するために限定されているか否かを評価し、限定されていない場合は推奨を行うこと b.5) 【AND】取り扱う個人データへのアクセスが、その取扱いのためにアクセスする必要のある者に限定されているか否かを評価し、限定されていない場合は推奨を行うこと b.6)【AND】暗号化、仮名化及び匿名化技術の使用に係る適用の要否を評価すること b.7)【AND】実施された技術的及び組織的措置が最新の技術水準に適合しているか否かを評価すること 【AND】 C) DPO又は法律専門家は、次の事項を確認しなければならない。 c.1) 当該分析及び適切な措置に関する提言が適切であること c.2) 【AND】取扱目的を達成するための個人データの収集に関して、よりプライバシーへの侵襲が少ない解決策を特定しなかったこと c.3)【AND】適用可能な推奨が実施されたこと	申請者は、取扱いの手段を決定する際及び決定後に、個人データのライフサイクルの各段階の全てを通じて、個人データ及び特定の取扱いに関する個人データ取扱いの原則を保護するために設計された、証明可能かつ効果的な措置及び保護措置を講じることが期待される。特に、次の事項を考慮するのが望ましい。 - 取扱いの性質（すなわち、その特定） - 取扱いの範囲（すなわち、その規模及び範囲） - 取扱いの文脈（すなわち、その状況） - 取扱いの目的（すなわち、その目標） - 自然人の権利及び自由に対する多様な蓋然性及び深刻度のリスク（すなわち、上記の要素を考慮しながら、個人データの保護を通じて個人を保護すること） 申請者は、リスク分析を実施し、これを記録するのが望ましい。すなわち、原則違反がデータ主体に対してどのようなリスクをもたらすかを特定し、その蓋然性が高いか、及び、発生した場合に個人に対する結果がどの程度深刻であるかを判断するのが望ましい。 申請者は、取扱いに関連する選択した措置及び保護措置の効果性の評価の背後にある理由を示すことが期待される。特に、申請者は、次の事項に関する情報を提供しなければならない。 - 提供する組織的及び技術的措置が、市場で利用可能な最新技術に準拠しているか否か - 提供する措置が、取扱いに関連する異なる分野の枠組み、規格、認証、行動規範などにおいて既存かつ認識されているか否か その際、申請者は、措置の選択及び適用において、実施コストを考慮することができる。いかなる場合でも、コストにかかわらず、申請者は、取扱いがデータ取扱原則に違反しないことを確保しなければならない。 プライバシー・バイ・デザインの原則は、個人データの取扱いを伴うあらゆる行動が、その設計段階から個人データの保護を考慮して実施され、そのライフサイクルの各段階の全てを通じて必要なプライバシー措置を実装するのが望ましいことを意味する。 プライバシー・バイ・デフォルトは、管理者が、ライフサイクルの全てを通じて、各特定の取扱目的に対して厳密に必要な個人データのみが取り扱われることを確保する適切な技術的及び組織的措置を実施するのが望ましいことを定めている。 申請者は、取扱いに使用される電子機器の設定（初期設定など）が、取扱いのために予め定められた適法な目的を達成するために必要な範囲に限定して個人データが取り扱われ、かつ、必要以上に保存されないように設定されているのを確保することが期待される。 申請者が第三者のソフトウェアを使用する場合、その製品のリスクアセスメントを実施し、初期設定に法的根拠がない機能若しくは取扱いの目的と両立しない機能、又は、その両方が含まれていないことを確保するのが望ましい。 申請者は、次の記録を保持するのが望ましい。 - データ保護バイデザインの観点から、認証を受けるデータ取扱いの分析 - データ取扱いを保護するために実施された効果的な技術的及び組織的措置 - 該当する場合、特定された措置を実施しなかった理 データ最小化措置は、保管、研究又は統計の目的のためのデータ取扱いに関連する特定の要件（GDPR第89条）を考慮するのが望ましい。 組織的措置の実施のレビューは、組織図並びに役割及び責任の定義のレビューによって検証できる。面談では、CISO及びDPOからの手順及び方針の適切な適用を確認するため、存在する場合は最高執行責任者との面談が有用である。一般的に、申請者は、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を確保するために専用	方針、規則及び手順 労働者、CISO及びDPOとの面談 調査 DPOの評価及び声明 個人データ取扱いに関連するRBAC（ロールベースアクセス制御）を含む組織図、役割及び責任	25.1	1	13
G.6.1.2	C	S	A	データ最小化バイデフォルト	A) 申請者は、次の事項のために組織的又は技術的措置を実施しなければならない。 a.1) 取扱目的に必要な個人データのみを収集すること a.2) 【AND】取扱目的に必要なく、かつ、両立する目的及び法的根拠がない場合には、個人データを記録保存しないこと a.3)【AND】保持期間の終了時に、原則として、個人データを削除又は匿名化すること a.4)【AND】権限を与えられた要員のレジストリに基づいて、個人データへのアクセスを制限すること a.5) 【AND】データ主体の権利及び自由に対する取扱いの特定されたリスクを低減すべく、技術的及び組織的措置を実施するためにリスク分析を用いていること 【AND】 B) 申請者は、評価対象に適用可能な場合において、次の場合を含め、個人データを効果的に消去するための規則、手順又は仕組みを整備しなければならない。 b.1) データが、移転目的との関係において、もはや必要ない場合 b.2)【OR】データ主体によって同意が撤回された場合 b.3)【OR】データ主体が個人データの取扱いに対して異議を述べることに成功した場合 b.4)【OR】個人データが違法に取り扱われた場合	データ最小化は、取り扱われる個人データの量が、収集された目的を達成するために必要最小限に制限されるのが望ましいことを定めるものである。いかなる場合においても、申請者は、取扱いがデータ主体の合理的な期待の範囲内で行われていることを証明しなければならない。EDPBガイドライン4/2019も参照されたい。 不必要な個人データの保存は、それ自体がデータ主体のプライバシーに対する潜在的なリスクをもたらす。 申請者は、原則として、収集された全ての個人データが次の要件を充足することを証明する記録を保持するのが望ましい。 - 十分性（取扱活動の目的に対して適切な遵守に十分であること） - 関連性（取扱目的に関連していること） - 限定性（必要でない個人データを保持しないこと） GDPR第11条も考慮されるのが望ましい。 効果性は、手順の試験又は過去のデータ主体からの要求の分析によって証明され、かつ、データが有効に消去されていることが確認されるのが望ましい。 本基準のいずれかの条件を充足する場合、申請者は、自らの判断で個人データを消去することが期待される。消去は、個人データのリンク、コピー、バックアップ又は複製の全てを含むのが望ましい。	内部規則、方針及び手順 労働者、CISO及びDPOとの面談 調査 取扱いに対するRBACの文書	25.2	1	10
G.6.2				**取扱いの安全性**				**32**			
G.6.2.1	CP	G	A	セキュリティ方針	A) 申請者は、実施された技術的及び組織的措置について、取扱いのリスクに見合った適切なセキュリティ水準を示す書面による規則若しくは方針又はその両方を整備しなければならず、少なくとも次の事項が含まれなければならない。 a.1) 仮名化及び暗号化方針 a.2)【AND】データ機密保持方針 a.3)【AND】データ最小化方針 a.4)【AND】データアクセス制御方針 a.5)【AND】データ取扱いの制限 a.6)【AND】データの記録保存及び保持期間に関する方針 a.7)【AND】データの完全性、可用性及びバックアップ方針 a.8)【AND】個人データ侵害方針 a.9)【AND】「BYO（Bring Your Own Device）」方針及びデータコピーの制限 a.10)【AND】更新及びパッチ方針 a.11)【AND】暗号化及びパスワード方針 a.12)【AND】ネットワークセキュリティ方針 【AND】 B) 申請者は、個人データを取り扱う全ての労働者及び代理人に対して、教育・訓練の一環とし当該方針及び規則を伝達しなければならない（基準G.9.3.2参照）。	申請者は、次の措置を講じる手順を整備するのが望ましい。 - データ取扱い並びにデータ主体の自由及び権利に関連するセキュリティ関連リスクを分析及び特定すること - 特定された措置の実現可能性、コスト及び利益を分析すること - セキュリティリスク分析を文書化及び記録すること - （サイバー）セキュリティリスク分析及びテストが少なくとも年1回更新されるのを確保すること 申請者は、次の記録を保持するのが望ましい。 - セキュリティ方針及びガイドライン - セキュリティ監査若しくは認証、又は、その両方 - セキュリティリスクアセスメント - データ取扱いを保護するために実施された効果的な技術的及び組織的措置 - 該当する場合、特定された措置を実施しなかった理由 技術的及び組織的措置は、次の事項を考慮に入れるのが望ましい。 - 最新技術 - 実施コスト - 取扱いの性質 - 取扱いの範囲 - 取扱いの文脈 - 取扱いの目的 - 自然人の権利及び自由に対するリスク - リスクの蓋然性及び深刻度 取り扱われる個人データのセキュリティ水準の見直しは、あらかじめ定められたスケジュールに従って実施されるのが望ましく（少なくとも年1回実施することが推奨される）、また、データ取扱活動の文脈に変更があった場合にも実施されるのが望ましい。 セキュリティ方針は、適用可能な補完的各国規制も考慮に入れるのが望ましい。ISOなどの標準化された統制は、申請者が本認証の基準を充足していることを証明するのに役立つかもしれない。a.1) において仮名化及び暗号化が適用可能な場合は、T.1.2.1及びT.1.2.2のガイダンスを参照されたい。	セキュリティに関する規則及び方針 労働者、CISO及びDPOとの面談 セキュリティテスト報告書	32.1	1	13
G.6.2.2	CP	G	A	指示のみに基づく取扱い	申請者は、その権限の下で行動する自然人が、次の場合を除き、個人データを取り扱わないことを確保するための規則、方針、契約条項、運用指針又は仕組みを整備しなければならない。 a.1) 管理者から指示を受けている場合 a.2)【OR】EU法又はEEA加盟国の国内法により要求される場合	申請者は、次の記録を保持するのが望ましい。 - 個人データの取扱いを承認された自然人 - データ取扱活動 - 個人データの取扱いに関し、その権限の下にある自然人に伝達された指示及びその日付	セキュリティに関する規則及び方針 労働者、CISO及びDPOとの面談	32.4	1	2
G.6.2.3	CP	G	A	契約上の機密保持義務	A) 申請者は、個人データを取り扱う全ての自然人が、その活動の終了後も機密保持義務に法的に拘束されることを確保するための規則、方針又は手順を整備しなければならない。	申請者は、個人データにアクセスできる者が、申請者との業務関係終了後も含め、個人データに関連する全ての情報の機密を保持しなければならないように契約上拘束されていることを確保するのが望ましい。	規則、方針及び手順 雇用契約書 サンプル分析	32	1	1

G.6.2.4	CP	S	A	データ取扱いに関するリスクアセスメント	A) 申請者は、再現可能な方法に基づき、次の事項に関連するリスクを含む、自然人の権利及び自由に影響を及ぼすおそれのあるデータ取扱いよって生じるリスクを評価しなければならない。 a.1) 当該取扱い（その範囲、目的、文脈及び性質を考慮すること） a.2) 【AND】データの可用性及び継続性（個人データの偶発的又は違法な破壊又は紛失を含む） a.3) 【AND】データの完全性（個人データの偶発的又は違法な改変を含む） a.4) 【AND】データの機密性（個人データの偶発的、違法又は無権限の開示又はアクセス（第三国へのデータ移転を含む）を含む） a.5) 【AND】データのレジリエンス（個人データ侵害のリスクを含む） a.6) 【AND】データの不適切な取扱い（違法若しくは無権限の取扱い、又は、データの不正利用を含む） a.7) 【AND】データ主体の権利及び自由（差別、アイデンティティ・セフト又は詐欺、仮名化の無権限の再識別、評判又は財務的損害のリスクを含む） a.8) 【AND】該当する場合、BYODの実務 a.9) 【AND】物理的及び電子的なデータ環境 a.10) 【AND】監視及びログ記録活動 a.11) 【AND】アクセス及び認証メカニズム a.12) 【AND】該当する場合、暗号化、仮名化又は匿名化されたデータの再識別 a.13) 【AND】該当する場合、ウェブインターフェース、無線通信及びネットワーク 【AND】 B) リスク分析で特定されたリスクは、いかなる場合においても、DPO及びCISOへの助言のために提供されなければならず、かつ、当該特定されたリスクを低減するためのリスク低減計画をもたらさなければならない。 【AND】 C) リスクアセスメント及びリスク低減計画は、次の要件を充足しなければならない。 c.1) 実施されるべきセキュリティ措置及び既に実施されている措置を含むこと c.2) 【AND】該当する場合、データ輸出者によって要求されるセキュリティ措置を特定すること c.3)	G.6.2.4に基づくリスクアセスメントは常に必要であり、データ保護影響評価（DPIA）が必要な場合には（基準G.8.1.1を参照）、G.8.2.2で要求される評価の一部を構成する。また、申請者は、データ取扱いのセキュリティ及び可用性に関連するリスクも評価しなければならない。申請者は、従うべきリスクアセスメント手法を定義するのが望ましい。当該手法は、特定された各リスクの蓋然性及び潜在的影響の両方を考慮するのが望ましい。ISO 31000のような標準的手法は適切とみなされる場合がある。 リスクアセスメントは、取り扱われるデータの性質、並びに、自然人の権利及び自由に対して高いリスクをもたらす可能性のある個人データの取扱いであるか否かを考慮に入れるのが望ましい。これは、申請者が新たな技術的又は組織的解決策を利用する場合、脆弱なデータ主体に関するデータを収集する場合、大規模にデータを取り扱う場合、センシティブデータ若しくは高度に個人的なデータを取り扱う場合、又は、系統的な監視のためのツールを使用している場合に該当する。したがって、申請者は、少なくとも次のリスクを考慮及び評価するのが望ましい。 - 個人データの偶発的又は違法な破壊又は喪失 - 個人データの偶発的又は違法な変更 - 個人データの偶発的、違法又は無権限の開示及びアクセス、並びに、仮名化の無権限の再識別 - 特別な種類のデータの取扱い、プロファイリング若しくは大規模なデータ取扱いに起因し、又は、差別、アイデンティティ・セフト、詐欺、経済的損失、評判の損害、職業上の守秘義務によって保護された個人データの機密性の喪失、仮名化の無権限の再識別、その他の重大な経済的若しくは社会的な不利益、又は、データ主体の権利及び自由の行使の妨害に繋がる物理的、物的若しくは非物的損害 センシティブ、非常に個人的なデータ、脆弱な者のデータ、生体データ、又は、差別若しくは重大な社会経済的不利益を引き起こす可能性のあるその他のデータを明らかにするリスクは、高い影響を持つものとして評価されるのが望ましい。 申請者は、実施されたリスクアセスメント、当該アセスメントの結果として特定されたリスク、及び、当該アセスメントに応じて講じられ、又は、採用された低減措置若しくは緊急対応策又はその両方に関する明確な記録を保持するのが望ましい。 各適用可能な基準は個別に充足しなければならず、リスクアセスメントによって特定された措置は対処されなければならないことに留意することが重要である。リスクアセスメントの推奨事項が他の基準の要件を超える場合でも、前者は依然として充足しなければならない。 ISO27001及びISO27002の統制は、情報システムのセキュリティの文脈においてリスクアセスメントに言及しているため、関連し得る。 リスクアセスメント及びリスク低減計画は、定期的に見直されるのが望ましく、少なくとも年1回、新たなリスク	リスク分析報告の文書レビュー リスク評価方法の評価	32.2			
G.6.2.5	CP	S	A	補完的な技術的措置及び組織的措置	A) 申請者は、次の措置を講じなければならない。 a.1) 技術的及び組織的措置（TOM）の適切性を評価すること a.2) 【OR】評価対象において取り扱われるデータの安全性確保及び保護のために講じられた技術的及び組織的措置の補完的認証が、少なくとも本認証要件と同等であること 【AND】 B)	ユーロプライバシーは、技術的及び組織的措置の確認項目及び管理項目の包括的な一覧を維持している。当該一覧は申請者に提供され、記入の上、監査人に報告することができる。 DPOによる評価及び結論に疑義がある場合、監査人は当該結論に異議を唱え、補完的評価を要求するのが望ましい。 同等の認証は、ユーロプライバシー基準と同等のセキュリティ水準を達成するのが望ましい。	検査 技術的措置及び組織的措置評価報告書 補完的監査 検査 DPOの評価及び宣言	32	1	3	
G.7				**データ侵害の管理** 目的　評価対象に関連するデータ侵害が規制要件を遵守して対処されるのを確保すること。						
G.7.1				**所轄データ保護機関への個人データ侵害の通知**			**33**			
G.7.1.1	CP	G	A	データ侵害の文書化義務	A) 申請者は、少なくとも次の事項を含む、個人データ侵害の記録を保持しなければならない。 a.1) 個人データ侵害の性質 a.2) 【AND】影響を受け、又は、影響を受ける可能性のある個人データの種類 a.3) 【AND】影響を受け、又は、影響を受ける可能性のあるデータ主体の概数 a.4) 【AND】当該侵害に関係し、又は、関係する可能性のある個人データ記録のカテゴリー及び概数 a.5) 【AND】個人データ侵害の想定される結果 a.6) 【AND】個人データ侵害に対処するために講じられ、又は、提案された措置（悪影響を低減するための措置を含む）	申請者は、データ侵害が発生する前であっても、個人データ侵害の記録を整備しておくのが望ましい。	データ侵害の記録	33.5	1	6	
G.7.1.2	C	G	A	管理者の個人データ侵害の通知及び伝達義務	A) 申請者は、次の措置を実施するための規則、手順又は仕組みを整備しなければならない。 a.1) 個人データ侵害及び講じられた措置を、日時とともに記録すること a.2) 【AND】当該データ侵害が自然人の権利及び自由に対するリスクをもたらす可能性があるかを評価すること a.3) 【AND】リスク、その可能性及びデータ主体に対する潜在的影響を最小化するための適切な措置を決定及び実施すること a.4) 【AND】当該個人データ侵害が自然人の権利及び自由に対するリスクをもたらす可能性がある場合、不当な遅滞なく、かつ、認識してから72時間以内にデータ保護機関に通知すること a.5) 【AND】当該個人データ侵害が自然人の権利及び自由に対するリスクをもたらす可能性がある場合、G.7.2.2の例外が適用される場合を除き、不当な遅滞なくデータ主体に通知すること	申請者は、次の記録を保持するのが望ましい。 - 個人データに関連するセキュリティインシデントを認識した時期 - 全ての特定されたデータ侵害及びその日時 - 個人データ侵害に関連する基準G.7.1.1に記載された事実 - 個人データ侵害の想定される結果 - 個人データ侵害に関連する所轄データ保護機関若しくはデータ主体又はその両方への全ての通知若しくは連絡又はその両方 - 日時を含む講じられた措置 - 該当する場合、所轄データ保護機関（個人データ侵害を認識してから72時間以内）若しくはデータ主体又はその両方に通知しなかった理由 （もしあれば、）過去12か月間において、データ主体の権利及び自由をリスクにさらした全ての記録された侵害は、72時間以内に所轄データ保護機関に通知されるのが望ましい。 侵害通知に関する意見03/2014において、WP29は、侵害が次の3つの一般的な情報セキュリティ原則に基づいて分類できると説明されている。 -「機密性侵害」 - 個人データの無権限又は偶発的な開示又はアクセスがあった場合 -「完全性侵害」 - 個人データの無権限又は偶発的な変更があった場合 -「可用性侵害」 - 個人データへのアクセスの偶発的又は無許可の喪失又は破壊があった場合	規則、手順又は仕組み データ侵害の記録 労働者とDPOとの面談 調査 手順の試験	33.1, 34.1	1	5	
G.7.1.3	P	G	A	処理者の個人データ侵害を不当な遅滞なく通知する義務	A) 申請者は、次の措置を実施するための規則、手順又は仕組みを整備しなければならない。 a.1) 個人データ侵害及びその際に講じられた措置を日時とともに記録すること a.2) 【AND】データ主体に対するリスク及び潜在的影響を最小限に抑えるための適切な措置を特定し、これを講じること a.3) 【AND】自然人の権利及び自由に対するデータ侵害のリスクを評価するために管理者を支援すること a.4) 【AND】遅滞なく関連するデータ管理者に侵害を通知すること a.5) 【AND】個人データ侵害が自然人の権利及び自由に対するリスクをもたらす可能性がある場合、遅滞なく、かつ、それを認識してから72時間以内に所轄データ保護機関に通知すること	処理者（及び復処理者）は、いかなる侵害も対処し、関連するデータ管理者に不当な遅滞なく通知されることを確保するための規則、手順又は仕組みを整備しなければならない。データ管理者は、侵害に対処、通知及び連絡を行うための非常に厳格な期限を遵守しなければならないことを念頭に置く必要がある。処理者は、かかる通知を遅らせるべきではない。 申請者は、次の記録を保持しなければならない。 - 個人データに関連するセキュリティインシデントを認識した時期 - 全ての特定されたデータ侵害及びその日時 - 個人データ侵害に関連する基準G.7,1,1に記載された事実 - 個人データ侵害の想定される結果 - 個人データ侵害に関連する所轄データ保護機関若しくはデータ主体又はその両方への全ての通知若しくは連絡又はその両方 - 講じられた措置及びその日時 - 該当する場合、所轄データ保護機関（個人データ侵害を認識してから72時間以内の期間内に）若しくはデータ主体又はその両方に通知しなかった理由	方針、規則及び手順 労働者、CISO及びDPOとの面談 調査	33.2	1	5	
G.7.1.4	C	G	A	通知要件	A) データ侵害を所轄データ保護機関に通知する手順には、次の情報を含めなければならない。 a.1) 個人データ侵害の性質 a.2) 【AND】（可能な場合、）関係するデータ主体及び個人データの種類並びに概数 a.3) 【AND】データ保護オフィサー又はより多くの情報を入手することのできるその他の連絡窓口の名称及び連絡先 a.4) 【AND】個人データ侵害の想定される結果 a.5) 【AND】個人データ侵害に対処するために管理者によって講じられ、又は、提案された措置（該当する場合、悪影響	申請者は、通知のためのモデルテンプレートを有しているのが望ましい。通知手順には、次の情報を含めなければならない。 - 個人データ侵害の性質 - 関連するデータ主体及び個人データの種類並びに概数（可能な場合） - データ保護オフィサー又はより多くの情報を入手することのできるその他の連絡窓口の名称及び連絡先 - 個人データ侵害の想定される結果 - 個人データ侵害に対処するために管理者によって講じられ、又は、提案された措置（該当する場合、悪影響を低	規則、手順又は仕組み データ侵害の記録 労働者及びDPOとの面談 調査 手順の試験	33.3	1	5	
G.7.2				**データ主体への個人データ侵害の連絡**			**34**			

G.7.2.1	C	G	A	侵害連絡の要件	A) データ主体に対して個人データ侵害を通知するための手順又は仕組みは、明確かつ平易な言語により、少なくとも次の情報を含めなければならない。 a.1) 個人データ侵害の性質 a.2) 【AND】関係する個人データ記録のカテゴリー a.3) 【AND】データ保護オフィサー又はより多くの情報を入手することのできるその他の連絡窓口の名称及び連絡先 a.4) 【AND】個人データ侵害の想定される結果 a.5) 【AND】個人データ侵害に対処するために管理者によって講じられ、又は、提案された措置（若しくはデータ主体に推奨される措置、又は、その両方。必要とされる場合、悪影響を低減するための措置を含む。）	申請者は、次の文書化された記録を保持するのが望ましい。 - 全ての特定された個人データ侵害及びその日時 - 個人データ侵害に関連する事実 - 個人データ侵害の影響 - 個人データ侵害に関連する連絡 - フォローアップ措置及び是正措置並びにその日時 - 該当する場合、データ主体に通知しなかった理由。 証明は、過去の記録のサンプリング、文書化された演習又は技術的実証によって実施できる。 データ主体への影響の例には、差別、アイデンティティ・セフト若しくは詐欺、財務的損失及び評判への損害、侵害が人種的若しくは民族的な出自、政治的な意見、宗教上若しくは思想上の信条、労働組合への加入を明らかにする個人データを含む場合、又は、遺伝子データ、健康に関するデータ、性生活に関するデータ、有罪判決及び犯罪行為、若しくは、関連する安全管理措置を含む場合が含まれる。	違反及び連絡の記録 方針、規則及び手順 労働者及びDPOとの面談	34.2		
G.7.2.2	C	S	E	許容される免除	【IF】次の条件を充足する場合、【THEN】データ主体への直接的な通知は必要ないものとする。 A) 次のいずれかの例外により、連絡が行われなかった場合 a.1) 申請者が、侵害された個人データに対するアクセスを承認されていない者は当該個人データを理解できないようにするための適切な技術的及び組織的措置（暗号化など）を実施した場合 a.2) 【OR】管理者が、データ主体の権利及び自由に対する高いリスクがもはや現実化する可能性がないことを確保するための事後的な措置を講じた場合 a.3) 【OR】直接の連絡が過大な負担を要し、【AND】、これに代えて公表（、又は、データ主体が平等に効果的な方法で通知されるような類似の措置）が行われた場合	いかなる例外も、明確に正当化及び文書化されるのが望ましい。GDPRが一定の例外を認めている場合でも、ユーロプライバシーは、申請者に対し、例外の使用を最小限に抑えることにより、データ主体の権利と自由を優先する保守的な方針を採用することを奨励する。 「直接的」な連絡とは、個別のデータ主体に対して行われる連絡を意味する（例えば、公表ではない）。 申請者は、データ主体に通知しない理由を正当化し、又は、別の方法（例えば、公表）でデータ主体に通知するのが望ましい。	記録、内部方針及び手順 試験及び検証 調査 DPO及び労働者との面談	34.3		
G.8				**データ保護影響評価（DPIA）** 目的　評価対象におけるデータ取扱いがデータ保護影響評価を必要とする場合、データ保護影響評価が規制要件を遵守して実施されるのを確保すること。							
G.8.1				**データ保護影響評価（DPIA）が必要か否かを評価する義務**						**35**	
G.8.1.1	C	S	A	データ保護影響評価（DPIA）	A) DPIAプロセスは、次の措置を実施しなければならない。 a.1) 自然人の権利及び自由に対するリスクを低減するための評価及び措置にDPOを関与させること a.2) 【AND】データ主体又はその代理人の意見を考慮すること a.3) 【AND】該当する場合、DPIAの範囲に含まれる取扱い業務の影響を評価する際に、承認された行動規範、認証及びその他の拘束力がある実行可能な約束の遵守を考慮すること a.4) 【AND】該当する場合、リスクに対処するための措置の計画を採用すること（保護措置、セキュリティ対策及び仕組みが含まれる） a.5) 【AND】該当する場合、データ主体の権利及び自由に対するリスクを低減するために想定される措置を実施すること a.6) 【AND】DPIAが取扱いによって高リスクをもたらされることを示し、リスクを低減するための措置が取られなかった場合には、所轄データ保護機関に相談し、その通信を記録すること 【AND】 B) 申請者はDPIAを実施しなければならない。ただし、申請者が次の条件を満たす場合は除く。 b.1) データ主体の権利及び自由に対するリスクの事前の書面による評価を実施していること b.2) 【AND】書面による評価において、データ主体の権利及び自由に対する高リスクが存在しないと結論付けていること	DPIAは、単一のデータ取扱業務、又は、性質、範囲、文脈、目的及びリスクにおいて類似する複数の取扱業務に関して実施され得る。また、技術製品のデータ保護影響を評価するためにも有用である。DPIAは、データ主体の権利及び自由に対する全てのリスクを考慮するのが望ましい。 WP29ガイドライン（WP248 rev.01）（pg. 9-11）により提供される基準は、データ主体に対する高いリスクを特定するために考慮されるのが望ましい。申請者は、次を含むデータ取扱いに対してDPIAを実施するのが望ましい。 - 評価又はスコアリング - 法的効果又はこれに類する重要な影響を伴う自動的な決定 - 系統的な監視 - センシティブデータ又は高度に個人的な性質のデータ - 大規模なデータ取扱い - データセットの照合又は結合 - 脆弱なデータ主体に関するデータ - 新しい技術的又は組織的手段の革新的な使用又は適用 - データ主体が権利を行使し、又は、サービス若しくは契約を利用することを妨げる取扱い 申請者は、次の事項に関する文書化された記録を保持するのが望ましい。 - DPIAの適用可能性及び関連性の評価 - 該当する場合、DPIA文書及び結論 - 該当する場合、講じられたフォローアップ措置及び是正措置並びにその日時	DPIA報告書及び文書 DPOによる事前評価 DPOの声明 DPOとの面談	35.1, 35.3, 35.4	1	10
G.8.1.2	C	S	E	許容される免除	【IF】（EU又はEEA加盟国によって要求される場合を除き、）DPIAが必要ではない場合、【THEN】次のとおりとする。 A) 取扱いがEU法又はEEA加盟国の国内法に法的根拠があり、管理者が当該法律の適用を受け、【AND】、次の同様のデータ取扱いについて、影響評価が既に実施されている場合 【OR】	いかなる例外も、明確に正当化及び文書化されるのが望ましい。例えば、評価対象は、GDPR第35条第5項に基づき、DPIAの義務から除外される取扱いの国家一覧に該当する場合がある。	関連法	35.10.	1	2
G.8.2				**データ保護影響評価（DPIA）チェックの要件** 条件　【IF】DPIAが適用される場合、【THEN】次のとおりとする。						**27**	
G.8.2.1	C	S	A	DPIAのプロセス要件	A) DPIAプロセスは、次の要件を充足しなければならない。 a.1) 自然人の権利及び自由に対するリスクの評価及びこれを低減するための措置にDPOを関与させること a.2) 【AND】データ主体又はその代理人の見解を考慮すること a.3) 【AND】該当する場合、DPIAの対象となる取扱業務の影響を評価する際に、承認された行動規範、認証及びその他の拘束力があり執行可能な約束の遵守を考慮すること a.4) 【AND】該当する場合、リスクに対処するために想定される措置（保護措置、セキュリティ措置及び仕組みを含む）に関する計画を採用すること a.5) 【AND】該当する場合、データ主体の権利及び自由に対するリスクを低減するために予定された措置を実施すること a.6) 【AND】DPIAにより当該取扱いが高いリスクをもたらすことが示され、かつ、リスクを低減するための措置が講じられなかった場合、所轄データ保護機関と協議し、そのやりとりが記録されること 【AND】 B) 申請者は、次の措置を講じた場合を除き、DPIAを実施しなければならない。 b.1) データ主体の権利及び自由に対するリスクについて、書面による事前評価を実施していること b.2)	申請者は、次の段階を含め、DPIAプロセスがDPIAを実施するための一般的な反復プロセス（WP29ガイドラインWP248 rev.1）に整合していることを確保するのが望ましい。 - 想定される取扱いの記述 - 必要性及び比例性の評価 - 想定される措置の特定 - データ主体の権利及び自由に対するリスクの評価 - リスクに対処するために想定される措置の定義 - 文書化 - 監視及び見直し DPOの助言は求められ、当該助言に基づいて管理者が行った決定とともに文書化されるのが望ましい。DPIAの実施は、DPOによって監視されるのが望ましい。 申請者は、適切な場合、文脈に応じた様々な手段（調査、質問票等）を通じて、データ主体又はその代表者の意見を求めることができ、最終的な決定がデータ主体の意見と異なる場合には、その乖離の理由を記録しなければならない。データ主体又はその代表者の意見が求められなかった場合、申請者はその理由を提供しなければならない。	DPIA報告書及び文書 DPOとの面談	35.2, 35.7, b	1	10
G.8.2.2	C	S	A	DPIAの内容要件	A) DPIAは、少なくとも、次の要素を含まなければならない。 a.1) DPIAが実施される予定の取扱業務の体系的な記述 a.2) 【AND】個人データの取扱目的 a.3) 【AND】該当する場合、取扱いに関連して管理者が求める正当な利益 a.4) 【AND】目的との関係における取扱いの必要性及び比例性の評価 a.5) 【AND】データ主体の自由及び権利に対するリスクの評価 a.6) 【AND】リスクに対処するために想定される措置（該当する場合には保護措置、セキュリティ措置及び仕組みを含み、データ主体及びその他の関係者の権利及び正当な利益を考慮したもの） a.7) 【AND】該当する場合、EEA域内の所轄データ保護機関と協議することの推奨	DPIAは、取扱いの前に、かつ、取扱業務の設計において可能な限り早期に、一部の取扱業務がまだ不明であっても、実施されるのが望ましい。 GDPRに基づくDPIAは、データ主体の権利に対するリスクを管理するためのツールであり（WP29ガイドラインWP248 rev.1）、申請者は評価を実施する際にその視点を考慮するのが望ましい。 高いリスクの取扱いが計画されている場合、データ管理者は、次の措置を実施するのが望ましい（WP29ガイドラインWP248 rev.1 + 附属書2）。 - 取扱いの体系的な記述を実施、必要性及び比例性を評価、データ主体の権利及び自由に対するリスクを管理、及び、関係者を関与させる適切なDPIA手法を選択及び文書化すること; - 内部プロセス、文脈及び文化に従い、設計、開発、変更、リスク及び運用レビューのプロセスにDPIAを統合すること - 適切な関係者を関与させ、その責任を明確に定義すること - 必要に応じてDPIA報告書を所轄データ保護機関に提供すること - 緩和されない高いリスクが残存する場合、所轄データ保護機関と協議すること - 定期的にDPIAを見直すこと - 決定された事項を文書化すること DPIAプロセスは、特に是正措置若しくは行動計画又はその両方に関し、申請者に対し、評価の結論及びDPOの意見に基づく正式な決定を求めること DPIAは、次のようなリスクを考慮するのが望ましい。 - データ主体に対する差別及びその他の重大な経済的又は社会的不利益を伴うリスク -	DPIA報告書及び文書 DPOとの面談	35.7	1	7

G.8.2.3	C	S	A	データ主体関与の要件	申請者は、データ保護影響評価のために協議したデータ主体若しくはその代理人、又は、その両方の見解の記録を保持しなければなら（ず、又は、データ主体若しくはその代理人を関与させなかったことについての文書化された正当化理由を保持しなければなら）ない。	申請者は、文脈に応じて様々な手段（調査、質問票など）を通じて、データ主体又はその代表者の意見を求めることができ、最終的な決定がデータ主体の意見と異なる場合には、その理由を文書化するのが望ましい。データ主体の意見を求めなかった理由に関する文書も準備するのが望ましい。 申請者は、次の文書による記録を保持するのが望ましい。 - データ主体又はその代表者と協議するか否かの評価及び決定 - 該当する場合、競技の証拠 - 該当する場合、データ主体の懸念に対処するために講じられたフォローアップ措置及び是正措置 - 該当する場合、データ主体によって提起された懸念に対処しなかった理由 申請者は、データ主体又はその代表者によって提起された懸念がどのように考慮されたかを文書化するのが望ま	DPIAの報告書及び文書 DPOとの面談	35.9				
G.8.2.4	C	G	A	リスク変更に伴うDPIAの見直し	A) 申請者は、評価対象のデータ取扱いの範囲若しくは目的が実質的に変更された場合、又は、新たなリスクにさらされた場合には、DPIA又はDPIAを実施しないという決定を見直すための規則又は手続を整備しなければならない。	申請者は、DPIAが継続的に見直され、定期的に再評価されることを確保し、特に次のいずれかの場合にはDPIAを実施するのが望ましい。 - 実施条件（範囲、目的、収集される個人データ、データ管理者又は取得者の身元、データ保持期間、技術的及び組織的措置など）の変更が発生した場合 - 取扱業務から生じるリスクに変更が発生した場合 - 取扱活動の組織的又は社会的文脈に変更が発生した場合 該当する場合、申請者は、次の文書による記録を保持するのが望ましい。 - DPIAを見直すか否かの評価及び決定 - DPIAの見直し及びその結論 - DPIAの見直しの結論に対処するために講じられたフォローアップ措置及び是正措置	規則及び手順 DPOとの面談	35.1.m	1	1		
G.8.2.5	C	S	A	高いリスクが特定された場合の所轄データ保護機関への協議義務	【IF】DPIAによって、データ主体の権利又は自由に対する残存する高いリスクが特定された場合、【THEN】次のとおりとする。 A) 管理者は、次の措置を講じなければならない。 a.1) 特定されたリスクについて、所轄データ保護機関に通知し、協議すること a.2) 【AND】所轄データ保護機関の意見を受けること a.3) 【AND】該当する場合、当該意見に記載された推奨措置を実施すること a.4) 【AND】当該機関の意見に記載された実施措置について、所轄データ保護機関に通知すること a.5) 【AND】所轄データ保護機関とのやりとり及びその結果を、日時とともに記録すること	DPIAが高い残存リスクを明らかにした場合、データ管理者は、取扱いに関して所轄データ保護機関に事前協議を求める必要がある（第36条第1項）。この一環として、DPIAは完全な形で提供されなければならない（第36条第3項(e)）。 データ管理者がデータ主体の権利及び自由に対するリスクを許容可能な水準に低減するための適切な措置若しくは十分な措置又はその両方を見出すことができない場合（すなわち、残存リスクが依然として高い場合）、所轄データ保護機関との協議が必要である。この場合、特に、DPIAにデータ主体又はその代表者の意見を含めるの望ましい実務である。 また、加盟国法により、公共の利益のために管理者が実施する職務の遂行に関連する取扱い（社会的保護及び公衆衛生に関する取扱いを含む）について、管理者は、所轄データ保護機関と協議若しくは事前承認を取得、又は、その両方が求められている場合には、当該機関と協議しなければならない（第36条第5項）。 所轄データ保護機関がDPIAに関する協議を行う場合、申請者は、所轄データ保護機関に対し、次の情報を提供しなければならない。 - 管理者、共同管理者又は処理者のそれぞれの責任 - 意図された取扱いの目的及び手段 - データ主体の権利及び自由を保護するための措置及び保護措置 - （該当する場合） DPOの連絡先 - データ保護影響評価 - 所轄データ保護機関が要求するその他の情報 -	監督機関とのやりとり	36	1	1		
G.9				**データ保護オフィサー（DPO）** 目的　　評価対象におけるデータ取扱いのコンプライアンスを監督するデータ保護オフィサーの役割、機能及び資格が必要な要件を充足する（十分である）のを確保すること。						1	5
G.9.1				**データ保護オフィサーの指名**					**37**		
G.9.1.1	CP	G	A	データ保護オフィサーの指名	A) 申請者は、データ保護オフィサーを指名しなければならない。	GDPRはDPOの指名が常に必要ではないことを認めているが、ユーロプライバシー認証は、DPOが正式に指名されることを要求する。DPOは外部の者であってもよく、又は、他の機能を持つこともできるが、利益相反を生じさせてはならない。 DPOは、データ取扱いが適用可能な規制を遵守しているかを監督するのが望ましい。適切な独立性を確保するため、DPOはデータ取扱いの目的及び手段を決定する人物であってはならない。	DPOとの面談 DPOの契約書 申請者のウェブサイト	37.1	1	1		
G.9.1.2	CP	G	A	DPOの要件	A) 申請者のデータ保護オフィサーは、次を含む必要な専門的資質を有さなければならない。 a.1) GDPRを含むEEAのデータ保護法及び実務に関する正式な資格 a.2) 【OR】GDPRを含むデータ保護法の適用に関する最低5年の実務経験	特定の状況における例外に基づく越境移転は、明確に文書化されるのが望ましい。移転がデータ主体の同意に基づく場合には、当該同意は、事前に説明を受けた上で、データ主体によって明瞭かつ明確に与えられたものであるのが望ましい。	DPOの求人通知 DPOの履歴書 DPOとの面談 DPOの資格証明書	37.5	1	2		
G.9.1.3	CP	G	A	DPOの連絡先	A) DPOとの連絡先若しくは連絡の手段、又は、その両方は、次の要件を充足しなければならない。 a.1) データ主体に公開され、利用可能であること a.2) EU法又はEEA加盟国の国内法により要求される場合、所轄データ保護機関に通知されていること	DPOの連絡先は公表され、データ主体が利用可能であり、かつ、データ保護機関に通知されているのが望ましい。DPOの連絡先には、DPOの個人名を必ずしも含める必要はなく、データ主体か当該連絡先に送信された連絡及び要請が効果的にDPOに伝達される限りで足りる。	申請者のウェブサイト 所轄データ保護機関とのやりとり	37.7	1	2		
G.9.2				**データ保護オフィサーの位置付け**					**38**		
G.9.2.1	CP	G	A	DPO指令の伝達	A) 申請者は、次の規則、方針又は手順を整備しなければならない。 a.1) 労働者及び経営陣に対し、適時に、データ保護に関する全ての問題にDPOを関与させるよう要請すること a.2) DPOに対し、個人データの取扱業務の遵守状況を監視するための権限及び有効なアクセスを付与すること	申請者は、DPOのデータ保護に関する問題への関与を証明するため、DPOの活動に関する文書化された記録を保持するのが望ましい。申請者は、関連する規則、方針又は手順において、DPOに通知することが義務付けられている場合を含め、かつ、かかる指定について労働者に通知するのが望ましい。a.2)の文脈において、DPO及び他のプライバシー専門家は、その義務を履行するために必要な場合、個人データ及び取扱活動へのアクセスを付与されるのが望ましい。	規則、方針及び手順 DPO活動の記録	38.1	1	2		
G.9.2.2	CP	G	A	DPOの支援	A) 申請者は、DPOに対し、その職務遂行及び専門知識の維持（教育・訓練及び能力構築など）を可能にする資源を配分しなければならない。	データ保護に関連するワークショップ、ウェビナー、トレーニングコース又は会議への参加などのDPOの継続的な教育・訓練のため、専用の予算を配分するのが望ましい。	予算配分 DPOとの面談	38.2	1	1		
G.9.2.3	CP	G	A	DPOの独立性	A) 申請者は、次の目的のために規則、方針又は契約条項を採用しなければならない。 a.1) DPOがその職務を遂行する際の自律性及び独立性を保護すること a.2) 【AND】DPOがその職務を遂行する際に解任又は処罰されるのを防止すること a.3) 【AND】DPOが申請者の最高経営層に直接報告できるようにすること	DPOは完全に独立しているのが望ましい。例えば、EDPBは、EU域内に拠点を有する外部のデータ保護オフィサー（「DPO」）の役割と、EU域内の代理人の機能は両立しないと考えている。代理人は、管理者又は処理者から委任を受け、その代理として行動し、その直接的な指示の下で行動することになる。公平性の理由から、DPOは、過去24か月間において、その権限の下でデータ取扱活動の定義及び管理に関与しないのが望ましい。 DPOは外部の者であってもよく、又は、他の機能を持つこともできるが、利益相反を生じさせてはならない。 DPOは、データ取扱いが適用可能な規制を遵守しているかを監督するのが望ましい。適切な独立性を確保するため、DPOはデータ取扱いの目的を決定する者でないのが望ましい。	規則、方針及び手順 DPOの契約書	38.3	1	3		
G.9.2.4	CP	G	A	データ主体のDPOへのアクセス	A) データ主体は、その個人データの取扱いに関連する全ての問題及び自己の権利行使について、DPOに連絡することができなければならない。	申請者は、DPOの連絡先を明確な方法で提供し、外部ウェブサイトなどを通じて公に利用可能かつアクセス可能にするのが望ましい。 申請者は、次の完全な記録を保持するのが望ましい。 - DPOへのデータ主体からの要求及びその日付 - データ主体とのDPOの連絡及びその日付 - 要求の評価及びフォローアップ措置並びにその日付 - 該当する場合、DPOが当該要求に応じなかった理由 データ主体との連絡は、明確で理解可能な方法で行われるのが望ましい。	申請者のウェブサイト 調査 連絡手順の試験	38.4	1	1		
G.9.2.5	CP	G	A	適切なDPOの作業時間	A) DPOとの契約には、次の条項を含めなければならない。 a.1) DPOが、その職務遂行に関して、契約終了後も守秘義務又は機密保持に拘束されること a.2) 【AND】DPOが所轄データ保護機関と協力し、連絡するのを承認すること a.3) 【AND】DPOに対し、その職務遂行において、利益相反を回避し又は報告する義務を負わせること	機密保持条項は、DPOの契約上の義務の一部であるのが望ましい。ただし、当該契約上の義務は、EU法又はEEA加盟国の国内法に従い、DPOが所轄データ保護機関に対し、機密情報を連絡及び共有することを妨げないのが望ましい。 申請者は、利益相反を特定、報告及び対処するための手順を整備するのが望ましい。DPOが他の職務を遂行し、義務を履行する場合、その補足的な活動によって生じる利益相反のリスクを評価する手順を有することが推奨される。 申請者は、次の記録を保持するのが望ましい。 - 該当する場合、特定された利益相反のリスク - 特定された利益相反のリスクの評価及びフォローアップ措置 - DPOが他の職務を遂行し、義務を履行する場合、その補足的な活動に伴う利益相反のリスクが評価されたことを証明する文書 DPOは外部の者であってもよく、又は、他の機能を持つこともできるが、利益相反を生じさせてはならない。	DPOの契約書 規則及び方針	38.5, 38.6	1	3		

G.9.2.6	CP	G	A	適切なDPO作業時間	A) 申請者は、DPOの職務遂行を考慮して、必要となる作業時間を評価及び文書化しなければならない。	DPOのパートタイムの職位は、DPOがその職務を遂行するために割り当てられた作業時間が十分であることを条件として、許容される。	DPOの契約書 DPOの勤務時間評価の文	38.2	1	1	
G.9.3				**データ保護オフィサーの職務**				**39**			
G.9.3.1	CP	G	A	DPOの職務及び責務	A) 申請者は、次の職務がDPOに割り当てられていることを証明しなければならない。 a.1) データ取扱いに関与する申請者及びその労働者に対し、データ保護に関する義務について通知及び助言を行うこと a.2) 【AND】データ取扱いのリスク、並びに、適用可能なデータ保護規制、方針及び本認証への遵守状況を監視すること a.3) 【AND】取扱業務に関与する職員の意識向上及び教育・訓練を行うこと a.4) 【AND】データ保護監査を監督すること a.5) 【AND】データ保護影響評価の実施に関する助言を行い、その実施を監視すること a.6) 【AND】所轄データ保護機関と協力し、かつ、連絡窓口として行動すること a.7)	申請者は次の記録を保持するのが望ましい。 - DPOに係る契約 - DPOに割り当てられた職務 - DPAとの連絡 - DPOの活動 - データ保護に関する教育・訓練活動（参加したもの若しくは組織したもの、又は、その両方） - リスクアセスメント、DPIA、並びに、セキュリティ及びデータ保護監査 - DPOの決定及び推奨（可能な場合）。	DPOとの面談 DPOの契約書 規則及び方針	39.1	1	7	
G.9.3.2	CP	G	A	データ保護及びセキュリティに関する労働者の教育・訓練の義務	A) 申請者は、個人データに永続的又は定期的にアクセスする要員に対し、少なくとも年1回、定期的に教育・訓練するための方針、規則又は手順を整備しなければならない。	申請者は、個人データの取扱いを担当する要員が、個人データ保護規則及びセキュリティ要件について十分な知識及び理解を有することを確保する義務がある。 個人データを取り扱う全ての者に基本的な教育・訓練が提供されるのが望ましく、定期的にデータを取り扱う者には特別な教育・訓練が提供されるのが望ましい。 最初の教育・訓練はデータを取り扱う前に行われるのが望ましく、少なくとも年1回は定期的に繰り返されるのが望ましい。	DPOとの面談 教育・訓練の文書及び証拠		1	1	
G.10				**（該当する場合、）第三国又は国際機関への個人データの移転**							
				目的	評価対象の範囲に含まれる個人データを第三国又は国際機関に移転する場合、当該移転の前に、GDPRにより提供される保護水準が損なわれないよう、適切な保護措置、及び、必要な場合には補完的措置が講じられるのを確保すること。						
				条件	【IF】評価対象の個人データが第三国又は国際機関に移転される場合、【THEN】次のとおりとする。						
欧州経済領域（EEA）に属する国への個人データの移転は、第三国への移転に該当しない。国際機関への個人データの移転は、第三国への移転として考慮及び評価されるべきである。「EEA域外への移転／第三国への移転」という概念は、申請者が評価対象における個人データを同一又は他の第三国に所在する別の主体に移転する場合にも適用される。その場合、当該申請者は「データ輸出者」とみなされる。											
G.10.1				第三国又は国際機関への個人データの国際的な移転に関する一般的義務（データ輸出者）				**44**			
				条件	【IF】評価対象において取扱われる個人データが第三国（又は国際機関）に移転（又はアクセス可能と）される場合、【THEN】次のとおりとする。						
G.10.1.1	CP	S	A	EEA域外への移転の検証	A) 申請者は、ToEの範囲にある全ての個人データの流れ、並びに、第三国及び国際機関への移転を特定した明確なマッピング又は記録を有さなければならない。 【AND】 B) 申請者は、次の事項を考慮して、ToEの範囲にある個人データの移転の根拠を評価及び記録しなければならない。 b.1) 移転される個人データの保護のレベルを低下させない義務 b.2) 【AND】移転されるデータを保護するために講じられている保護措置及び対策 【AND】 C) 【IF】申請者が処理者である場合、【THEN】移転が管理者の書面による指示に基づいてのみ行われることを確保するための規則又は手順が整備されなければならない。 【AND】 D) 【IF】申請者がEEA域内に所在する場合、【THEN】次の措置の規則、方針又は手順が整備されなければならない。 d.1)	申請者は、第三国又は国際機関への個人データの移転を承認する前に、当該移転の遵守状況を評価及び確認するための規則、手順又は仕組みを整備するのが望ましい。 第三国の取扱い又は国際機関による取扱いのために個人データが移転される場合、申請者は、次の書面による記録を保持するのが望ましい。 - 第三国若しくは国際機関又はその両方で実施される全てのデータ取扱い - 当該移転の遵守状況の評価 - 当該移転によってデータ保護のレベルが低下するリスク、若しくは、データ主体の自由及び権利に影響を与えるリスク、又は、その両方の評価 - 移転データを保護するために講じられた保護措置、技術的及び組織的措置 第三国への移転を含む評価対象に対する認証の適用可能性は、補完的要件の対象となる場合がある。 当該移転は、適法性の根拠（GDPR第6条）及び国際データ移転のための十分な仕組みの使用（GDPR第46条）の両方を遵守していることが期待される。申請者は、当該両方の要件の遵守を文書化するのが望ましい。 第三国への個人データ移転に際して適用される保護措置に関する適切な文書は、認証機関及びEEA域内のデータ保護機関が利用できるように保持されるのが望ましい。	データフローのマッピング 文書評価 手順、仕組み又は方針 労働者との面談	*44, 46, 48, 49*	1	7	
G.10.1.2	CP	S	A	EEA域外への移転メカニズム	【IF】評価対象において取り扱われるいずれかのデータが第三国又は国際機関に移転される場合、【THEN】次のとおりとする。 A) データが移転される第三国は、十分性認定の恩恵を受けていなければならない。 【OR】 B) 十分性認定が存在しない場合、当該第三国への移転は適切な保護措置に基づき、かつ、補完的基準G.10.1.3、G.10.1.4及びG.10.1.5を遵守しなければならない。 【OR】	第三国に対してデータアクセスを提供することは、当該第三国への移転と同等であることに留意する必要がある。GDPRは、十分性認定が欧州委員会によって採択及び監視されることを要求する（第45条GDPR）。十分性認定の一覧は、欧州委員会のウェブサイトで最新の状態に保たれて公開されている。	文書レビュー DPOとの面談 十分性認定	*44*	1	3	
G.10.1.3	CP	S	A	適切な保護措置に基づくEEA域外への移転	【IF】個人データが適切な保護措置に基づき第三国（又は国際機関）に移転される場合、【THEN】次のとおりとする。 A) 当該データを受領する第三国の管理者又は処理者は、次の措置を講じるための手順、規則又は仕組みを整備しなければならない。 a.1) 評価対象に係るデータの取扱い若しくは記録保存又はその両方を行うインフラストラクチャのセキュリティについて、少なくとも年1回監査すること a.2) 【AND】データ主体がその権利を行使し、第三国に所在する管理者又は処理者から効果的な法的救済を受けることを可能にすること 【AND】 B)	データ管理者は、個人データを移転する前に、第三国又は国際機関（該当する場合）において講じられる保護措置の十分性及び効果を評価するのが望ましい。監査は、より広範なセキュリティ監査の一部となり得、かつ、ISO/IEC 27001（ISMSに関するISO/IEC 27001の適用範囲は、当該データ取扱活が含まれるのが望ましい）又は同等の認められた手法に準拠するのが望ましい。本監査報告書は、DPOによってレビューされ、第三国のデータ輸入者によって取り扱われる個人データに関して十分なセキュリティ水準を示すものとして考慮されることが期待される。 要件Aは、基準G.4.1.1、G.4.1.2、G.5.1.1、G.5.1.5、G.6.2.4、G.6.2.7に関連し、補完するものである。要件Bは、基準G.3.1.1、G.3.1.2、G.3.1.3、G.3.1.4、G.3.1.6、G.3.3.1、G.3.3.2に関連し、補完するものである。要件Cは、基準G.3.1.1、G.3.1.2、G.3.1.3、G.3.1.4、G.3.1.5、G.3.1.6、G.3.1.7、G.3.1.8、G.3.2.1、G.3.2.2、G.3.3.1、G.3.3.2、G.3.3.3、G.3.4.1、G.3.4.2、G.3.4.3、G.3.5.1、G.3.6.1、G.3.6.2、G.3.6.3、G.3.7.1、G.3.8.1、G.3.8.2、G.3.9.1、G.3.10.1、G.3.10.2、G.3.11.1、G.3.11.3に関連し、補完するものである。	文書レビュー 手順、規則及び方針 サプライチェーン契約及びSLAのレビュー DPOとの面談 調査	*46*	1	3	
G.10.1.4	CP	S	A	適切な保護措置のための認められたメカニズムの利用	【IF】評価対象において取り扱われるいずれかのデータが、適切な保護措置に基づいて第三国又は国際機関に移転される場合、【THEN】申請者は、当該データ移転が少なくとも次のいずれかのメカニズムの恩恵を受けることを証明しなければならない。	本基準は、適切な保護措置に基づいて個人データを移転する際に、少なくとも1つの適切な保護措置を提供するよう認められた手段が使用されるのを確保することを目的としている。 適切な保護措置とは、次を意味する。 - 管理者及び処理者が、第三国において執行可能な拘束力がある約束を整備していること - 当該拘束力があり執行可能な約束が、取扱業務における適切な保護措置の適用を確保すること - 当該拘束力があり執行可能な約束に含まれる適切な保護措置が、全てのデータ主体の権利にも適用されること - 第三国における国内法及び法制度の状況の影響が考慮されていること	DPOとの面談 提供された保護措置に関する文書	46.1. 46.2	1		
				公的機関	A) データ移転は、**公的機関又は公的組織間における法的拘束力があり執行可能な法律文書**によって提供される十分な		法的拘束力のある法律文書	46.2.a		1	
				拘束的企業準則	【OR】 B) データ移転には、次の要件を充足する**拘束的企業準則**による十分な保護措置が提供されていること b.1) EEAのデータ保護機関によって承認されていること b.2) 【AND】署名されており、かつ、拘束的企業準則に基づき評価対象において取り扱われる個人データを受領する全てのエンティティに適用されること b.3) 【AND】輸出エンティティと輸入エンティティが拘束的企業準則を保有する同一グループに属していること b.4) 【AND】拘束的企業準則によって要求されるデータ保護監査の結果が申請者のDPOと共有されること	拘束的企業準則は、所轄監督機関によって承認されていなければならない。当該準則は法的拘束力があり、データ主体に対して執行可能な権利を付与するものでなければならない。BCRは、これを保持するグループのエンティティが同一グループの他のエンティティに対して行う移転にのみ使用できる。	拘束的企業準則 所轄データ保護機関とのやりとり	46.2.b, 47		4	
				標準データ保護条項（標準契約条項）	【OR】 C) データ移転は、次の要件を充足する、データ輸入者と輸出者が共同で署名した標準データ保護条項によって提供される十分な保護措置を有すること c.1) 標準データ保護条項は、欧州委員会によって承認され、公表されていること c.2) 【AND】両当事者は標準データ保護条項の附属書を記入していること c.3) 【AND】両当事者は標準データ保護条項に署名していること c.4) 【AND】両当事者はそれぞれの連絡先及び役割（誰がデータ輸出者及びデータ輸入者として行動するか）に関する情報を提供していること	GDPR第46条に定める標準データ保護条項は、通常、標準契約条項（SCC）と呼ばれる。 GDPRは、標準契約条項が（GDPR第93条第2項に従い）欧州委員会によって採択されること、又は、所轄データ保護機関によって採択され、かつ、欧州委員会によって承認されることを要求する。 データ輸入者及びデータ輸出者は、SCCを遵守する法的拘束力のある契約を締結する際に、SCCの附属書に記入し、その不可分の一部を構成する附属書に署名しなければならない。さらに、当事者は、本条項に基づく連絡先及び各当事者の役割（誰がデータの輸出者で、誰がデータの輸入者であるか）に関する情報を提供しなければならない。 また、SCCに依拠し、透明性を確保するため、当該条項は、全当事者によって署名され、拘束力を有し、選択された法域の民事法上の要件に従って契約に組み込まれなければならない。	契約書 標準データ保護条項の公表	46.2.c,46.2.d		5	

				承認された行動規範	【OR】 D) データの移転は、次に適用される、（GDPR第40条及び第46条に基づく）承認された**行動規範**によって提供される十分な保護措置を有すること d.1) 申請者	GDPRは、行動規範がGDPR第40条に従い、EEA域内のデータ保護機関によって正式に確認されていることを要求する。行動規範は、GDPR第46条に基づく移転ツールとして採用される。規則2016/679に基づく行動規範及び監視機関に関するEDPBガイドライン1/2019を参照することが推奨される。申請者は、拘束力があり執行可能な約束を持整備するのが望ましい。	行動規範	46.2.e, 40			
				認証	【OR】 E) データ移転は、次の条件を充足する場合、（GDPR第42条及び第46条に基づく）**承認された認証**方法によって提供される十分な保護措置を有すること e.1) 認証書は有効であり、かつ、所管国内機関によって認定された認証機関によって発行されていること e.2) 【AND】認証書は、実施される個人データの移転を対象としていること	GDPRは、認証方法がGDPR第42条に基づき正式に承認されていることを要求する。当該承認された認証制度の一覧は、EDPBによって公表されている。 移転ツールとして使用される認証方法は、GDPR第46条に基づいて承認されるのが望ましい。 データ輸入者は、認証を補完し、その中に含まれる適切な保護措置（データ主体の権利に関するものを含む）を適用することを目的として、契約上拘束力があり執行可能な約束に署名することが期待される。 移転ツールとしての認証に関するEDPBガイドライン07/2022を参照することが推奨される。	認証文書及び参照	46.2.f, 42, 43	2		
				所轄データ保護機関からの承認	【OR】 F) データ移転は、管理者又は処理者と、第三国又は国際機関の管理者、処理者又は個人データの取得者との間の承認済みの契約条項に基づき、**データ輸出者のEEAデータ保護機関によって承認**されること		所轄データ保護機関による承認	46.3	2		
					【OR】 G) データ移転は、公的機関又は公的組織の間の取決め（当該取決めは、執行可能かつ効果的にデータ主体の権利を確保するため、データ保護機関によって承認された条項を含なければならない）に基づき、データ輸出者のEEAデータ保護機関によって承認されること		所轄データ保護機関による承認	46.3	1		
G.10.1.5	CP	S	A	移転影響評価	【IF】評価対象において取り扱われる個人データが、十分性認定の適用なく、第三国又は国際機関に移転される場合、【THEN】次のとおりとする。 A) 申請者は、次の事項を評価するために移転影響評価を実施しなければならない。 a.1) 第三国の公的機関によるアクセス及び取扱いが明確、正確かつアクセス可能な規則に基づいているか a.2) 【AND】データ取扱いの必要性及び比例性の原則を尊重及び遵守するための仕組みが整備されているか a.3) 【AND】第三国（若しくは国際機関又はその両方）の機関が監視の仕組みを確立しているか a.4) 【AND】データ主体に対して効果的な救済手段が提供されているか a.5) 【AND】移転ツールによって講じられた保護措置が効果的に実施されているか a.6) 【AND】移転によって移転データの保護レベルが低下しないか 【AND】 B) 申請者は、次の措置を講じなければならない。 b.1) 移転データの保護のレベルが低下しないのを確保するため、特定された懸念に対処するための補完的措置を採用すること b.2) 【AND】移転影響評価を定期的に再評価するための効果的な手順又は措置を整備すること 【AND】 C) 【IF】申請者がデータ管理者の代わりに行動するデータ処理者である場合、【THEN】移転影響評価はデータ管理者の指示に従って実施され、かつ、当該データ管理者に共有されなければならない。	申請者は、関与する第三国の関連する法制度及び慣行がEDPBの欧州の本質的保証を遵守しているかを確認するのが望ましい。 1 - 第三国の機関によるアクセス及び取扱いは、明確、正確かつアクセス可能な規則に基づいている。 2 - データ取扱いの必要性及び比例性の原則を尊重及び遵守するための仕組みが整備されている。 3 - 各国機関は、監視メカニズムを確立している。 4 - 個人に対して効果的な救済手段が提供されている。 十分性認定が移転の根拠として用いられる場合、全ての必要な保護措置を提供する。 EUの個人データ保護水準の遵守を確保するための移転ツールを補完する措置に関するEDPB勧告01/2020は、本要件の対応方法に関する明確な運用指針を提供している。 1「移転を知る」－データ移転の明確なマッピングを行うこと（基準G.10.1.1参照） 2 「移転ツールを検証する」－それが十分であることを確保すること（基準G.10.1.2、G.10.1.3及びG.10.1.4参照）。 3 「第三国を評価する」－第三国の法令及び慣行を評価し、当該第三国の法令が形式的にはEUのスタンダードを充足している場合であっても、実務上明らかに適用／遵守されていないか否か、及び、当該第三国において関連法令が不足している場合に、移転ツールの約束と適合しない慣行が存在するか否かを判断すること 4 「補完的措置を特定及び採用する」－申請者は、自らの決定が実効的な分析に基づくものであり、強力な暗号化、仮名化、分割／マルチパーティ処理、契約上の通知義務（報告、「令状のカナリア」など）といった十分な補完的措置の特定及び採用に繋がっていることを証明しなければならない。 5「必要な正式な手順的措置を講じる」－推奨事項01/2020に従うこと 6 「保護水準を適切な間隔で再評価する」－申請者は、第三国へのデータ移転に関連するリスクを年次で再評価する内部手続を採用するのが望ましい。当該再評価は、通常のリスクアセスメント方針に統合することができる。 データ輸出者（、及び、処理者が輸出者としてデータを移転する場合には管理者）は、（該当する場合）当該移転に対する補完的措置の特定及び適用に責任を負う。国際データ移転に関連する特定されたリスクに対処するために補完的措置が必要な場合、データ輸入者は当該措置をデータ輸出者と調整することが期待される。データ輸入者及びデータ輸出者の双方が、暗号化、仮名化及び匿名化などの補完的措置を実施するために協力することが	DPOとの面談 リスクアセスメント及び採 用された措置に関する文書	46	1	9		
G.10.1.6	CP	S	A	第三国におけるデータ輸入者の約束	【IF】評価対象において取り扱われるいずれかの個人データが、十分性認定なく、認証方法又は行動規範に基づき第三国又は国際機関に移転される場合、【THEN】次のとおりとする。 A) 申請者は、データ主体の権利に関するものを含む、認証又は行動規範に定められた適切な保護措置を適用するためのデータ輸入者の拘束力があり執行可能な約束を有さなければならない。	GDPR第42条の求めに従い、第三国におけるデータ取得者は、データ主体の権利を含む適切な保護措置を適用するため、契約条項又はその他の法的拘束力のある法律文書に拘束されるのが望ましい。データ輸出者は、かかる約束が整備され、かつ、移転データを十分に保護していることを確保する責任がある。 拘束力がある執行可能な約束については、7/2022の第4節及び欧州委員会の研究の第8. 5節（198～199頁）に一覧化された各種の文書を参照することが推奨される。これらには最低限の要件が存する。当該文書は、関連する裁判所によって有効と認められ、請求の法的根拠を提供するものであることが期待される。一覧化された文書の種類は、1) 二者間契約、2) 多数当事者間契約、3) 一方的契約的約束、4) 条約である。 EUのデータ輸出者に適用される説明責任の原則により、データ移転に対する最終的な責任、特に適切な保護措置の存在に関する責任は、データ輸出者に帰属する。したがって、データ輸出者は、データ取得者に対し、認証に関する証拠の提供及び当該保護措置の適用について約束を求めるのが望ましい。	DPOとの面談 リスクアセスメント及び採 用された措置に関する文書	42	1	1		
G.10.1.7	CP	S	A	特定の状況における例外規定に基づくEEA域外への移転	【IF】個人データが、十分性認定（GDPR第45条）及び適切な移転ツール（GDPR第46条）なく、特定の状況に対する例外として、第三国又は国際機関に移転される場合、【THEN】次のとおりとする。 A) 移転は、同意に基づくものでなければならず、かつ、次の条件を充足しなければならない。 a.1) データ主体は、データ移転が意図されている国又は国際機関について通知されなければならない。 a.2) 【AND】データ主体は、十分性認定及び適切な保護措置が存在しないことによる権利及び自由に対するリスクについて通知されなければならない。 a.3) 【AND】データ主体は、提案された移転に対し、明確かつ有効な同意を与えなければならない。 【OR】 B) データ移転の必要性は、次の目的のために評価及び確立されなければならない。 b.1) データ主体が合意した契約の履行、又は、データ主体の要求に基づく契約締結前の措置の実施 b.2) 【OR】EU法又はEEA加盟国の国内法により認められた公共の利益に関する重要な理由 b.3) 【OR】訴えの提起若しくは攻撃防御 b.4) 【OR】自然人の生命に関する利益の保護 【OR】 C) 移転は、次の要件を充足する公的登録機関から行われるものでなければならない。 c.1) 適用可能なEU法又はEEA加盟国の国内法に従い、公衆に対する情報の提供を目的とすること	特定の状況における例外規定に基づく越境移転は、明確に文書化されるのが望ましい。移転がデータ主体の同意に基づく場合、当該同意は、情報に関連するリスクの情報提供を受けた後に、データ主体によって明確かつ明示的に与えられたものであるのが望ましい。「特定の状況における例外規定」の定義及び適用範囲は、本規則において明記されている。要件c.2)は、協議の法的条件を充足する限りにおいて適用される。 「適切な移転ツール」とは、適切な保護措置を意味する（G.10.1.4参照）。 有効な同意は、データ主体がG.3.2.1及びG.3.3.1の基準に従って適切に情報提供を受けた上で、G.1.2.1、G.2.1.2及びG.2.1.3の基準を遵守することを要する。 適法性への言及は、GDPR第V章の規定を指し、GDPR第6条の意味での適法性を指すものではない。申請者は、GDPR第6条に基づく適法性及びGDPR第V章の両方を遵守するのが望ましい。 例外規定は、GDPR第45条第3項に基づく十分性認定又はGDPR第46条に基づく適切な保護措置が存在しない場合に限り、利用することができる。	文書レビュー 手順、規則及び方針 DPOとの面談 調査	*49*	1	9		
G.10.1.8	CP	S	A	十分性認定に基づく移転	【IF】申請者が十分性認定に基づいて第三国にデータを移転する場合、【THEN】次のとおりとする。 A) 次の措置を実施するための規則、方針又は仕組みが整備されていなければならない。 a.1) 少なくとも年に1回、十分性認定が引き続き有効であることを確認すること a.2) 【AND】十分性認定を失った国へのデータ移転について、移転影響評価が実施され、かつ、移転は継続可能であると結論付けられる未その間、当該データ移転を停止すること	十分性認定がある場合、申請者は、当該認定が引き続き有効であることを確認するのが望ましい。十分性認定が取り消された場合、申請者は、その国への全てのデータ移転を停止し、移転が再開できるかの条件を評価するのが望ましい。	面談 調査 文書レビュー サンプル分析	46	1	2		
									0	0		

ステータスコード	トット	%	意味 / 説明
OK	#REF!	#REF!	適守：要件は**管理**され、適守されているようであり、また、不適守は特定されなかった
OK+	#REF!	#REF!	単なる遵守を超えた優良実務（プラクティス）
Obs	#REF!	#REF!	観察
	#REF!	#REF!	0%
Min NC	#REF!	#REF!	軽微な（重大でない）不適守が特定された
Maj NC	#REF!	#REF!	重大な不適守が特定された。
	#REF!	#REF!	0%
?	#REF!	#REF!	情報不足／不明

NA	#REF!	#REF!	対象となる認証には管理項目は**適用されない**				
	#REF!	#REF!		0%			
合計	#REF!	#REF!		0%			

基準の略語	
C	管理者のみに適用される。
P	処理者のみに適用される。
CP	管理者及び処理者の両方に適用される。
S	評価対象ごとに固有かつ明確である。
G	複数の評価対象に共通する一般的なものである。
A	全てに対する義務的要件。
B	単純なデータ取扱いには必要ないが、高いリスクのデータ取扱いには義務的である。
E	免除。

	Q	CQ	E
G.1	3	4	
G.2	1	3	
G.3	26	4	4
G.4	3	2	
G.5	8	1	1
G.6	13	0	
G.7	5	0	1
G.8	6	0	1
G.9	9	0	
G.10	5	0	1
	0	0	