ESOMAR データ保護チェックリスト

世界調査行動規範およびガイドライン

社会・世論および市場調査の世界的協会である ESOMAR は、130 か国において 4,900 社の加盟企業を有し、市場調査の推進、発展および向上を目的とする主要機関です。行動規範およびガイドラインは、www.esomar.org でご覧いただけます。

Official Translation Partner:
Language Connect

© 2015 ESOMAR. 2015 年 1 月発行。最終更新：2015 年 12 月。

目次

1　はじめに

グローバルな環境で作業をする調査者は、個人のプライバシーおよび個人データの保護の尊重を確実にするために制定された各国で異なる法律に対処しなければならない場合が増えている。調査者は、業務を展開する国における法的要件だけでなく、調査を実施、またはデータ処理を行う全ての国におけるデータ保護法の確認および遵守に責任を負っている。

同時に、生活のあらゆる面における新しいテクノロジーの普及のため、調査者が使用できる個人データ量が増大すると同時に、保護しなければならない新しいタイプの個人情報も増加している。

その中でも、調査者が回答者と顧客に対する平明性を確実にし、提供する情報への信頼を維持し、調査参加者に対する配慮を示すことにより、市場、社会および世論調査の評判を守る必要があるということに変わりはない。

2　範囲

本書の目的は、調査者、特にデータ保護要件に関する広範なリソースまたは経験が不足しがちな小規模機関の調査者に対し、調査参加者が各自の個人情報を確実に管理するため、データ保護のグローバルな枠組み内における調査者の責任に関して、全般的なガイダンスを提供することにある。使用される特定の枠組みは、経済協力開発機構（OECD）によって開発されたものである。本枠組みには、プライバシーを確実にし、個人データを保護するために作成された 8 原則が含まれている。

- データ収集の制約
- データの質
- 目的の特定
- 使用の制限
- セキュリティ保護
- 公正さ
- 個人の参加
- 説明責任

これらの広義の原則は、世界各国で既存および制定されつつあるプライバシーおよびデータ保護法の大半に反映されている。

ただし、調査者は、OECD の原則は EU データ保護要件と非常に密接に関連していること、そのため、その他の地域で調査を実施する調査者は、適用される可能性のあるその他の枠組みを調べる必要があることに注意すべきである。これには、アジア太平洋経済協力（APEC）プライバシーフレームワーク、米国セーフハーバーのプライバシーに関する原則、そして米国公認会計士協会（AICPA）およびカナダ公認会計士協会（CICA）が作成した「一般に公正妥当と認められたプライバシー原則」（GAPP）が含まれる。一般的に、これらの枠組みには法的効力はないが、調査者が該当地域で業務を行う際に採用しなければならない基本的な原則を示している。

さらに、特定の国では基本原則の実施方法が異なる場合があるため、調査者は、フィールドワークおよびデータ処理を計画する各国で定められるデータ保護および市場調査の自主規制要件を確認し、遵守しなければならない。本文書で提供するガイダンスは最低限の基準であり、特定の調査プロジェクトでは追加的な方策で補足する必要がある可能性がある。調査者は、自主規制要件を確実に遵守するため、調査を実施する国によっては、法的機関に問い合わせる必要がある。また、ディーエルエイ・パイパー社（DLA Piper）が作成し、毎年更新するオンラインリソースである The Data Protection Laws of the World も参照のこと。

最後に、ヘルスケア調査など専門的な分野において調査を実施する調査者は、さらなるガイダンスとして、 2014 年 EphMRA 有害事象報告ガイドラインなど、具体的なガイダンスを参照のこと。

3 「しなければならない」と「すべきである」の使用

本書では、必須要項を区別するため、「しなければならない」という表現が使用される。調査者が ICC／ESOMAR 市場および社会調査における国際行動規範を遵守するために従う義務がある原則または手続きを説明する際に、「しなければならない」という表現が使用される。「すべきである」という表現は、実施について説明する際に使用される。この表現の使用は、調査者は、調査デザインに応じて異なる方法で、原則または手続きの実施を様々な方法で選択できることを示すことを意図している。

4 定義

ビジネス・トゥ・ビジネス調査（B2B）とは、企業、学校、非利益団体などの法人組織に関するデータ収集を意味する。

ビジネス・トゥ・コンシューマー調査（B2C）とは、個人からのデータ収集を意味する。

同意とは、回答者が、個人データの収集および処理に対して、自由意思でおよび情報を基に与えた承諾を意味する。市場、社会および世論調査では、この同意は、調査参加者に対して、収集されるデータの性質、そのデータが使用される目的、および個人データを保管する個人名または組織名に関する明確な情報の提供に基づく。調査参加者は、いずれか時点でも、同意を取り消すことができる。

データ管理者とは、個人テータの処理方法の決定に責任を担う個人または組織を意味する。例えば、調査依頼企業が顧客に関するデータの管理者である、政府の福祉事務所が福祉受給者から収集したデータの管理者である、調査パネルプロバイダーがオンラインパネルメンバーから収集したデータの管理者である、調査企業がオムニバス調査の参加者から収集したデータのデータ管理者である。

データ処理者とは、データ管理者の依頼を受け、その指示のもとで、個人データの取得、記録、保持、または（分析を含む）作業を実施する者を意味する。上記に記した通り、調査機関はオムニバス調査のデータ管理者であると同時にデータ処理者になり得る。

プライバシー保護法とは、国内法または規制、本文書に設定される原則に則った個人データの処理に効力を持つ法の施行を意味する。

市場調査とは、社会・世論調査を含み、見識を得たり、意思決定の根拠とするため、応用社会科学による統計的および分析的方法および手法を使用して、個人または組織に関する情報を体系的に収集し、解釈することを意味する。調査に参加する個人の身元は、その個人の明示的な同意なく情報の使用者に開示されず、情報提供の直接的な結果として、その個人に対して販売促進がされることはない。

パッシブなデータ収集とは、伝統的な質問・回答という形式ではない方法で収集されたデータを意味する。

個人データとは、身元が特定されたまたは特定可能な自然人（法人またはその他同等の団体と対比される個人）に関するすべての情報を意味する。身元の特定が可能な個人とは、特に身分証明番号、または身体的、生理学的、精神的、経済的、文化的または社会的特徴の言及により、直接的または間接的に特定が可能な個人である。一部の調査では、このようなデータ記録として、調査中に収集した画像、動画、録音、またはその他の個人情報によって個人の特定が可能な状況が含まれる場合がある。

個人データの処理には、自動化された方法またはそれ以外の方法を使用した、個人データの収集、記録、整理、保存、適合または修正、読み込み、協議、使用、送信による開示、普及またはそれ以外の方法で使用可能にすること、配列または組み合わせ、ブロッキング、削除または破棄が含まれるが、これらに限定されない。

調査参加者とは、調査プロジェクトにおいて、アクティブなインタビューまたはパッシブな方法で個人データが収集される個人を意味する。

調査者とは、顧客の組織に勤める者や、技術プロバイダなど使用されるあらゆる下請業者を含み、市場調査プロジェクトを実施する、またはコンサルタントとして行動する個人または組織を意味する。

調査の顧客またはデータ使用者とは、調査プロジェクトの全体またはいずれかの部分を要求、依頼、資金を出資し、購読する個人または組織を意味する。

センシティブなデータとは、身元特定が可能な個人の人種的または種族的出自、健康または性生活、犯罪歴、政治的意見、宗教または哲学的信念、または労働組合のメンバーシップなどに関するすべての情報を意味する。司法管轄地域により、他の情報もセンシティブであると定義している場合がある。例えば、米国では、個人の健康に関する情報、収入またはその他の経済的情報、金融に関する識別情報、および政府が発行した、あるいは経済的に個人を特定可能である文書もセンシティブとみなされる。

転送とは、データに関して、媒体の種類にかかわらず、1 つの組織から別の組織へのデータの開示、コミュニケーション、複製、または移動を意味する。これには、ネットワーク間の移動、現物の移動、1 つのメディアまたはデバイスから他のメディアまたはデバイスへの転送、またはデータへのリモートアクセスが含まれるが、これに限定されるものではない。

個人データの国外への転送とは、データを収集した国以外の国からのデータへのアクセス、およびデータに対するクラウドテクノロジーの使用を含み、何らかの方法で国境を越えた個人情報の移動を意味する。

5　データ保護方針および手順のセルフヘルプチェックリスト

下記のチェックリストを使用する際、項目の表題と順序は、OECD で使用されているものとは異なることに注意すること。ここでの目的は、調査者が慣れた言語および順番で原則を示すことにある。また、項目が相互に関連し、重複していることがある。 それでも、本チェックリストを全体として考慮し、個々の項目は排他的ではなく補足的なものとみなし、組織がデータ管理者またはデータ処理者として行動しているかどうかによる違いに注意を払うことが重要である。以下の質問に「はい」と回答できない場合は、プライバシー保護体制における潜在的なギャップがあり、そのため 1 つまたは複数のデータ保護法に違反する潜在的なリスクがあることを示唆している。

5.1　最小限の影響

1. *調査プロジェクトをデザインする際、調査目的に必要な項目だけに個人データの収集を限定し、その目的とは相容れない方法で使用されないことを確実にしているか？*

調査者は、インタビューをその特定の個人に対して確実に実施するために必要とされ、また、品質管理、サンプリング、および分析という点で必要になると思われる個人データのみを収集および保持しなければならない。B2B 調査の場合、これには参加者個人の組織内での役職や職位が含まれるが、それはこの情報が調査の目的で必要である可能性があるからである。

伝統的な質問・回答を使用せずに個人情報が収集されるパッシブなデータ収集方法にも、同じ原則が適用される。そのため、収集する個人情報が調査の目的で必要なものだけであることを確実にするのは、調査者の責任となる。それ以外の個人情報を得た際は、それらの項目はフィルター処理したうえで削除しなければならない。

2. *市場調査プロジェクトに協力した直接的な結果として、調査参加者が損害を被ったり不利な影響を受けたりしないことを確実にするプロセスを実行しているか？*

調査者は、調査結果から個人情報が突き止められたり、個人の身元が交差分析（演繹的開示）、小サンプル、またはその他の方法で推論できないことを確実にしなければならない。その例として、地理的データ、顧客満足度調査から具体的な社員の特定が可能な、能力などの補助的情報を合わせたものが含まれる。

3. *委託業者またはその他の第三者サプライヤを使用して業務を実施する計画がある場合、下請業者が合意された業務を遂行するのに必要な最低限の情報を開示しているか？委託業者が同水準の保護を保証することを記載した契約書はあるか？*

委託業者を使用する際は、合意した業務の遂行に必要な最低限の個人データのみを提供し、常に契約書や指示書を通して、それらのデータを所有する委託業者の責任を明確にする。すべての委託業者は、調査機関と同一の法規制を遵守しなければならない。さらに、個人情報を下請業者またはその他の第三者サプライヤに転送する場合は、調査機関の顧客から事前に同意または委託を受けなければならない。

上記は、調査参加者に対し、収集したデータは全て機密事項として扱われ、集計されたレベルでのみ分析および報告されることを保証することを想定したものである。調査参加者が自分の回答に個人情報を結び付けることに同意した場合は、調査参加者に対し、その情報がどのように共有および使用されるかを通知しなければならない。

5.2 通知と同意

4. *個人情報が収集される全ての参加者から同意を得ているか？*

OECD が定めるプライバシー原則のもと、いかなる個人データも、合法的で公正な方法で、そして適切な場合は、調査参加者がそれについて知り、かつ同意したうえで、取得するべきである。一般的に、国内法は合法的で公正な根拠を提供するが、多くの場合、調査者は同意に依拠する義務がある。

同意を得る責任が他の者にある例もある。よく見られる例には、第三者パネルの使用、または顧客データベースの使用が含まれる。これらの、および状況や同様の状況においては、調査者は適切に同意を得たことを確認しなければならない。

同意は次の通りでなければならない。

- 自由意思（任意、いかなる時点でも取り消しが可能）
- 具体的（1 つまたは複数の認識可能な目的に関している）
- 情報に基づいている（同意することに関連する結果をすべて理解している）

同意は、以下の項目の情報を提供された調査参加者の表明または行動によっても、明確に示されていなければならない。つまり、調査参加者に対し、（a）個人情報が使用される方法、（b）収集される具体的なデータ、（c）データを収集する企業または組織、データ収集者と同一の組織でない場合は、データ管理者の名前、住所、連絡先情報、（d）データが第三者に開示されるかどうかが通知されるべきである。

調査者は、同意を得るために使用し、通常、オプトアウト、オプトイン、黙示的、情報に基づいた、または明示的、と表現されるメカニズムについて慎重に検討すべきである。選択された特定の方法は、文書化するべきである。

一般的に、データ収集がよりセンシティブ、侵入的、または明白でないほど、要求される同意の基準も高くなる。一部の司法管轄地域では、データを収集する前に該当する個人による明示的な同意を得ることを義務付けている「センシティブな個人データ」のクラスを定義している場合がある。

調査者が、意図せず、または参加者とは定義されない個人からデータを収集または取得する場合もある。その例には、参加者が任意に提供した情報、調査実施に必要な以上の情報を含

む顧客が提供したリスト、および画像または動画に写った参加者ではない個人などが含まれる。調査者は、このような情報をその他の個人データと同じ方法で取り扱うべきである。このようなデータは、特にデータが収集された個人に対して、データの所在、保存、または使用について通知する方法がない場合には、ただちに匿名化し、破棄すべきである。一部の司法管轄地域では、意図的に取得したその他の情報と全く同じ方法でこのようなデータを削除したり、取り扱うことが義務とされている。

5. データを収集し、維持する目的をはっきりと理解しているか？

調査業界はこれまで長い間、市場調査と、広告、販売促進、リスト開発、ダイレクトマーケティング、および直接販売など他の目的でのデータ収集を区別している。この区別は、規制当局および一般の人たちにとって、調査の目的を明確にし、肯定的な印象を促進するうえで重要である。近年、新しいテクノロジーが出現し、オンライントラッキングやダウンロード可能な携帯アプリなどを通して個人情報を収集する機会が増加している。どのような場合にも、何らかのデータ収集に先立って、調査参加者となる可能性のある者に対し、そのデータが使用される目的、品質管理を目的とするフォローアップなど、その結果として起こり得ることについて、通知することが不可欠である。

調査者が市場調査の目的で使用する個人データを調査参加者から収集する時、それを通知する際に調査参加者に対する平明さは重要な要素となる。調査参加者は、収集される個人データに意図される使途および第三者とのあらゆる共有について、十分な情報を与えられていなければならない。例えば、個人データに意図される使途が、調査回答を顧客プロフィールと結びつけるものである場合、個人データを収集する時に調査参加者に対してそのことを開示しなければならない。

調査者は、プライバシー通知を定期的に見直し、収集するデータのタイプおよび意図される使途に変更がないことを確認しなければならず、調査組織内で使用される実際の業務慣行やテクノロジーが調査参加者に対してなされたコミットメントと一致し、進化する規制要件を遵守していることを確実にしなければならない。個人データに予定される各使途は、国内のプライバシー保護法の遵守、ICC／ESOMAR の行動規範および ESOMAR のガイドラインの遵守、そして調査回答者に対してなされたプライバシーに対する確約との整合を確実にするため、分析されなければならない。

6. 収集される特定のデータについて明確に理解しているか？

一部の司法管轄地域では、個人データの定義は広範であるため、収集される可能性のある個人データのあらゆる要素を検討してから調査回答者に対する通知を作成する。個人データには、氏名、住所、メールアドレス、電話番号、携帯電話番号、生年月日、携帯デバイス識別子、IP アドレス、画像、音声記録、動画、身分証明番号（運転免許証、ソーシャルセキュリティ、国民年金）、組織から与えられるユーザー識別子、ソーシャルメディアのユーザー名、クッキーに保存されるデータ、またはトラッキングピクセル／タグなどが含まれる可能性がある。また、単一データだけでは国内法において身元が特定できるデータとみなされない場合でも、他のデータ（例えば、郵便番号、性別、勤務先または学校、役職名と給与）と組み合わせると個人が特定可能になる場合がある。

さらに、個人データを受け取る可能性のあるすべての者にも考慮が必要である。調査者、調査機関、第三者サービスプロバイダ、およびエンドクライアントはいずれも、調査プロジェクトの過程で個人データを収集および使用できる可能性がある。

7. 参加者が認識しない可能性もあるパッシブなデータ収集を含み、データの収集方法を明確にしているか？

従来、調査は個人データを収集する主な方法として、インタビューに依存してきた。上記 5 に記載される通り、新たなテクノロジーが出現しているため、データが収集されている個人が知らないうちに広範な個人データを収集することが可能になっている。全ての調査参加者は、収集される具体的なデータ、および、インタビューなどのアクティブな方法、または携帯アプリやオンラインのクッキーを通じたトラッキング行為などのパッシブな方法を問わず、データの収集に使用される方法について知らされていなければならない。

調査者は、収集されるデータまたはデータ収集方法のどのような要素が調査参加者にとって予想できないかを検討し、収集方法を明確に開示するべきである。予期されていない、または侵入的である可能性があるデータ収集および使用を説明するため、プライバシーに関するより詳細な通告に重ねて、「簡易」通告を検討すること。特にジオロケーション機能を持つ携帯アプリ、「パッシブ・リスニング」、および携帯デバイスのオペレーティングシステムの計測はいずれも、このような行為に関して調査参加者に詳細を説明し、調査参加者の明示的な同意を得る必要がある。

5.3 統合 / セキュリティ

8. *収集した全ての個人データが正確、完全、そして最新のものであることを確実にする手順が整っているか？*

品質確認は、調査プロセスの全段階において実施されるべきである。アンケートまたは調査アプリの開発をする際、データ収集におけるエラーのリスクを最小限に抑えるため、フィールドワークが開始される前にテストをするべきである。データ収集段階では、適用される調査品質基準に従って、入手データをモニターし、検証するべきである。データ処理および報告の段階では、データが正確であり、分析、結論および推奨事項がデータと整合していることを確認するため、さらなる品質確認を実施すべきである。

パネルを運営する調査者は、パネルメンバーがいつでも自分のデータを見直しおよび更新できることを確認し、パネルメンバーに定期的にこの作業をすることを促すべきである。パネルから抽出されたサンプルには、最新の人口統計学的情報が含まれているべきである。これに関する標準的な実施方法は、ISO 26362:2009（市場、世論及び社会調査におけるアクセスパネル）を参考にすること。

9. *情報の収集、さらに処理に必要な期間を超えて情報が保存されないことを確実にしているか？情報が必要でなくなった際に、身元を特定する情報を別の場所に保存または削除するための手順があるか？*

調査者は、データ保持期間をできるだけ短期間に、ただし、いずれの場合も適用される法律、収集する個人データのソース、および調査者がデータ管理者またはデータ処理者として行動しているかどうかに基づいて設定するべきである。後者の場合、顧客が契約によって保持期間を指定する可能性がある。

個人データのソースにかかわらず、長期にわたる調査の情報、またはパネリストのプロフィール情報は、一般的に、パネリストがアクティブなメンバーである間使用および保持される。反対に、アドホック調査に参加する非パネル参加者に関する個人データは、保持期間をはるかに短い期間とするべきである。当然ながら、正確性を確認し、データの完全性・プライバシー原則に関する要件を満たすために、データ処理の段階で品質確認が実施されなければならないため、個人情報を早すぎる時期に破棄しないことが重要である。

個人データが使用される際のベストプラクティスは、調査者による仮名の識別子の使用である。参加者の氏名、住所または電話番号と、それに対応する内部生成された ID 番号を結びつけるマスターファイルは、サンプリングまたはパネル管理担当社員など、少人数にアクセスを限定し、安全に保管されなければならない。そのため、参加者レベルのデータを分析するために必要な業務を行う調査者、データ処理およびコーディング担当者は、参加者の氏名、住所または電話番号を見ずに作業することが可能である。

調査への回答が処理され、集計された統計的データとして報告される際、調査組織が個人データを保持することがないよう、参加者に関する個人データをそれに対応する仮名化された識別子とともに削除するべきである。

10. *収集した可能性のある個人データについての個人からの要求に対応する手順は整っているか？個人からのアクセスの要求に対処する手順には、その個人の身元の承認、妥当な期間内での要求への対応、不正確なデータの修正または完全な削除の許可が含まれているか？*

機関が保持している個人データへのアクセスを希望する個人に対応する正式な手順を策定し、伝達し、従うべきである。個人情報を他者に不適切に開示されることを防ぐため、アクセスを要求する個人の身元の承認は重要である。

アクセスを要求する個人の身元が承認されたら（その者が申し出通りの者であり、該当する個人データへのアクセスに対する法的権利を有している）、調査者は、適用される法律により 10 日または 30 日以内など、できるだけ迅速にアクセスの要求を満たす努力をすべきである。調査機関が要求を満たすためにさらに時間が必要な場合は、その個人に通知し、理由が妥当である限り、法律で設定された期限を延長できる場合がある。例えば、協議したり、複数のデータベースから要求された情報を集める場合などに、さらに時間が必要になることがある。

データ保護法には、特定の状況において調査機関が個人情報への個人のアクセスを拒否する例外措置が設けられている場合があるが、これらの例外措置は市場調査に関連して処理された個人情報に適用される可能性はほとんどない。例えば、適用される法律で、情報が弁護士依頼者間秘匿特権である場合、機関がアクセスの要求を拒否できる場合がある。他の例では、調査機関が法執行または国家安全の目的で情報を政府機関に開示する場合、その政府機関は調査機関に対しアクセスを拒否、または情報が開示されたことを明らかにしないよう、指示する場合がある。

11. 各データの喪失、不正アクセス、破壊、使用、修正または開示などのリスクから保護するためのセキュリティ・プロトコルは整えられているか？

これらの責任の遂行は、個人情報およびその他のタイプの機密情報を保護するためのセキュリティ方針を策定し、実行することから始まる。ISO 27001 は、徹底したセキュリティ方針が基づくべき情報セキュリティ基準として認識されている。

必要な保護を提供するために適切なセキュリティ措置の使用には次が含まれている。

- 物理的な方策（ファイリングキャビネットに鍵をかける、オフィスへの入室を制限する、警報システム、セキュリティカメラ）
- 技術的ツール（パスワード、暗号化、ファイアウォール）
- 組織的管理（バックグラウンド確認、コンピュータの社外持ち出しに関する規則、「知る必要がある」者のアクセス制限、社員研修、顧客および下請業者との契約）

セキュリティ方針には、個人データが開示されるというデータ違反の可能性への対処手順も含まれているべきである。顧客のデータベースなど、データが他者から収集および供給された場合、その当事者に直ちに通知しなければならない。開示により、データが開示された参加者がリスクにさらされる場合（個人情報の盗難など）は、参加者に通知し、そのリスクから保護するための適切な措置をとられなければならない。

12. 個人データの保持期間について、明確に記述されているか？

個人データの保持期間は、Q9 への対応において記された様々な状況に応じて、調査プロジェクトごとに異なる場合がある。

一般的な保持はプライバシー方針に含まれているべきだが、異なるタイプの研究に正確な保持期間を伝達することは、必ずしも現実的ではないかもしれない。そのため、調査者は、調査依頼資料、アンケートの導入部分、または特定の調査のための同意フォームにデータ保持情報を掲載することも検討するべきである。調査者は、要求に応じて、該当するプロジェクトのデータ保持期間を知らせる準備を整えておくべきである。

5.4 データの転送

13. 個人データの使用および開示に関する決まった規則および手順があるか？

これらの規則および手順は、その国のプライバシーおよびデータ保護法においてはっきりと説明されている。社員が個人データの管理方法に関する手順を実行し、規則と手順に精通し

ていることを確実にするために、法律が意味することを、プロセスとともに明確に文書化するべきである。例えば、これには、いかなるデータも、顧客や顧客機関の調査者に対しても、調査参加者の同意なく、開示できないという原則が含まれる。

14. *個人データが開示される可能性のある条件は、明確で明白か？*

調査参加者は自分の個人データの状況を知っていなければならず、このことは、口頭で説明されるか、あるいは調査参加者が同意したことのエビデンスとして記録される同意書を通して、書面または文書で提供されなければならない。

15. *社員はこれらの規則を知っていますか？また、手順の実行方法について研修を受けているか？*

機関のプライバシー方針には、機関のデータ収集および管理方法が説明されている。参加者に対してなされたプライバシーに関する約束が守られていることを確実にするため、社内標準操作手順（SOPs）を開発することも同様に重要である。

プライバシーに関する社員研修は、適用される法律、業界の行動規範、機関の顧客対応プライバシー方針、SOPs が含まれているべきである。プライバシーに関する研修は、最低でも年に 1 度実施し、出席を記録すべきである。

参加者に直接対応する現場の全社員は、機関の方針および手順について詳細に説明できるべきである。また、対応できない問い合わせに対するサポートを得るために、誰に連絡すべきかを知っているべきである。

手順に従っていることを確認する何らかのモニタリングなど、監督および責任が明確に説明されているべきである。

5.5 国境を越えた個人データの転送

16. *個人データが別の法管轄地域に転送される場合、転送元と転送先の両法管轄地域におけるデータ保護要件を満たす方法で転送されているか？*

これは多くの場合、「個人データの国境を越えた転送」と呼ばれる。これは、データが国境を越えて収集される場合、またはデータ処理が他の国で実施されるか、アウトソースされる場合に生じる。例えば、顧客が提供した顧客またはサービス使用者のデータを使用して、他の国で調査を実施するため、他の国の調査者と協力する場合がある。各国には、このようなデータを取扱い保護する方法に関する独自の規則があり、調査者はそれを遵守しなければならない。これは複雑に見えるかもしれないが、調査者が直面するコンプライアンスに関する問題が、次の 3 つの問題に分けられる際、役に立つものである。

- 個人データの国境を越えた転送が、適用される法律を遵守して実行することを確実にする。国境を越えたデータの転送に対する十分な保護を確実にするための根拠として最もよくみられるのは、同意または適切な契約条項であり、当該国の法律で要求される場合、当該国のデータ保護当局またはその他の該当するプライバシー規制当局から取得するこれらの契約の使用に対する事前承認も根拠となる。追加されるセキュリティ方策として、およびデータ処理が他国で実施される場合のリスクをさらに減少させるため、実行可能な場合、個人レベルのデータと参加者の身元を結びつけるために 偽名の ID 番号のみを使用するよう、個人を特定できるデータは削除されるべきである。

- 顧客が提供したサンプルを使用して調査を実施する場合など、調査者がデータ処理者として行動する場合に国境を越えた転送を実施する規模。調査者が国境を越えた転送を規定する規則を確実に遵守するよう注意している場合でも、調査者がデータ管理者（調査依頼企業など）の代わりにデータ処理者として個人データを処理する場合、調査者はデータ管理者として管理する個人データの国境を越えた転送を許可できない場合があり、その場合はプロジェクトの実施に影響を与える可能性がある。上記に関して、両当事者間で書面による合意が交わされているべきである。

- 他国の調査参加者から個人データを収集する場合の個人データの国境を越えた転送。例えば、調査者が調査を管理する国とは異なる国に住む調査参加者を対象としたオンライン調

査など。プライバシーに関して適用される法律は、通常、調査者の居住国の国内法となる。ただし、調査者は、調査またはパネルが、データが収集される国で適用されるその他一切の法律を遵守していることも確実にしなければならない。以下を確実にするが推奨される：（1）国を含めた調査者の法的詳細（企業名、住所など）が全ての依頼資料に明確に記されている、（2）使用されるオンラインプライバシー方針に、調査またはパネルの参加によって起こる国境を越えた転送に関する平易かつ明確な説明が含まれる、そして（3）パネル依頼の際の同意を求める質問に、国境を越えた転送について言及されている。

5.6 調査のアウトソーシングおよび委託

17. 組織外のデータ処理者またはその他の委託業者の適切な監督を含む明確な要件はあるか？

何らかの形態のデータが転送される際、組織外のデータ処理者またはその他の委託業者がすべて従うべき個人データに関するデータ保護規則を明確に伝達しなければならない。データが個人レベル、集計データレベルにかかわらず、あらゆるデータの転送に対し、転送されるデータの暗号化または安全な FTP 転送プラットフォームの使用など、専用の IT 処理を使用して、さらなる保護をすべきである。委託業者または組織外のデータ処理者により、バックアップとして複製が作成される場合、保管中にこれらのデータを保護し、必要がなくなった時に削除するための明確なプロセスがなければならない。

5.7 プライバシー保護方針

18. プライバシーおよび個人データ保護プログラムに関する情報はすぐに入手可能で、参加者がわかりやすい形式になっているか？

多くの司法管轄地域では、調査参加者がプライバシー保護方針に関する情報をすぐに入手できることが求められている。要求される内容および詳細は国によって異なるが、調査者は調査参加者に対し自分の身元をはっきりとさせ、調査の目的、個人データの収集方法、個人データの管理方法（保存、使用、アクセスおよび開示）、そして詳しい情報の入手方法または苦情の提起方法が説明されていることを確実にしなければならない。

調査者は、方針が理解しやすく、読み手に関連するものであり、探しやすく、できるだけ簡潔であり、機関の業務に合わせたものであることを確実にしなければならない。これには、方針を適切な全ての言語で入手可能にし、定期的に見直し、必要があれば更新することが含まれる。

19. データ管理者の身元および責任は明確か？

調査者は、個人データの管理に対する役割と責任を調査参加者に対して明確にしなければならない。これには、データ管理者の特定、組織外のデータ処理者を使用するかどうかなどが含まれる。データ管理に最終的に責任を負う機関に関して、参加者が疑問を持たないようにしなければならない。

一部の司法管轄地域では、機関のデータ保護業務の責任者として個人を特定することも求められている。

顧客が提供するサンプルを使用した盲検の場合、インタビュー開始時に、顧客名に関する情報は回答にバイアスを生じる可能性があるため、その情報は調査が終了するまで明らかにされないことを参加者に伝えるべきである。多くの国のデータ保護法は、調査者が個人データを収集した対象者について知る法的権利を参加者に与えているため、参加者が要求した場合は、調査者は常に顧客名を特定する準備をしなければならない。

20. データがある場所にかかわらず、データ管理者はその管理下にある個人情報に対して責任があることは明確か？

調査者が個人データの処理に委託業者を使用、または他の法管轄地域に個人データを転送する場合、調査者はデータ管理者に対し、委託業者および処理する場所に関する情報を提供する準備をし、必要な場合、データ管理者から書面による同意を事前に得なければならない。

調査機関がデータ管理者である場合、データ処理者の使用に言及し、適切な場合、プライバシー保護方針に国または広域地域を挙げるべきである。調査者は、一部の司法管轄地域は、同等のデータ保護法がない国または地域への個人データの転送を禁じているという事実に注意すべきである。該当する国の法律によって課せられる国境を越えた転送を規定する規則の遵守を条件として、大半の司法管轄地域では複数国に広がるグループにおける個人情報の転送は許可されているが、一部の国はデータが置かれる場所をデータ提供者に通知することが求められている。

6 特別な問題

6.1 子供からのデータ収集

保護者による許可を必要とせずにデータを収集できる年齢を規定する規則は国により大きく異なる。調査者は、保護者による許可が必要な場合、または文化的に繊細な事柄のため特定の取り扱いが必要な場合を判断するため、データが収集される国の国内法および自主規制の行動規範を調べなければならない。国のガイドラインがない場合、ESOMAR のガイドライン、青少年へのインタビューを参考にすること。

子供からのデータ収集には、その子供の法的保護者から検証可能な許可を得る必要がある。親または責任を負う大人が情報に基づいて子供の参加を決定できるように、調査プロジェクトの性質について十分な情報を提供しなければならない。調査者は、責任を負う大人の身元、および子供との関係について記録すべきである。

6.2 ビジネス・トゥ・ビジネス調査

多くの調査プロジェクトが、企業、学校、非営利組織、または同様の組織からデータを収集している。このような調査には、収益、社員数、セクター、地域など、組織に関する情報の収集が伴う場合が多い。

あらゆる場合において、参加組織は報告における身元開示に対して、他の調査形式において個人に与えられるものと同等の水準の保護を受ける権利がある。

多くの国のデータ保護法は、個人の役職名および職場の連絡先情報を個人データとみなしていることに注意が必要である。一部のデータ保護法では、その要件をさらに自然人および法的主体（個人と法人など）にまで拡大している。

6.3 画像、録音、および動画

いくつかの新しい調査手法により、調査プロセスの一環として画像、音声および動画を作成、保存および転送することができる。主な例として、エスノグラフィーやミステリーショッピングの 2 つが挙げられる。

調査者は、画像、音声、および動画は個人データとなり得るうえ、その場合はそのように取り扱われないければならないことを、認識しなければならない。調査者が参加者に対してこのような形態で情報提供を依頼する場合、調査者は、特に参加者以外の人からの求められていないデータ収集を避ける方法に関するガイダンスも提供するべきである。

最後に、ある種の観察調査では、調査参加者として依頼されていない人も含む公共の場での画像・動画の撮影または録音を伴う場合がある。このような状況では、調査者は顔がはっきりと写り、身元の特定が可能な人たちから、この画像の共有に対する許可を得なければならない。許可が得られない場合、その個人の画像はピクセル化または、それ以外の場合は匿名

化しなければならない。さらに、責任を負う個人または組織の連絡先情報と共にその地域が観察下にあることが記載されている明確でわかりやすい掲示を設置すべきである。カメラは、観察を目的とする地域のみをモニタリングするよう設置すべきである。

6.4 クラウドストレージ

個人データのクラウドへの保存は、慎重に決定すべきである。調査者は、クラウドストレージサービスプロバイダのセキュリティ管理および標準的な利用条件を評価しなければならない。セキュリティ違反が生じ、個人データが危険にさらされた場合、多くのクラウドストレージサービスプロバイダが提供する補償は十分ではない。これは、影響を受けた個人が損害を受ける結果となる重大なプライバシー侵害により、調査者の機関が生経済的損害および損失の大きなリスクを受けることを意味している。

そのため、調査者は、このようなリスクから守るために代替統制を実行するべきである。例えば、調査者は、実行中（クラウドへ／からの転送）および保存中（クラウドプロバイダーのサーバに保存）に個人データを暗号化すべきである。調査者は、サイバー賠償責任保険の加入も検討すべきである。

調査者はまた、クラウドストレージが国境を越えた転送であるかどうかを判断するため、個人データが保存される具体的な場所についても検討しなければならない。詳細については、本文書のセクション 5.5 を参照すること。一部のクラウドサービスプロバイダは、場合によっては適切であると思われる、国ごとに保存場所を提供している 。

最後に、調査者は、個人データをパブリッククラウドではなく、プライベートクラウドに保存するべきである。プライベートクラウドとは、特定のデータセンターで調査者の機関専用の装置を割り当てているクラウドである。プライベートクラウドの主なメリットは、調査者が個人データの保管場所を常に知っていることである。反対に、パブリッククラウドは、データが 2 つ以上のデータセンター、2 つ以上の大陸に保存される結果になる場合があり、そのため、データ保護法に定められる適用要件、およびデータ管理者との間で締結している個人データの保存場所を指定する契約の両方の遵守に関する問題が生じる可能性がある。

6.5 匿名化と仮名化

調査者のデータ保護に関する主な責任は、顧客または一般の人に対して開示する前のデータの匿名化である。匿名化とは、データを個人が特定ができない形態にするため、個人を特定する情報の削除または変更のいずれかを含む保護措置の 1 つである。その例には、特定の個人の特定が不可能であることを確実にするため、画像をぼやかして顔を隠したり、集計された統計として結果を報告することが含まれる。

仮名化には、ID 番号などの固有の識別子の使用やハッシュアルゴリズムにより、データセット内で個人特定が依然として可能である方法で個人データを変更する一方、確認の目的で個人データを分離して保持することが含まれる（Q9 参照）。

このような手法を採用する際、調査者は、このようなデータの匿名化／仮名化に関する法的基準を満たすために、どの要素を削除すべきかを判断するため、国内法および自主規制の行動規範を調べるべきである。

7 参考文献

ディーエルエイ・パイパー社、Data Protection Laws of the World

EphMRA Adverse Event Reporting Guidelines 2014

ICC／ESOMAR 市場および社会調査における国際行動規範

ESOMAR 青少年へのインタビューに関するガイドライン

ISO 26362:2009（市場、意見及び社会調査におけるアクセスパネル）

ISO 20252（市場・世論・社会調査）

OECD プライバシー原則

8 プロジェクトチーム

共同主催者：

- レグ・ベーカー（Reg Baker）、ESOMAR 職業基準委員会コンサルタント、Marketing Research Institute International
- デイヴィッド・スターク（David Stark）、ヴァイスプレジデント（統合、コンプライアンスおよびプライバシー）、GfK

プロジェクトチームメンバー：

- デブラ・ハーディング（Debrah Harding）、マネージングディレクター、Market Research Society
- スティーブン・ジェンカ（Stephen Jenke）、コンサルタント
- キャシー・ジョー（Kathy Joe）、ディレクター（国際基準およびパブリックアフェアー）、ESOMAR
- ヴァンダ・メイヤー（Wander Meijer）、グローバル COO、MRops
- アシュリン・クアーク（Ashlin Quirk,）、法務顧問、SSI
- バリー・ライアン（Barry Ryan）ディレクター（ポリシー・ユニット）、Market Research Society
- ジェイン・ファン・サウウェ（Jayne Van Souwe）、プリンシパル、Wallis Consulting Group

ESOMAR は、世界における市場調査の
推進、発展、および向上を目的とする
主要機関です。

www.esomar.org