実践ガイド

移転影響アセスメント

最終版

2025 年 1 月

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

目次

1.序文 3

1.1 背景 3

1.2 TIA の目的 3

1.3 このガイドの目的 4

2.移転影響アセスメントを実施する前に 6

2.1 個人データの移転の有無 6

2.2 TIA 実施の必要性 7

2.3 当事者の資格と TIA 実施の責任 8

2.4 TIA の範囲とオンワード・トランスファーの検討 10

2.5 GDPR の原則に基づく移転の遵守 11

3.TIA のさまざまなステップ 12

3.1 移転先を知る（ステップ 1） 12

3.2 使用する移転ツールを識別する（ステップ 2） 18

3.3 データ移転先の国の法律と慣行、および移転ツールの有効性をアセスメントする（ステップ 3）。 19

3.4 補足措置を特定し、採用する（ステップ 4） 25

3.5 補足措置を実施する（ステップ 5） 30

3.6 適切な間隔で再評価を行う（ステップ 6） 31

1. 序文

1.1 背景

その地位（公的か私的か、営利か非営利か）や規模（多国籍企業か中小企業か、地方行政か中央行政か、職人か自由業か）にかかわらず、非常に多くのデータ管理者やデータ処理者が欧州経済領域（[1]）（EEA）外へのデータ移転の問題に関与している。ネットワークの相互浸透と国境を越えたサービスの発展、特にクラウド・コンピューティング・サービスにより、パーソナルデータ（以下、単に「データ」と呼ぶこともある）の全部または一部が EU 法の対象者ではない第三国で処理さ状況が増加している。こうした状況は、一般データ保護規則（General Data Protection Regulation[2]）（GDPR）に基づく移転の原因となる可能性がある。

GDPR の原則は、データが移転された場合、そのテキストによって与えられる保護と実質的に同等の保護の恩恵を受け続けなければならないというものである。GDPR の前文 101 には、「個人データが連合域内から第三国または国際機関の管理者、処理者、その他の取得者に移転される場合、この規則によって連合域内で確保される自然人の保護レベルが損なわれるべきではない」と記されている。GDPR の第 5 章には、データ移転に関する具体的な規定が含まれている。

欧州連合司法裁判所（CJEU）は、いわゆる「シュレムス 2 号」判決（[3]）において、個人データの処理が EU データ保護法に定められた保護水準に準拠して実施され、今後も継続されることを保証する転出者と転入者の責任（[4]）を強調した。同裁判所によれば、転出者は、転入者が個人データ保護に関する約束を遵守できない場合、または遵守できなくなった場合、個人データの移転を停止し、および／または契約を解除する責任も負う。したがって、個人データの移転のために GDPR 第 46 条に記載された移転手段を利用する転出者は、目的地である第三国の保護レベルおよび補足措置の必要性をアセスメントする義務を負う。**このような評価は「移転影響アセスメント」または「TIA」と呼ばれる。**

1.2 TIA の目的

EEA 域外の第三国へのデータ移転が GDPR 第 46 条に基づくものである場合、データ管理者または処理者のいずれであるかにかかわらず、GDPR の適用を受ける転出者は、転入者の協力を得て、データ移転の前に TIA を実施しなければならない。仕向け国が欧州委員会の十分性認定を受けている場合、転出者はこの義務を負わない。また、GDPR 第 49 条に列挙された適用除外のいずれかに基づいて移転が行われる場合、転出者は TIA を実施する必要はない。

TIA の目的は、**転入者が、**選択した**移転手段に定められた義務を遵守できるかどうかをアセスメントし、文書化する**ことである。この目的のため、転出者は、現地の法令が提供する保護のレベルを評価し、意図する移転の観点から第三国の認可当局の慣行を考慮に入れなければならない。必要な場合、TIA はまた、データ保護において特定された欠点を是正し、EU 法が要求するレベルを確保するために、補足措置が可能かどうかを評価しなければならない。

---

[1]欧州経済領域（EEA）は欧州連合（EU）加盟国、ノルウェー、アイスランド、リヒテンシュタインで構成され、GDPR は EEA 協定に組み込まれることで適用されるようになった。

[2]個人データの処理に関する自然人の保護および当該データの自由な移動に関する 2016 年 4 月 27 日付欧州議会および理事会規則（EU）2016/679 であり、指令 95/46/EC（一般データ保護規則）を廃止するものである。

[3]2020 年 7 月 16 日付欧州連合司法裁判所判決、「シュレムス 2 世」、C-311/18、InfoCuria、https://curia.europa.eu/juris/document/document.jsf?mode=DOC&pageIndex=0&docid=228677&part=1&doclang=EN&text=&dir=&oc c=first&cid=14906588

[4]EDPB の定義によれば、「転出者」とは、処理について GDPR の適用を受ける管理者、共同管理者または処理者であって、当該処理の対象となる個人データを、第三国（欧州経済領域（EEA）外）に所在する「転入者」、管理者、共同管理者または処理者が利用できるように、送信その他の方法により開示する者をいう。第 3 条の適用と GDPR 第 5 章による国際移転に関する規定との相互作用に関するガイドライン 05/2021（PDF、807ko）、EDPB を参照のこと。

1.3 このガイドの目的

欧州データ保護委員会（EDPB）の移転ツールを補足する措置に関する勧告（[5]）に従い、CNIL は転出者向けに TIA の実施を支援するための本ガイドラインを作成した。

本ガイドブックは、**TIA を実施する前の段階、および TIA を実施する際に考慮すべきさまざまな要素を**特定する方法論である。EDPB 勧告に示されたステップに従って**どのように分析を行うかについての**ガイダンスを提供し、関連文書を参照する。本書は、第三国の法律や慣行のアセスメントを構成するものではない。本ガイドラインの使用は必須ではなく、他の要素を考慮し、他の方法論を適用することもできる。

TIA を実施する前のステップ（セクション 2）に関して、本ガイドは以下の規準／要件を中心に構成されている：

i. 個人データの移転の有無

ii. TIA を実施する必要がある

iii. TIA の実施責任

iv. TIA の範囲、特に移転を考慮した範囲

v. GDPR の原則を遵守する

TIA の実施（セクション 3）に関して、本ガイドは、EDPB が推奨する TIA を実施するために従うべき 6 つの異なるステップに従って構成されている

1. 移転を知る
2. 使用した移転ツールを識別する
3. データの移転先国の法律と慣行、および移転有効性を評価する。
4. **補足**措置を識別し、採用する。
5. **補足**実施する
6. 適切な間隔で保護レベルを再評価し、保護レベルに影響を与える可能性のある事態を監視する。

ステップ 1 では、エクスポーターが**移転について説明する**ことができる

ステップ 2 は、TIA を実施するか否かを決定するために**、説明された移転の**枠組みや分析に**使用されるツールを文書化することから**なる。

ステップ 3 では、転出者が**仕向国で施行されている法律と慣行を評価**し、使用した移転ツール（ステップ 2 で文書化）を通じて提供されるセーフガードの有効性を損なう可能性のある要素があるかどうかを特定する。

[5]個人データ保護の EU レベルへの準拠を確保するための移転ツールを補足する措置に関する勧告 01/2020（バージョン 2.0）、EDPB、https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020measures-supplement-transfer_en。

ステップ 4 は、移転（ステップ 1 に記載）および第三国の法律と慣行のアセスメント（ステップ 3）を考慮し、第三国において適切なデータ保護レベルを確保する**既存のセキュリティ対策**（技術的、契約的、組織的）を特定することからなる。これらの措置が満足のいくものでない場合、転出者は、、移転されたデータが第三国において EEA 域内と実質的に同等の保護レベルを享受することを確保するために**実施すべき補完的措置を特定しなければならない**。

ステップ 5 には、ステップ 4 で識別された補足措置と可能な手続きステップを運用するためのモデル**行動**計画が含まれている。

最後に**ステップ 6 では**、転出者による**将来的な**移転の**再アセスメントを**想定している。

移転の説明（ステップ 1）及び移転手段の特定（ステップ 2）により，移転の特性及び感受性が，第三国の法令及び慣行のアセスメントにおいて考慮され，可能な補足措置（ステップ 4）を実施するための移転手段（ステップ 3）の有効性が考慮される。

2. 移転影響アセスメントを実施する前に

TIA を実施する前に、いくつかの要素を検証しなければならない。分析を文書化することを推奨する。

2.1 個人データの移転の有無

何よりも、それを確実にすることが必要だ：

- **当該データは個人データである。**

GDPR の第 4 条 1 項は、個人データを「識別された、または識別できる自然人（「データ対象者」）に関するあらゆる情報」と定義している。識別できる自然人とは、特に、氏名、識別番号、位置情報、オンライン識別子などの識別子、またはその自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに固有の *1* つ以上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できる者を指す。[6]

- **個人データの移転が行われる。**

EDPB はそのガイドライン（[7]）において、加工作業が移転に該当するかどうかを判断するための累積的な規準として、以下の 3 つを挙げている：

1) 管理者、共同管理者または処理者（「転出者」）は、所定の処理について GDPR の適用を受ける。

2) 転出者が、管理者、共同管理者、または処理者のいずれであるかを問わず、当該個人データを他の事業体（「転入者」）に送信またはその他の方法で開示する。

3) 転入者が第三国（非 EEA）に拠点を置いており、第 3 条に従って所定の処理について GDPR の適用を受けるか否かを問わず、または転入者が国際組織である。

EDPB[8]、「個人データの第三国または国際機関への移転」という概念は、法的に異なる 2 つの事業体（それぞれが管理者、共同管理者またはデータ処理者）が関与する個人データの開示にのみ適用される。したがって GDPR 第 5 章は、同一事業体内でのデータの送信や利用可能化には適用されない。つまり、EU 域内の管理者の従業員が、出張中などに第三国から雇用主のデータベースにリモートアクセスすることは、GDPR の意味における移転には当たらない。

逆に、同じグループに属する 2 つの事業体間でデータを送信または利用可能にすることは、移転に該当する可能性がある。[9]

---

[6] [6]例えば、CNIL のウェブサイトにある様々な資料を参照のこと：

- "Personal Data : definition", https://www.cnil.fr/en/personal-data-definition ;
- 「Sheet n°1: 個人データの識別」 https://www.cnil.fr/en/sheet-ndeg1-identify-personal-data

[7]第 3 条の適用と国際移転に関する規定との相互作用に関するガイドライン 05/参照のこと。

V of GDPR (PDF, 807 ko), EDPB, https://www.edpb.europa.eu/system/files/2023-02/edpb_guidelines_052021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_0.pdf

[8]同上、§20。

[9]同上、§21。

EEA 域内に保管されたデータへの第三国からのリモートアクセスや、EEA 域外でのデータのクラウドストレージは、これらの活動が転出者とは法的に異なる事業体によって行われる場合、移転に該当する。

2.2 TIA を実施する必要がある

第三国へのデータ移転が GDPR 第 46 条の手段に基づいて行われる場合、その前に TIA を実施しなければならない。例えば、欧州委員会標準契約条項（[10]）や拘束力のある企業規則（BCR）に基づいて移転されるデータに関するものである□[11]□一方、以下の場合は TIA を実施する必要はない

- **欧州委員会が適切な保護レベルを提供していると認めた国にデータを移転する。**

欧州委員会が適切なレベルの保護を提供すると認めた国（[12]）への個人データの移転は、GDPR 第 5 章に基づくデータ移転ツールまたは補足措置の実施を必要としない。このような国への個人データの移転が行われる場合、当該データの十分な保護レベルが確保される。**この場合、TIA を実施する必要はない**

EDPB が意見書 22/2024 で言及しているように、欧州委員会は、これらの適切な国々について、別の第三国または国際機関へのデータの移転に関する規則、判例法、データ対象者の効果的で強制力のある権利、データ対象者のための効果的な行政および司法の救済手段をすでに考慮している。[13]。

十分性認定決定の対象範囲は限定されていたり（例えば、カナダの十分性認定決定は、商業活 動の過程で個人データを処理する民間団体のみを対象としている[14]、日本の十分性認定 決定は、放送機関、新聞発行者、通信社その他の報道機関、専門的な執筆活動に従事する者、大学、宗教団体、 政治団体[15]）、第三国で認定された特定の事業体のみを対象としていたりする（例えば、米 国の十分性認定決定[16]）。データの移転が十分性認定の範囲に含まれない場合、第 46 条の手段の一つを使用するか、第 49 条の適用除外に依拠する必要がある。前者の場合、TIA を実施する必要がある。

十分性認定は定期的に見直される。したがって、新たな決定が下されたり、リストから削除されたりした場合に備えて、十分性認定の対象となった国のリストを定期的にチェックすることをお勧めする。

- この移転は、第 49 条の適用除外に基づくものである。

TIA が必要となるのは、第 46 条の手段の一つが使用される場合のみである。従って、第 49 条の適用除外のひとつに基づく移転は、同条に定められた適用条件を遵守する以外には、何ら形式的な手続きを踏むことなく実施することができる

---

[10]「標準契約条項（SCC）」、欧州委員会：https://commission.europa.eu/law/law-topic/data-保護/国際次元データ保護/標準契約約款-scc_ja

[11]「拘束力のある企業規則（BCR）」欧州委員会 https://commission.europa.eu/law/law-topic/data-protection/internationaldimension-data-protection/binding-corporate-rules-bcr_en

[12]このような決定の対象となった国の全リストについては、欧州委員会（https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en）の「十分性認定決定」を参照のこと。

[13]「処理者およびサブ処理者への依存から生じる一定の義務に関する意見書 22/2024」、EDPB、§92-93

[14]欧州委員会、欧州議会および理事会指令 95/46/EC に従い、カナダの個人情報保護および電子文書法が提供する個人データの適切な保護レベルを確立する 2001 年 12 月 20 日の決定 2002/2/EC、EUR-Lex、https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002D0002。

[15]欧州委員会、個人情報保護法に基づき日本が提供する個人データの適切な保護に関する欧州議会および理事会規則（EU）2016/679 に基づく 2019 年 1 月 23 日付実施決定 2019/419、第 1 条、EUR-Lex、https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019D0419

[16]European Commission, Implementing Decision (EU) 2023/1795 of 10 July 2023, establishing, in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council, EUR-Lex, https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32023D1795.米国の具体的な事例については、"Adéquation des États-Unis : les premières questions-réponses" [in French], CNIL, https://www.cnil.fr/en/adequation-des-etats-unis-les-premieres-questions-reponses を参照されたい。

EDPB がガイドライン 2/2018 で指摘しているように、「第 49 条に規定されるような適用除外は、実際には "ルール "になってはならず、特定の状況に限定される必要があり、各データ転出者は、移転が厳格な必要性テストを満たすことを確認する必要がある」[17]

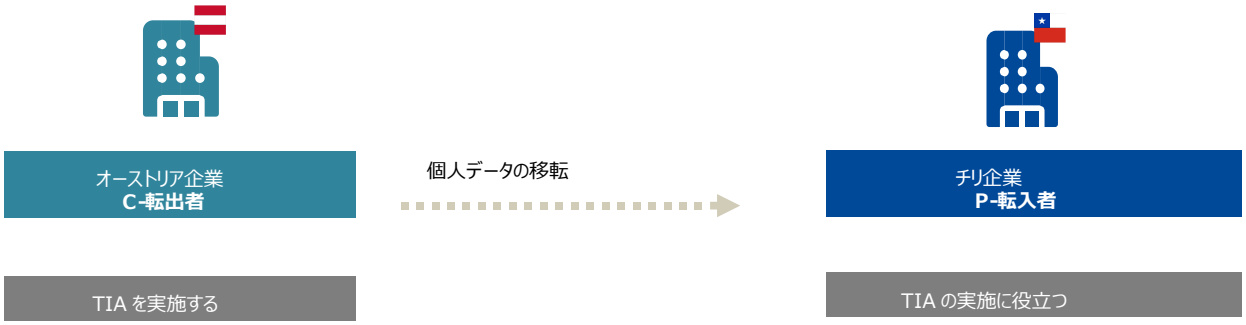
2.3 当事者の資格と TIA 実施の責任

移転に関与する異なる事業体の資格（管理者、共同管理者、処理者）[18] 、責任の配分を決定し、当事者に異なる義務を伴うため、識別しなければならない。EDPB はこれらの概念に特化したガイドライン[19] を作成した。情報は CNIL のウェブサイトでも入手できる。[20]

TIA は、管理者であれ処理者であれ、転入者の協力を得て転出者が実施しなければならない。第三国で移転されるデータが実質的に同等レベルの保護を受けていることを確認し、TIA を実施するのは主に転出者の責任である。とはいえ、転入者はアセスメントに必要な多くの情報にアクセスでき、またアセスメントされた法令に関する知識を有しているため、TIA の実施には転入者の支援が不可欠である。

処理における当事者の役割とその資格によって、いくつかのケースを区別することができる：

ケース 1：EEA 域内の管理者が輸出業者として、第三国の転入者である処理者にデータを移転する：



管理者は、処理者の協力を得て TIA を実施することが求められる。処理関係においては、GDPR 第 28 条(3)(h)に基づき、プロバイダは、自らの義務の遵守を証明するための情報を管理者に提供する必要がある。[21]この情報には、特に公的機関によるデータへのアクセスに関して、データ管理者が現地の法律および慣行の分析を実施することを可能にする、あらゆる関連資料を含めることができる。

当局の法令および実務に関する具体的な証拠としては、第三国の当局による EEA から移転されたデータへのアクセスに関する報告書、データ転入者もしくはその処理者、または同じ活動分野の関係者が過去に受けたアクセス要求に関する報告書、加盟国の実務言語に翻訳

[17]規則 2016/679 に基づく第 49 条の適用除外に関するガイドライン 2/2018 (PDF, 733 ko), p.4, EDPB、https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

[18]管理者（または共同管理者）：単独で、または他者と共同で、個人データの処理の目的と手段を決定する自然人または法人、公的機関、代理店、その他の団体、処理者：管理者に代わって個人データを処理する自然人または法人、公的機関、代理店、その他の団体（GDPR 第 4 条(7)および(8)参照）。

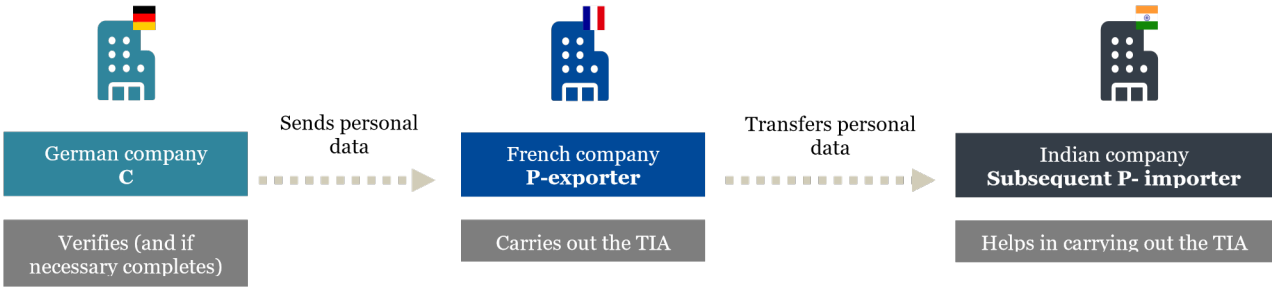
[19]GDPR における管理者と処理者の概念に関するガイドライン 07/2020、EDPB を参照のこと。

[20]例えば、"Responsable de traitement et sous-traitant : 6 bonnes pratiques pour respecter les donées personnelles" [in French]を参照のこと、CNIL

[21]EDPB はガイドライン 07/2020 の中で、「契約には、GDPR 第 28 条に規定された義務の遵守を証明するために関連する処理の詳細について、管理者が十分な情報を得られるように、処理者と管理者の間の情報の流れがどのような頻度で、どのように行われるべきかについての詳細を含めるする。このような情報には、*[…]*データの場所、データの移転、誰がデータにアクセスでき、誰がデータの取得者であるか、使用されるサブ処理者等に関する情報が含まれるべきである

された第三国の法令に関する情報、または EEA 加盟国の国民が不服申立てを行う場合の不服申立ての処理に関する管轄当局の情報などを適宜含めることができる。[22]

ケース 2 - GDPR 対象者に代わり、転出者として行動する GDPR 対象データ処理者が、第三国で転入者として行動するサブ処理者にデータを移転する：



EEA 域外（上図ではインド）へのデータ移転が管理者（上図ではドイツ企業）ではなく、処理者（フランス企業）によって行われる場合、処理者は転出者として行動することになるため、その移転のコンプライアンスを確保し、TIA を実施する責任は処理者にある。

GDPR 第 28 条(3)(h)に従い、処理者（フランスの会社）は管理者に以下を提供する必要がある。

(ドイツ企業)に対し、実行された TIA を含む後者の義務の遵守を証明するための情報を提供する。移転加工業者（フランス企業）が、具体的な証拠を提出することなく、TIA の単純な結論や要旨、または第三国の法規に関するアセスメントを送信しても、その義務を履行することはできないことに留意すべきである。[23]。

さらに、この処理者およびそのサブ処理者（フランス企業およびインド企業）と契約するかどうか、または彼らとの契約関係を維持するかどうかの最終決定は、GDPR 第 28 条 1 項に基づき提供される保護措置を検証する義務を負う管理者（ドイツ企業）が行う。データ対象者の権利と自由に対するリスクが高ければ高いほど、実施されるチェックはより重要でなければならない。[24]これは、処理者から受領した情報（TIA を含む）に依拠し、必要な場合（不完全、不正確または疑問がある場合など）にはそれを補足することによって行うことができる

---

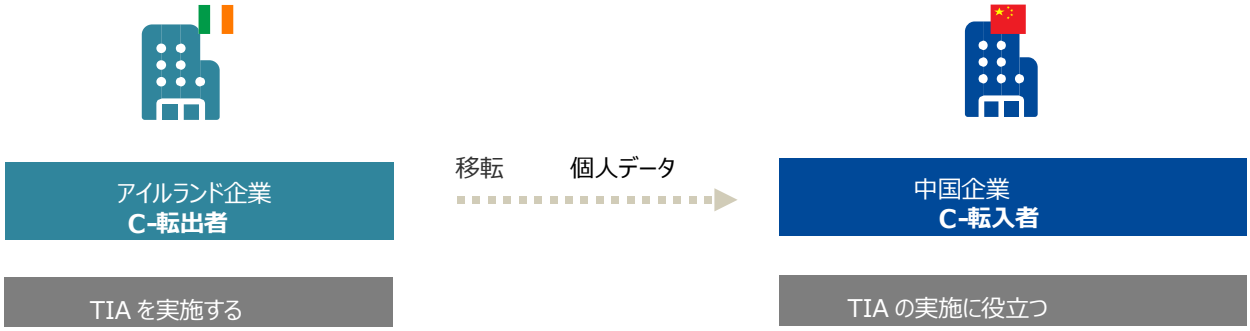
[22]EDPB 勧告 01/2020 の附属書 3「個人データの EU 保護水準への準拠を確保するための移転手段を補完する措置」（§144 の「第三国を評価するための可能な情報源」）、EDPB, https://www.edpb.europa.eu/system/files/2021-/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf に引用されているような信頼できる情報源に依拠することは可能である。

[23]EDPB は、意見書 22/2024 の§96 において、「管理者は、適切な保護措置が講じられているかどうかを評価し、最初の処理者との契約で定められた義務をサブ処理者が遵守することを妨げる可能性のある問題のある法規制について注意を払うべきである」と規定している。具体的には、管理者は、判例に従い、*EDPB* 勧告 *01/2020* で説明されているように、「移転影響アセスメント」を確実に実施すべきである。導入された適切な保護措置、「移転影響アセスメント」、可能な補足措置に関する文書は、（適切な場合には、加工業者／転入者と協力して）加工業者／転出者が作成すべきである。管理者は、（サブ）加工者が作成したアセスメントを信頼し、必要であればそれを基にすることができる。例えば、管理者が受領したアセスメントが不完全、不正確、または疑問があると思われる場 合、管理者は、アセスメントが *EDPB* 勧告 *01/2020* 及びその中で規定されているステップ *98* に沿ったものであることを念頭に置きながら、追加情報を求め、情報を検証し、必要であれば補完／修正すべきである。これには、移転のすべての状況に照らして関連する法律および慣行を特定し 99 、必要であれば適切な補足措置を特定することが含まれる。

[24]EDPB Opinion 22/2024 のエグゼクティブサマリーおよび§60 を参照のこと：*EEA* 域外への個人データの移転が、管理者の指示に従って *2* つの（サブ）処理者間で行われる場合、管理者は、*GDPR* が保証する保護レベルが個人データの移転によって損なわれないようにするための第 *44* 条に基づく義務に加えて、「十分な保証」に関する *GDPR* 第 *28* 条第 *1* 項に由来する義務にも引き続き服する。処理者／転出者は、判例法に従い、また *EDPB* 勧告 *01/2020* で説明されているように、関連文書を準備すべきである。管理者は、当該文書を評価し、管轄 *SA* に提示できるようにしなければならない。管理者は、加工業者／転出者から受領した文書または情報に依拠し、必要に応じてそれを基にすることができる。この文書をアセスメントする管理者の義務の範囲と性質は、移転に使用される根拠と、移転が初回移転にあたるか、またはオンワード移転にあたるかによって異なる。EDPB はまた、「*SA* は、（サブ）処理者が提供する保証の十分性の検証が、管理者が満足するように行われたことを、管理者が証明できるかどうかを評価すべきである」と述べている。管理者は、処理者から受領した情報に依拠し、必要な場合（例えば、不完全、不正確、または疑問があると思われる場合）にはそれを基にすることを選択することができる。より具体的には、データ対象者の権利および自由に対するリスクが高い処理については、管理者は、提供された情報の確認という点で、検証のレベルを高めるべきである。

ケース 3 - GDPR 対象者が転出者として第三国の管理者にデータを移転する場合

転出者として行動する GDPR 対象者と、転入者として行動する第三国に拠点を置く管理者との間のデータ移転の文脈では、第三国で移転されるデータが EEA 域内で保証されるものと本質的に同等の保護レベルを享受できるようにすることは転出者の責任であり、したがって転入者の協力を得て TIA を実施する必要がある。



2.4 TIA の範囲と先への配慮

TIA 実施の最初のステップは、データ移転のマッピングである（本ガイドのステップ 1 を参照）。このマッピングは、転入者と第三国を適切に識別することである。これにより、データ転出者（最終的には、データ移転が自ら行われない場合はデータ管理者）は、実施すべき補足措置を特定することができる（ステップ 4 および 5 を参照）。

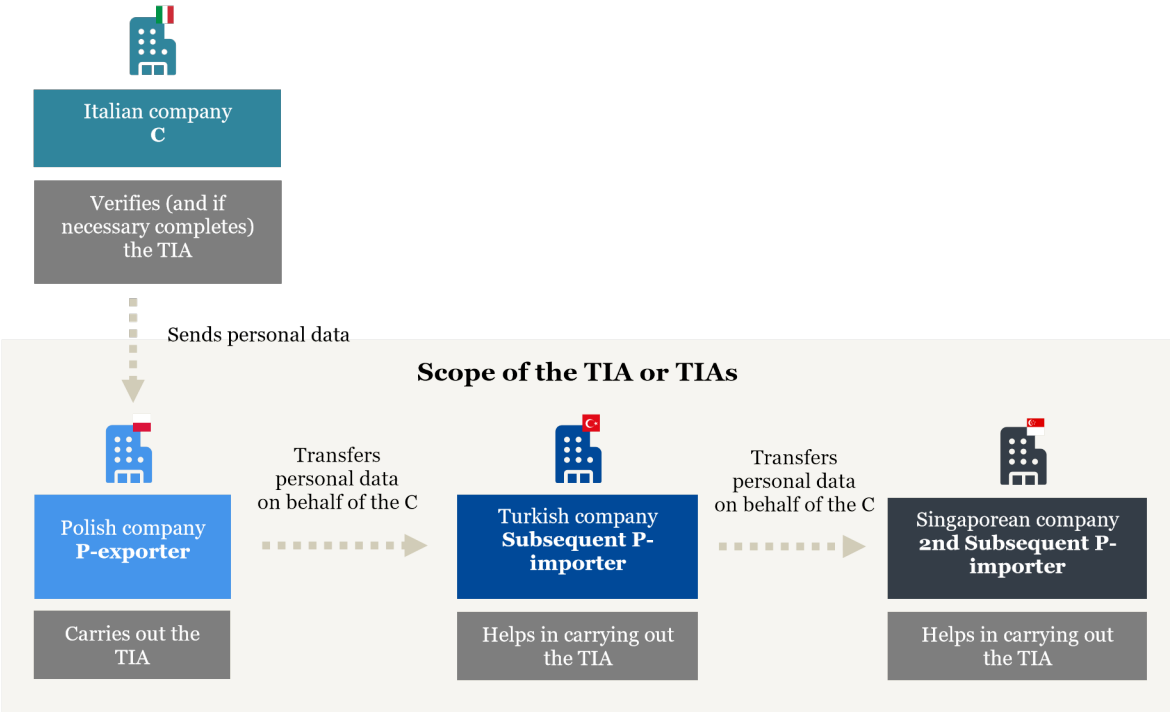
転出者は、（転出者として行動するか否かを問わず）データ管理者が EEA 域外へのすべてのデータ移転に関連するリスクを評価できるように、**前方移転を含むデータフロー全体を分析に考慮しなければならない。**[25]

TIA は、単一の移転または一連の移転に関するものである。従って、転出者は、同一又は複数の文書内で分析を文書化する選択権を有する。移転の連鎖に変更が生じた場合、転出者は既存の分析を修正することも、既に実施した既存の分析にリンクさせた新たな分析を行うこともできる。転出者が加工業者である場合、この情報を管理者と共有しなければならない。

その上、いかなる移転も、転入者が使用する移転ツールに規定された義務を遵守することを条件とする。標準契約条項（SCCs）[26] が締結されている場合、転入者は、第三者が SCCs に拘束されるか、または適切なモジュールの下で SCCs に拘束されることに同意しない限り、個人データを欧州連合域外に所在する第三者に、データ転入者と同じ国または他の非適格な第三国に開示（以下、「オンワード移転」という）しないことを約束する。そうでない場合、データ転入者は、SCCs に規定された条件を満たし（モジュール 1、第 8.7 条および第 8.8 条、モジュール 2 および 3-第 8.8 条）、適合性を証明するために必要な文書を保管する義務を遵守する場合に限り、オンワード移転を行うことができる（モジュール 1 および 3、第 8.9 条、モジュール 2-第 8.8 条）。

[25]意見書 22/2024 の 97 項で、EDPB は「管理者は、そのようなオンワード移転に関する文書を提示できるべきである」と述べている。つまり、管理者は（サブ）加工業者／転出者からこの情報を受け取り、転入者が適切なセーフガード制度に規定されているオンワード移転の要件を実際に遵守していることを示すべきである」と述べている。

[26]欧州委員会発行の標準契約条項 EUR-Lex（https://eurlex.europa.eu/eli/dec_impl/2021/914/oj）を参照のこと。



2.5 原則を遵守した移転

データの移転は、他の処理と同様、GDPR のすべての原則に準拠しなければならない。GDPR 第 5 条によると、管理者は（転出者自身である場合は直接、転出者が処理者である場合は処理者を通じて）、移転が適法であり、GDPR 第 6 条および適用される場合は第 9 条の法的根拠のいずれかに基づいていることを保証しなければならない。また、データは適切かつ関連性があり、処理目的に必要なものに限定されなければならない。したがって、移転されるデータは、移転によって追求される目的にとって厳密に必要なものに限定されることを保証する必要がある。

また、GDPR 第 13 条および第 14 条に従って、データ対象者への情報提供を確実に行うことも必要である。可能であれば、EDPB のガイドラインに従って匿名化プロセスが効果的に識別に使用されるようにしながら、個人データの代わりに匿名化データを開示または送信することが望ましい□[27]□この場合、GDPR は適用されない

[27]匿名化の詳細については、Article 29 Working Party (G29), Opinion 05/2014 on Anonymisation Techniques (PDF, 721 ko), European Commission, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf ; および "L'anonymisation de données personnelles" [available in French], 05/19/2020, CNIL, https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles を参照のこと。

3. TIA のさまざまなステップ

TIA を実施するには、以下の 6 つのステップを踏むことが推奨される：

3.1 移転先を知る（1）

データがどこで処理されるにせよ、移転されるデータと本質的に同等の保護レベルを確保するためには、まず移転について説明する必要がある。移転の記述（ステップ 1）により、データの移転先国の法律と慣行、および移転ツールの有効性（ステップ 3）をアセスメントする際に、可能な補足措置（ステップ 4）を講じることを視野に入れながら、移転の特徴と機微性を考慮することができる。

以下の表を完成させるために、処理活動の記録やデータ移転に関わる契約書など、 既存の内部文書を使用することができる。この情報を転入者に求めることも可能である。

輸出	
転出者名	
連絡先および連絡詳細（移転に関する社内の担当部署または担当者）	
移転国	
データ移転における転出者資格[28]	□ コントローラー □ ジョイントコントローラー □*Processor*」または「*Joint controller*」の場合、コントローラまたは他のジョイントコントローラの名前を指定する
その他有用な情報	

[28]EDPB, Guidelines 07/2020, op.cit.を参照のこと。

転入者	
転入者名	
連絡先および連絡詳細（移転に関する社内の部署または責任者）	
転入国	
データ移転における転入者資格	☐ データ管理者 ☐ ジョイントコントローラー ☐ 処理者 「*Processor*」または**「*Joint controller*」の場合は、**コントローラの名前を指定する
転入者の活動内容[29]	性質を特定する： データの仕向け国の法律によって特に保護されているデータ転入者か。[30]
その他有用な情報	

[29]第三国で適用される法律の特定を容易にする情報。

[30]第三国の転入者は、例えば患者に医療を提供するため、あるいは依頼人に法律サービスを提供するためなど、国内法によって特別に保護される場合がある。EDPB, Recommendations 01/2020 on measures supplementing transfer instruments to ensure compliance with the EU level of protection of personal data（EDPB 勧告 01/2020 個人データ保護の EU レベルへの準拠を確保するための移転手段を補完する措置に関する§91）参照。

移転されたデータに対する転入者の処理活動 (*IT* サポート、マーケティング、クラウドソフトウェアの提供、データホスティングなど）。	
移転の種類 (転入者がデータを利用できるようにする方法）。	□**ダウンロード／保存の可能性がないリモートアクセス** - 個人データは EEA 域内の転出者によって管理される。転入者はデータのコピーをダウンロードすることはできないが、EEA 域外の不十分な国からリモートアクセスすることはできる。 □**ダウンロード／保存の可能性を伴うリモートアクセス** - 個人データは EEA 域内の転出者によって管理される。転入者は第三国からデータにアクセスする可能性があり、必要であればデータのコピーをダウンロードし、不十分な EEA 第三国に保管することもできる。 □**送信およびホスティング/ローカル保管** - 転入者が EEA 非適格国で個人データをホスティングまたは保管する。 □その他
移転方法 (例えば、セキュア・ファイル移転プロトコル（*SFTP*）による送信、電子メールによる送信、アプリケーション・プログラミング・インターフェース（*API*）による接続、リモート・サーバーへの接続、物理的媒体へのデータの保存と送信など）。	
移転されるデータの形式	□　分かりやすく言えば □　暗号化されている □　化されている □　その他 也」の場合は具体的に記入すること：
移転の頻度	□単身赴任 □単発／臨時の移転（再発は指定される）

	☐ 定期的な移転（再発は指定される）
転入者のためのオンワード・トランスファーの可能性 *(上記 2.4 節参照)*	☐ はい ☐ いいえ **はい」の**場合は具体的に記入する
移転される個人データのカテゴリー	☐ 識別データ（具体的に記入すること）： ☐ 連絡先（具体的に） ☐ 家庭生活に関するデータ（具体的に記入すること）： ☐ 労働生活に関するデータ（具体的に記入のこと）： ☐ サービス利用データ（具体的に記入のこと）： ☐ その他（具体的に記入のこと）
移転される個人データの特別カテゴリー（「機微データ」）。	☐ 人種または民族的出身を明らかにするデータ（具体的に記入のこと）： ☐ 政治的意見を明らかにするデータ（具体的に記入のこと）： ☐ 宗教的または哲学的信条を明らかにするデータ（具体的に記入のこと）： ☐ 労働組合への加盟を明らかにするデータ（具体的に記入のこと）： ☐ 自然人を一意に識別するための遺伝子データまたは生体データ（具体的に記入のこと）： ☐ 健康データ（具体的に記入すること） ☐ 自然人の性生活に関するデータ（具体的に記入のこと）：

	☐　上記のカテゴリーに該当しない
その他の高度な個人データの移転	☐　前科、犯罪に関するデータ[31]（具体的に記入のこと）： ☐　国民識別番号[32]（具体的に記入のこと）： ☐　ジオロケーションデータ[33]（具体的に記入のこと）： ☐　不正支払いに使用される可能性のある財務データ[34]（具体的に記入のこと）： ☐　その他（具体的に記入のこと） ☐　上記のカテゴリーに該当しない
データ対象者のカテゴリー	
データ対象者のうち脆弱性のある者 （例：未成年者、被扶養者）	☐　はい ☐ いいえ はい」の場合は具体的に記入すること：
[35]（該当する場合）譲渡の性質（全部または一部	☐　合計 ☐　部分的

[31]GDPR 第 10 条

[32]GDPR 第 87 条

[33]Article 29 Working Party (G29), Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for purposes of Regulation 2016/679, p.11, European Commission, https://ec.europa.eu/newsroom/article29/items/611236 を参照のこと。

[34]同上。

[35]移転されたデータは、処理されたデータの全部または一部のみを代表する。

	部分的」の場合は、（可能であれば）パーセンテージを指定する：
移転データ量（可能な場合）	
データ対象者の数（可能な場合）	
移転開始予定日（可能な場合）	
想定される移転の終了日または期間（可能であれば）	

3.2 使用する移転ツールを識別する（ステップ 2）

使用する移転ツールを特定することで、移転の説明は完了する（ステップ 1）。その有効性をアセスメントする必要がある（ステップ 3）。

第 46 条の移転ツール	
第 46 条 移転の枠組みとして使用される移転ツール	☐ 標準契約条項（SCC）[36]（以前はモジュールが指定されていた）： ☐ 拘束力のある会社規則（BCR）「コントローラー[37] ☐ 拘束力のある企業規則（BCR）「処理者[38] ☐ 行動規範 [39] ☐ 認証メカニズム[40] ☐ その場限りの契約条項
移転ツールの証拠と文書がある (例：データ転入者と締結した契約書、データ転入者の証明書、データ転入者を含む BCR の一部を構成する事業体のリストが記載された BCR のコピー）。	

移転が GDPR 第 46 条の移転手段の一つに基づいている場合、TIA を実施する必要があり、ステップ 3 に進むことが適切である。

TIA を実施する必要がない場合（2.2 項参照）、TIA を実施しない決定を 文書化することを推奨する。

[36]欧州委員会が公表している標準契約条項を参照のこと。SCC に関する FAQ の中で、欧州委員会は、GDPR の対象となる転入者への移転に特化した SCC の追加セットを開発中であると述べている。この新しいゲームが採用されれば、GDPR の対象となる転入者への移転の枠組みとして使用することが可能になる。FAQ の §25 を参照のこと。"新標準契約条項-Q&A 概要"、欧州委員会、https://commission.europa.eu/law/law-topic/data-protection/international-dimensiondata-protection/new-standard-contractual-clauses-questions-and-answers-overview_en

[37]BCR-コントローラーについては、承認申請に関する勧告 1/2022、およびコントローラー拘束力のある企業規則（GDPR 第 47 条）に見られる要素と原則に関する勧告 1/2022、EDPB を参照のこと。

[38]BCR-下請け業者については、G29「処理業者拘束力のある企業規則書式（wp265）の承認に関する勧告」（欧州）を参照のこと。

委員会、

および処理者に関する拘束力のある企業規則に関する作業文書（wp257rev.01）、欧州委員会、

[39]移転のツールとしての行動規範に関するガイドライン 04/2021、EDPB を参照のこと。

[40]移転のツールとしての認証に関するガイドライン 07/2022、EDPB を参照のこと。

3.3　データ移転先の国の法律と慣行、および移転ツールの有効性をアセスメントする（ステップ 3）。

移転と使用される手段の明確なビジョンが得られたら、第 3 段階は、使用される手段の保証の有効性を損なう可能性がある、または転出者または転入者が義務を履行することを妨げる可能性がある要素が転入第三国の法律または慣行にあるかどうかを判断することである。移転の説明（ステップ 1）により、データの仕向け国の法律や慣行、移転ツールの有効性（ステップ 3）をアセスメントする際に、その特徴や機密性を考慮することができる。

この作業には転入者の協力が不可欠である。輸出業者は、特に当局によるデータへのアクセスに関して、自国の法律の分析を提供するよう求めるか、少なくとも適用法のリストを提供する必要がある。したがって、TIA の実施に転入者を関与させることが重要である。転入者は転出者および管理者（転出者が処理業者の場合）の指示に従わなければならないからである。

このステップを完了させるために、EDPB 勧告の附属書 3 を参照することが推奨される。附属書 3 には、移転ツールを補足する措置について、使用可能な情報源が非網羅的に列挙されている。これらの情報源は、関連性があり、客観的で、信頼性があり、検証可能であり、一般に入手可能であるか、その他の方法でアクセス可能でなければならない

第三国におけるデータ保護の枠組み（データ保護法およびデータ保護当局の存在）に関する情報が掲載されている CNIL の「Data protection around the world」のページを参照することができる。

公的機関によるデータアクセス法制の分析については、国際機関の報告書や、EDPB が特定の国について委託した分析などの専門家による分析に頼ることもできる。これらの分析は必要に応じて完成させ、更新する必要がある。

DPO のネットワーク、専門家連盟、企業や行政のグループを通じて分析を共有することが推奨される。

データ保護法		
転入者に適用されるデータ保護の枠組みは何か？	参考文献	
その範囲はどうなっているのか？	☐　枠組み ☐　分野別アプリケーション	セクター別に申請する場合は、具体的に記入すること：
第三国の国際データ保護条約への加盟	☐ ☐　いいえ	はい」の場合は具体的に記入すること：
第三国に管轄データ保護当局（または同等の権限を持つ行政団体）があるか。	☐ ☐　いいえ	行政機関の名称
これは 権威・事業体なのか？	☐	正当化する：

データ保護法		
[41]	☐ いいえ	
データ対象者の権利とは何か？	**データ対象者の権利**	
	アクセス権 ☐ はい ☐ いいえ	もしそうなら、参考にしてほしい：
	修正権 ☐ はい ☐ いいえ	もしそうなら、参考にしてほしい：
	削除権 ☐ はい ☐ いいえ	もしそうなら、参考にしてほしい：
	特定の状況における処理に反対する権利 ☐ はい ☐ いいえ	もしそうなら、参考にしてほしい：

[41] 認可機関が独立しているかどうかを判断するには、GDPR 第 52 条から第 54 条、欧州評議会条約第 108+号第 15 条（https://www.coe.int/en/web/data-protection/convention108-and-protocol）、世界プライバシー総会（WPA）の活動を参考にすることができる：

- 手続規則第 5.1 条（PDF、224 ko）、GPA、https://globalprivacyassembly.org/wp-content/uploads/2020
- 認可原則の原則 B.2（PDF、189 ko）、GPA、http://globalprivacyassembly.org/wpcontent/uploads/2015/02/Resolution-on-Accreditation-Features-of-Data-Protection-Authorities.pdf ; および
- 会議の将来に関する作業部会の文書「自治と独立の規準の解釈」、GPA、https://globalprivacyassembly.org/wp-content/uploads/2019/12/ICDPPC-Background-document-onindependence-criteria_post-Coe-comment.pdf。

また、経済協力開発機構（OECD）のより一般的な活動を基礎とすることも可能である：

- 独立した規制当局であること』https://www.oecd.org/en/publications/being-an-independent-regulator_978926425540
- The Governance of Regulators, https://www.oecd.org/en/publications/the-governance-of-regulators_24151440.html ;
- 自立の文化を創造する』https://www.oecd.org/en/p

データ保護法		
	自動意思決定に反対する権利 ☐ はい ☐ いいえ	もしそうなら、参考にしてほしい：
	その他の権利 ☐ はい ☐ いいえ	はい」の場合は具体的に記入すること：
	これらの権利に対する法的制限は、民主主義社会において必要かつ適切なものだろうか？	はい」の場合は具体的に記入すること：
	☐ はい ☐ いいえ	
救済と制裁	効果的な法的救済措置はあるか？ ☐ ☐ いいえ	正当化する：
	効果的で思いとどまらせる制裁措置はあるのか？ ☐ ☐ いいえ	正当化する：
	これらの権利と救済措置は、EEA 内のデータ対象者が行使できるか？ ☐ ☐ いいえ	正当化する：

アクセスを許可する法律および/または慣行	
	はい」の場合、リストアップする

	参考文献	説明（範囲、関係公的機関、義務の性質など）
転入者に適用される監督法の中に、移転された個人データを開示する義務や、公的機関に対し当該データへのアクセスを許可する義務を定めたものがあるか[42] ☐ はい ☐		
転入者に適用される慣行で、移転された個人データを開示する義務、または公的機関に当該データへのアクセス を許可する義務を伴うものがあるか。[43] ☐ はい ☐		

必須保証 [44]	
上記で識別されたデータへのアクセスは、明確かつ正確でアクセス可能なルールによってガバナンスされているか。 ☐ ☐ いいえ	正当化する
データへのアクセスは、GDPR 第 23 条 1 項に列挙された目的の一つを保護するために、民主主義社会において必要かつ比例するのか[45] ☐ ☐ いいえ	正当化する

[42]これらの法律は、一般的な適用法であったり、刑法の適用や国家安全保障の保護に関するものであったりする。政府機関、規制当局、税務当局、警察、情報機関などの認可が関係することもある。

[43]同上

[44]監督上の措置に関する欧州の必須セーフガードに関する EDPB 勧告 02/2020 を参照のこと

[45]これらの目的は以下の通りである：(a) 国家安全保障、(b) 国防、(c) 公共安全保障、(d) 公共安全保障に対する脅威の保護および防止を含む、刑事犯罪の予防、捜査、検知もしくは防御、または刑事罰の執行、(e) その他、連邦または加盟国の一般的な公共の利益、特に、通貨、予算および財政の分野、公衆衛生および社会保障を含む、連邦または加盟国の重要な経済的または財政的利益に関する重要な目的；(h) (a)から(e)および(g)に掲げる場合において、公的権限の行使に関連する監視、検査または規制の任務。

データへのアクセスは独立した監視機構によって管理されているか？ ☐ ☐ いいえ	正当化する：
当該認可当局は、透明性と定期的な監視義務を負っているか？ ☐ ☐ いいえ	正当化する：
データ対象者は、独立した公平な機関において一般的（非国籍）かつ効果的な救済を受けられるか。 ☐ ☐ いいえ	正当化する

支配		
移転されたデータによって影響を受けるデータ対象者が、個人データへの違法なアクセスに対す る救済を求める能力に影響する法治上の問題はあるか？ ☐　はい ☐	はい」の場合、リストアップする	
	問題	データ対象者の権利行使にどのように影響するか

リクエスト

転入者は、（少なくとも近年において）EEA 国民の個人データへのアクセス要請を受けていないか、または第三国当局による直接アクセスの対象者になっていないことを証明できるか。 ☐ はい ☐ いいえ	**「はい」の**場合、どのようにそれを証明できるかをここに明記すること。[46] **そうでない場合は**、受領した申請書の種類、処理された量と方法、および／または将来その対象となる可能性があると考える理由をここに明記すること：
特に、特定された法律又は問題は、移転されるデータ及び転入者に実際には適用されないため、転入者が第三 国の当局による情報入手又は直接入手の要請の対象者になると信じる理由がないことを証明できるか（その活動 分野及び第三国の当局による情報入手の要請の履歴を考慮に入れて[47] ☐ はい ☐ いいえ この場合、補足措置を実施せずに移転を進めることを決定することも可能である	**「はい」の**場合、どのようにそれを証明できるかをここに明記すること。[48]

結論
☐移転ツールは、現地の法律や慣行のアセスメントに照らして有効であり、補足措置なしに移転を実施することが可能である(1)。 ☐現地の法律や慣行のアセスメントに照らすと、移転ツールは効果的ではなく、補足措置を講じる必要がある(2)。 ☐実施された評価に照らすと、移転ツールは有効ではないが、問題のある法律が実際に適用されると信じる理由はなく、補足措置を実施せずに移転を進めることを決定する(3)。 正当化する：

[46]例えば、当局による転出者または他の転出者のデータへのアクセス要求に関する透明性報告書などである。

[47]実施されたアセスメントに照らして移転ツールが有効でない場合であっても、移転されたデー タ及び／又は転入者に問題のある法律が実際に適用されると信じるに足る理由がない場合には、追 加措置を実施せずに移転の続行を決定することも可能である。その場合、転入者と協力し、同じ分野および／または類似の移転された個人データに関連する分野で活動する他の業者の経験や他の情報源も考慮に入れながら、必要に応じてこのアセスメントを実証し、文書化することが必要である。EDPB, Guidelines 01/2020, §43.3 を参照のこと。

[48]例えば、同じ部門および／または関連部門で活動する他のアクターが出版した資料などを通じて。

実施されたアセスメントに照らして、移転ツールが**有効である**(1)、またはツールの効果がないにもかかわらず、補足措置を講じることなく移転を実施することが可能である(3)という結論に達した場合、ステップ 6 に進む。

実施されたアセスメント（2）に照らして、移転ツールが効果的でないという結論に至った場合は、補足措置を特定するためにステップ 4 に進む。

3.4 補足措置を特定し、採用する（ステップ 4）。

ある第三国への移転のために、どのような補足措置が効果的かをケースバイケースで特定する必要がある。ステップ 1 における移転の説明により、特にその特性と機微性が、実施すべき補完措置のアセスメントに考慮される。データ対象者の権利と自由に対するリスクが高ければ高いほど、実施されるチェックと実施される補足措置は大きくなる。[49]

これらの措置は、EEA における個人データ保護レベルの遵守を確保するために使用される移転手段を補足するものであるため、「補足的」と呼ばれる。したがって、以下の表では、すでに実施されている措置（もしあれば）と新たに識別された措置の両方を識別する必要がある。

移転ツールを補完する措置に関する EDPB 勧告の附属書 2 には、ユースケースとして実施可能な技術的、契約的、組織的措置の非網羅的リストが示されている。また、EDPB が有効な措置を特定できないユースケースも紹介している。[50]

複数の補完的措置を組み合わせる必要がある場合もある。ほとんどの場合、契約上および組織上の措置だけでは、第三国当局によるデータへのアクセスの可能性を防ぐには不十分であり、適切に実施された技術的措置によって補完する必要がある。[51]

補足措置の有効性は、ステップ 1 で説明した転入者や第三国によって異なるため、ステップ 3 で詳細な分析を行うことが重要である。**場合によっては、当該移転について欧州法と本質的に同等の保護レベルを確保するための補完的措置がないという結論になり、当該データの移転が放棄されることになる。**

補足措置を特定するこのプロセスは、転入者との協力のもと、十分な注意を払って実施されるべきであり、文書化されるべきである。最高情報システム責任者の関与は不可欠である。相談した個人または事業体（DPO、法的・技術的助言、情報システム責任者、データ保護当局など）の意見または分析を TIA に添付することが推奨される。

すでに実施されている補足措置	
説明	**施策のインパクト**
(各対策について、その説明、転入者または輸出業者が実施しているかどうか、EDPB 勧告にどの程度準拠しているかを記入すること)	(各施策について、緩和された／緩和されたリスクを明記する。

[49]EDPB はその意見 22/2024 の中で、「データ対象者の権利と自由に対するリスクが高い処理については、プロバイダは提供された情報の検証レベルを高めるべきである」と述べている。さらに、具体的な移転に関しては、次のように述べている：(サブ)処理者が、データ対象者の権利と自由に対するリスクに関係なく、管理者が決定した適切な措置を実施するための "十分な保証 "があるかどうかを検証する管理者の義務は、適用されるべきである。ただし、このような検証の程度は、技術的および組織的措置の性質によって異なり、そのようなリスクのレベルに応じて、より厳格になることもあれば、より広範になることもある」。EDPB, Opinion 22/2024 on certain obligations following from the reliance on processor(s) and sub-processor(s), Executive Summary, §60 and 83 を参照のこと。

[50]EDPB 勧告 01/2020、ユースケース 6 および 7、§93-97 を参照のこと。

[51]契約上及び認可上の措置だけでは、一般的に、問題のある法律及び／又は慣行に基づく第三 国の公的機関による個人データへのアクセスを克服することはできない。実際、適切に実施された技術的措置のみが、第三国の公的機関による個人データへのアクセス、特に監視目的でのアクセスを妨げたり、実効性を失わせたりする状況も存在するであろう。

すでに実施されている補足措置			
技術的対策 (技術的措置が有効であるためには、脚注に記載されているすべての管理ポイントを検証すること)	□仮名化 [52] □暗号化 [53] □その他（具体的に記入のこと）		

[52]EDPB、勧告 01/2020、ユースケース 2、§85 を参照のこと：

1. データ転出者が、個人データを特定のデータ対象者に帰属させることができなくなるような 方法で処理された個人データを移転する場合、または追加情報を使用することなく、より大規 模なグループの中からデータ対象者を特定するために使用することができなくなるような 方法で処理された個人データを移転する場合、

2. 追加情報がデータ転出者によってのみ保持され、加盟国または第三国において、*EEA* 内または *EEA* 内で保証される保護と実質的に同等のレベルの保護を提供する管轄区域のもとで、転出者が信頼する事業体によって個別に保管されること、

3. その追加情報の開示または無許可の使用が適切な技術的および組織的セーフガードによって防止され、データ転出者がその追加情報を使用して再識別を可能にするアルゴリズムまたはリポジトリの唯一の管理権を保持することが保証される。

4. データ管理者が、当該データの徹底的な分析により、取得国の公的機関が保有し使用することが予想されるあらゆる情報を考慮に入れて、仮名化された個人データが、当該情報と照合しても識別される自然人または識別できる自然人に帰することができないことを立証した場合。

[53]EDPB、勧告 01/2020、ユースケース 3、§90 を参照のこと：

1. データエクスポート業者が個人データをデータインポート業者に移転する場合、その法域の法律および/または慣行により、データエクスポート業者が第三国へインターネット経由でデータを移転している間、これらのデータへのアクセスに関する欧州の基本的な保証なしに公的機関がデータにアクセスすることができる場合、移転の暗号化が使用され、その暗号化プロトコルが最先端のものであり、第三国の公的機関が利用可能であることが分かっているリソースを使用した能動的および受動的攻撃に対する効果的な保護が提供されていることが保証される、

2. コミュニケーションに関与する当事者が、信頼できる公開鍵認証局またはインフラストラクチャーに合意する、

3. トランスポート暗号化を提供する送受信システムへの能動的・受動的攻撃に対しては、ソフトウェアの脆弱性やバックドアの可能性のテストを含め、具体的な防御策や最新の対策が用いられている、

4. インフラや使用するソフトウェアの脆弱性の経験により、トランスポート暗号化だけでは適切なセキュリティが得られない場合、個人データはアプリケーション層でも最先端の暗号化方法を用いてエンド・ツー・エンドで暗号化される、

5. 暗号化アルゴリズム及びそのパラメータ化（例：鍵長、可用性攻撃モード）が最先端技術に適合しており、第三国へのデータ移転時に公的機関が利用可能なリソース及び技術的能力（例：ブルートフォース攻撃のための計算能力）を考慮して実行する暗号解読に対して堅牢であると考えられること（上記脚注 *80* 参照）、

6. 暗号化の強度は、暗号化された個人データの機密性が保持されなければならない特定の期間を考慮に入れている、

7. 暗号化アルゴリズムが、既知の脆弱性を持たず、適切に保守されたソフトウェアによって、正しく実装されている、

8. 鍵が、転出者または実質的に同等の保護レベルを提供する法域において転出者に信頼さ れている事業体によって、確実に管理（生成、管理、保管、関連する場合は取得者の身元との 関連付け、および失効）されている。

すでに実施されている補足措置			
組織的対策 [54]	☐ アクセス要求の文書化（要求の受領、回答、法的根拠、関係者） データの最小化（厳格かつきめ細かなアクセス、プライバシー・ポリシー、知る必要性に基づくアクセス、監査による管理、懲戒措置） ガバナンス（すべてのアクセス要求に対するデータ保護責任者または GDPR 参照者の 情報および関与）。 ☐ セキュリティおよびデータ保護標準の採用 (認証と安全標準への準拠）。 ☐ アクセス要求の処理に関する社内方針および手順 ☐ 同一グループ内の事業体間での責任の分担、アクセス要請を処理する特定のチームの任命、そのような要請の管理を担当するスタッフの研修。 ☐ その他（具体的に記入のこと）		
契約上の措置 [55]	☐ 補足的な技術的または組織的措置を拘束力のあるものに含める。 ☐ 契約 ☐ 透明性の要求 転入者は、法律、慣行、アクセス防止措置、アクセス要求、および上記情報の提供が法的に禁止されているかどうかを記載する義務がある。 ☐ データへのアクセスを容易にするバックドアやプロセスの使用禁止		

[54] EDPB, Recommendation 01/2020, Section 2.3 Organisational measures, §128-143 を参照のこと：

[55] EDPB, Recommendation 01/2020, Section 2.2 Additional contractual measures, §98-127 を参照のこと。

すでに実施されている補足措置			
	☐ コンプライアンスを確認するための監査を実施することができる。 ☐ 公的機関によるデータへのアクセスの場合、転出者（およびデータ対象者）への通知 ☐ アクセス要求に挑戦することを約束する ☐ 転入者は、開示命令の合法性を検討し、理由があればそれに異議を申し立てることを約束する。 ☐ 裁判所が本案について決定するまで、命令の効力を停止する暫定措置を求めることを約束する。 ☐ 契約上のコミットメントを遵守できない場合に通知することを約束する。 ☐ データ対象者への補償を含む違反に対する制裁措置 ☐ データ移転に関する義務を遵守しなかった場合の契約解除 ☐ 転入者は、第三国当局からのアクセス要求に対応する際、必要最小限の情報のみを提供することを約束する。 ☐ 転入者が、データ保護法に適合しないことを第三国の認可機関に通知し、同時に輸 出業者に通知することを約束すること。 ☐ 明確なデータは、転出者の明示的または黙示的な同意がなければアクセスできない。		

すでに実施されている補足措置			
	☐　その他（具体的に記入のこと）		
		☐　移転ツールは、これらの既存の措置と組み合わされ、実施されたアセスメントに照らしても**効果的である**。 ☐　移転ツールは、これらの既存の措置と組み合わせても、実施されたアセスメントに照らして**有効ではない**。そのような場合は、さらなる補完的措置を検討する必要がある。	

新たな補完		
説明 (各対策について、その説明、転入者または輸出業者が実施しているかどうか、EDPB 勧告にどの程度準拠しているかを記入すること)		**施策のインパクト** (補足的措置によって緩和される／緩和されるリスクを具体的に示す
技術的措置 （上記の例を参照のこと）		
組織的対策 （上記の例を参照のこと）		
契約上の措置 （上記の例を参照のこと）		
	☐　移転ツールは、実施されたアセスメントに照らせば、既存および新規の補足措置と組み合わされ、**効果的である**。 ☐　移転ツールは、既存および新規の補足的措置と組み合わされているが、実施されたアセスメントに照らすと**有効ではない。**	

これらの措置と組み合わせた移転ツールが、実施されたアセスメントに照らして有効であるという結論に達した場合、補足措置の効果的な実施を条件として移転することができる。すでにある措置で十分な場合は、そのままステップ 6 に進むことができる。既存の対策に加えて）補足的な対策が必要な場合は、ステップ 5 に進むことが推奨される。

TIA の完了後、または再アセスメント中に、移転ツールの有効性を確保するために必要な措置を講じることが不可能であるという結論が出た場合、計画された移転は実施されるべきではない。すでに移転が進行している場合は、それを中止する必要がある。後者の場合、転入者はすべてのデータを消去して輸出業者に証明するか、すべてのデータを返却して既存のコピーを消去しなければならない。

3.5 補足措置を実施する（ステップ 5）

移転されたデータが実質的に同等の保護レベルを享受することを保証するための補完的措置が 特定されたら、新たな補完的措置を実施するために取るべき行動を、従うべき手続き上の手 順とともに下表に列挙することが推奨される。こうすることで、それらの措置が効果的であることを保証し、障害（例えば、財政的な困難、有能なチームの不在など）を予期することができる

従うべき手続き上のステップは、移転のベースとなる移転ツールによって異なる可能性がある。EDPB Recommendations on Measures that Supplement Transfer Tools（移転ツールを補完する措置に関する EDPB 勧告）には、これらの手順の一部が記載されている。[56]

アクション	
アクション 1 名前	説明：
	個人/日数での見積もり費用（オプション）：
	担当者（法律専門家、技術専門家、事業部門など）
	完成予定日
アクション 2 名前	説明：

[56]EDPB 勧告 01/2020, Section 2.5 Step 5, §59-68 を参照のこと。例えば、SCC が改正され、それによって SCC に含まれる権利と義務が制限される場合、または追加措置が SCC と矛盾する場合、転出者は所轄官庁に認可を申請する必要がある。

アクション	
	個人/日数での見積もり費用（オプション）：
	担当者（法律専門家、技術専門家、事業部門など）
	完成予定日
…	…

オプション
データ保護担当者（該当する場合は、データ保護責任者）の意見。
情報システムのセキュリティ担当者（該当する場合は、最高情報セキュリティ責任者）の意見

社内ガバナンス・ルールに従った移管責任者による妥当性確認

3.6 適切な間隔で再評価を行う（ステップ 6）

適切な間隔で、移転ツールや、場合によっては移転のために実施された補足措置を再評価することが推奨される。これは、第三国において移転ツールや補足措置がもはや有効でない場合、移転が中断または終了することを確実にするために不可欠である。このため、以下の表では、移転の定期的な見直しが推奨されている

これらの適切な間隔は、データの仕向け国、および移転に関わるデータ対象者の権利と自由に対するリスクのレベルに応じて、ケースバイケースで決定される。様々な状況において、例えば、第三国の法律または慣行の変更、転入者がその約束を遵守できない場合、または第三国で適用される法律に関する欧州委員会の評価が変更された場合など、次回の見直しの初回期日前に移転保護を再評価する必要が生じる可能性がある。このため、当該国におけるデータ保護の再評価が必要かどうかを予測できるよう、当該国の法制上のニュースをフォローすることが推奨される。

防御を再評価する	
レビュー間隔 (例：2 年ごと)	
次回審査日	
早期審査がある場合はその旨と、その正当性	