ESOMAR
WORLD RESEARCH

World Research Codes and Guidelines

CHECKLISTE FÜR DEN DATENSCHUTZ

ESOMAR, the World Association for Social, Opinion and Market Research, gathers around 4900 members in over 130 countries and is the essential organisation for encouraging, advancing and elevating market research. Codes and guidelines are available at www.esomar.org

INHALTSVERZEICHNIS

1 EINLEITUNG

Weltweit arbeitende Markt- und Sozialforscher sehen sich zunehmend mit unterschiedlichsten gesetzlichen Bestimmungen zum Schutz der Privatsphäre und der persönlichen Daten konfrontiert. Sie haben die Verantwortung, nicht nur die Gesetze des Landes zu prüfen und einzuhalten, in dem sie tätig sind, sondern auch die Datenschutzerfordernisse all der Länder zu beachten, in denen sie Marktforschung durchführen und / oder Daten verarbeiten.

Gleichzeitig hat die ständig weitere Verbreitung neuer Technologien in alle Aspekte unseres Lebens nicht nur die potenziell den Forschern zur Verfügung stehende Datenmenge vergrößert, sondern sie führt auch zu völlig neuartigen personenbezogenen Daten, die zu schützen sind.

Dabei hat sich eine Sache nicht verändert, nämlich die Notwendigkeit, dass Marktforscher den Ruf der Markt-, Sozial- und Meinungsforschung schützen müssen. Dazu sind Vorgehensweisen erforderlich, welche die Transparenz gegenüber den Interviewpartnern und den Kunden sicherstellen, das Vertrauen in die von den Marktforschern gegebenen Informationen fördern und die zeigen, dass die Belange der Forschungsteilnehmer berücksichtigt werden.

2 ZIELSETZUNG

Das Ziel dieses Dokuments ist es, den Marktforschern generelle Empfehlungen zu ihrer Verantwortung bezüglich eines weltweit gültigen Rahmens von Datenschutzanforderungen an die Hand zu geben, damit die Forschungsteilnehmer die Kontrolle über ihre Daten behalten. Dabei werden insbesondere Marktforscher angesprochen, welche in kleineren Organisationen tätig sind, die über keine großen Ressourcen oder Erfahrungen im internationalen Datenschutz verfügen. Der hier verwendete Rahmen wurde von der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (Organisation for Economic Co-Operation and Development, OECD) entwickelt. Er beinhaltet ein Set von acht Prinzipien zur Ausgestaltung von Programmen zum Schutz der Privatsphäre und der personenbezogener Daten. Diese Prinzipien sind:

- Begrenzung der Datenerhebung
- Datenqualität
- Zweckorientierung
- Nutzenbegrenzung
- Sicherheitsvorkehrungen
- Transparenz
- Individuelle Teilhabe
- Verantwortlichkeit

Diese allgemeinen Prinzipien finden sich in den meisten der weltweit existierenden oder in Vorbereitung befindlichen Gesetze weltweit zum Schutz der Privatsphäre und der persönlichen Daten.

Marktforscher sollten jedoch beachten, dass die OECD-Prinzipien am engsten mit den Datenschutzanforderungen in der EU verbunden sind. Marktforschern, die in anderen Regionen tätig sind, wird deshalb empfohlen, andere möglicherweise relevante Regelwerke zu prüfen. Dazu gehören das Rahmenwerk zum Schutz der Privatsphäre (Privacy Framework) der Asia-Pacific-Co-operation (APEC), die US-amerikanischen Safe Harbour Prinzipien zum Schutz der Privatsphäre (Privacy Principles) und die „Allgemein Akzeptierten Prinzipien zum Schutz der Privatsphäre“ (Generally Accepted Privacy Principles, GAPP), die von dem US-amerikanischem AICPA-Institut und dem kanadischen Institut CICA entwickelt wurden. Obwohl diese Regelwerke allgemein keine Gesetzeskraft haben, so definieren sie doch die Grundprinzipien, die Forscher beachten müssen, wenn sie in der betreffenden Region arbeiten.

Zusätzlich müssen Marktforscher die Gesetze und die Selbstregulierungsregeln zum Datenschutz in jedem Land überprüfen und beachten, in dem sie Daten erheben oder

verarbeiten wollen, da die Grundprinzipien in den einzelnen Ländern unterschiedlich angewendet werden können. Die in diesem Papier zur Verfügung gestellten Leitlinien stellen einen Minimalstandard dar und müssen gegebenenfalls bei bestimmten Forschungsprojekten durch zusätzliche Maßnahmen ergänzt werden. Es kann daher für Marktforscher notwendig werden, sich juristischen Rat aus dem Land zu holen, in dem die Marktforschung stattfinden soll, damit die vollständige Einhaltung aller Regeln sichergestellt werden kann. Dabei kann auch eine online-Recherche bei „The Data Protection Laws of the World“ hilfreich sein, die von DLA Piper betrieben und jährlich aktualisiert wird.

Schließlich kann es für in Spezialgebieten tätigen Marktforscher sinnvoll sein, spezielle Richtlinien zu Rate zu ziehen. Ein Beispiel sind die „EphMRA Adverse Event Reporting Guidelines 2014“ im Bereich der Gesundheitsforschung.

3 BEDEUTUNG VON „MUSS“ BZW. „DARF NICHT“ UND „SOLL“

In diesem Dokument wird „muss“ bzw. „darf nicht“ zur Bezeichnung von verpflichtenden Erfordernissen verwendet. „Muss“ bzw. „darf nicht“ wird verwendet, wenn ein Prinzip oder eine Vorgehensweise beschrieben wird, die Forscher beachten müssen, um dem „ICC/ESOMAR internationale Kodex für Markt- und Sozialforschung“ zu genügen. Das Wort „soll“ wird verwendet, wenn die Umsetzung der Prinzipien beschrieben wird. Dadurch soll berücksichtigt werden, dass Marktforscher abhängig vom Forschungsdesign eine Regel auf unterschiedliche Art und Weise umsetzen können.

4 DEFINITIONEN

Business-to-business Forschung (B2B) bezeichnet die Erhebung von Daten über rechtliche Einheiten wie Unternehmen, Schulen, Non-Profit Organisationen usw.

Business-to-consumer Forschung (B2C) bezeichnet die Erhebung von Daten von Einzelpersonen.

Zustimmung bedeutet die freiwillige und informierte Einwilligung einer Person zur Sammlung und Verarbeitung ihrer personenbezogenen Daten. In der Markt-, Sozial- und Meinungsforschung basiert diese Zustimmung darauf, dass die Forschungsteilnehmer über die Art der gesammelten Daten, die Zwecke, für die diese verwendet werden und die Identität der Person oder Organisation, welche die personenbezogenen Daten hält, verständlich informiert werden. Der Forschungsteilnehmer kann seine Zustimmung jederzeit widerrufen.

Verantwortliche Stelle ist die Person oder Organisation, die bestimmt, wie personenbezogene Daten verarbeitet werden. So ist beispielsweise ein Forschungskunde die verantwortliche Stelle für die Daten seiner Kunden, eine Sozialbehörde für die Daten der Empfänger ihrer Sozialleistungen, ein Betreiber eines Online-Panels für die Daten der Mitglieder dieses Panels und ein Forschungsinstitut für die von den Teilnehmern einer Omnibusbefragung gesammelten Daten.

Datenverarbeiter bezeichnet eine Stelle, die von einer verantwortlichen Stelle personenbezogene Daten erhält und diese für die verantwortliche Stelle und nach deren Anweisungen speichert, weiter verarbeitet und / oder analysiert. Wie bereits oben erwähnt, ist ein Forschungsinstitut, das eine Omnibusumfrage durchführt, gleichzeitig verantwortliche Stelle und Datenverarbeiter.

Gesetze zum Schutz der Privatsphäre sind nationale Gesetze oder Regulierungen, deren Durchsetzung personenbezogene Daten im Sinne dieses Dokuments schützt.

Marktforschung, einschließlich Sozial- und Meinungsforschung, ist die systematische Erhebung und Auswerten von Informationen über Personen oder Organisationen mit Hilfe der statistischen und analytischen Methoden und Techniken der angewandten Sozialwissenschaften, um Einsicht zu gewinnen oder das Treffen von Entscheidungen zu unterstützen. Die Identität der Befragten wird gegenüber dem Nutzer der Information ohne ausdrückliche Zustimmung nicht enthüllt, und es werden keine Verkaufsmethoden ihnen gegenüber angewendet als unmittelbare Folge der von ihnen gegebenen Informationen.

Passive Datenerhebung bedeutet die Erhebung von Daten, ohne dass wie im traditionellen Interview Fragen gestellt und beantwortet werden.

Personenbezogene Daten sind alle Informationen, die einer identifizierten oder identifizierbaren natürlichen Person (wie einer Privatperson im Gegensatz zu einer Firma oder einer ähnlichen Einheit) zugeordnet werden können. Identifizierbar ist eine Person dann, wenn sie direkt oder indirekt bestimmt werden kann, insbesondere durch eine Identifizierungsnummer oder ihre physischen, physiologischen, mentalen, ökonomischen, kulturellen und / oder sozialen Eigenschaften. Bei manchen Forschungsarten kann die Identifizierung auch durch Fotos, Video- oder Tonaufnahmen oder andere persönlichen Informationen, die im Laufe der Forschung erhoben wurden, möglich sein.

Verarbeitung personenbezogener Daten schließt u.a. ein die Sammlung, Aufnahme, Organisation, Speicherung , Anpassung oder Änderung, Abfrage, Erforschung, Nutzung, Weitergabe, Verbreitung oder anderweitiges zur Verfügung stellen, Zuordnung oder Kombination, Sperrung, Löschung oder Zerstörung. Dies kann automatisiert oder nicht automatisiert erfolgen.

Forschungsteilnehmer ist jeder, dessen personenbezogenen Daten in einem Forschungsprojekt gesammelt werden, sei es durch aktive oder passive Datenerhebung.

Marktforscher bezeichnet jedes Individuum und jede Organisation, die Marktforschung durchführt oder dabei beratend tätig ist, einschließlich der betreffenden Personen in der Kundenorganisation und der für die Forschung genutzten Unterauftragsnehmer wie z.B. Technologielieferanten.

Marktforschungskunde oder Datennutzer bezeichnet jedes Individuum oder jede Organisation, die ganz oder teilweise ein Forschungsprojekt nachfragt, in Auftrag gibt, finanziert oder bezieht.

Besonders sensible Daten sind alle personenbezogenen Informationen über die rassische oder ethnische Herkunft, die Gesundheit oder das Sexualleben, Informationen zu kriminellen Handlungen, zu religiösen oder philosophischen Überzeugungen oder zur Mitgliedschaft in einer Gewerkschaft. Es können weitere Informationen in bestimmten Rechtssystemen als besonders sensible Daten angesehen werden. So werden in den USA neben persönlichen Gesundheitsinformationen auch das Einkommen und andere Finanznformationen sowie die durch die Regierung herausgegebenen Dokumente zur finanziellen Identität als besonders sensibel erachtet.

Weitergabe von Daten bedeutet jede Offenlegung, Kommunikation, jedes Kopieren oder jeder Transfer von Daten von einer Stelle zu einer anderen, unabhängig vom genutzten Medium, u.a. Transfer der Daten in einem Netzwerk, durch physikalische Weitergabe von Datenträgern, Transfer von einem Gerät oder Medium zu einem anderen oder durch Fernzugriff auf die Daten.

Grenzüberschreitende Weitergabe personenbezogener Daten bedeutet die Weitergabe von Daten über nationale Grenzen hinweg, durch welches Mittel auch immer, einschließlich des Zugriffs auf die Daten von einem Land aus, in dem nicht die Erhebung der Daten erfolgte. Dies kann auch durch die Cloud-Technologie erfolgen.

5 CHECKLISTE ZUR SELBSTÜBERPRÜFUNG VON DATENSCHUTZREGELN UND –PROZEDUREN

Die Anwender der folgenden Checkliste werden möglicherweise feststellen, dass die Überschriften und ihre Anordnung nicht mit dem zugrunde liegenden OECD Dokument übereinstimmen. Die dahinter stehende Absicht ist es, die Prinzipien in einer Sprache und in einer Anordnung darzustellen, die Marktforschern eher vertraut ist. Die Nutzer können auch feststellen, dass die einzelnen Punkte zueinander in Beziehung stehen und sich teilweise überlappen. **Dennoch ist es wesentlich, dass die Checkliste insgesamt betrachtet wird und einzelne Punkte eher als sich ergänzend denn als sich ausschließend gesehen werden. Dabei wird besondere Aufmerksamkeit auf die Unterschiede verwendet, die sich ergeben, je nachdem eine Organisation als verantwortliche Stelle oder als Datenverarbeiter agiert. Jede Frage, die nicht mit „ja“ beantwortet werden kann, signalisiert eine potenzielle Lücke im Datenschutzprogramm und daher ein potenzielles Risiko, dass ein oder mehrere Datenschutzgesetze verletzt werden.**

5.1 Minimale Auswirkungen

1. *Wurde beim Design des Forschungsprojekts die Erhebung personenbezogener Daten auf die Daten beschränkt, die zur Beantwortung der Forschungsfrage erforderlich sind? Wurde sichergestellt, dass die erhobenen Daten nicht in irgendeiner Art und Weise verwendet werden, die durch den Forschungszweck nicht gedeckt ist?*

Marktforscher dürfen nur solche personenbezogene Daten erheben und halten, mit denen sichergestellt werden kann, dass eine bestimmte Person befragt wurde und die für die Qualitäts-, Stichprobenkontrolle und / oder für Analysezwecke erforderlich sind. Bei B2B-Forschung beinhaltet das auch personenbezogene Daten zur Stellung oder Führungsebene des Teilnehmers im Unternehmen, da dies für den Forschungszweck erforderlich sein kann.

Der gleiche Grundsatz gilt bei passiven Datenerhebungsmethoden, bei denen personenbezogene Daten auch ohne die traditionelle Form von Frage und Antwort im Interview erhoben werden. Daher ist es in der Verantwortung des Marktforschers sicherzustellen, dass nur solche Daten erhoben werden, die für den Forschungszeck erforderlich sind. Wenn weitere personenbezogene Daten empfangen werden, so müssen diese herausgefiltert und gelöscht werden.

2. *Sind Verfahren eingeführt, die sicherstellen, dass die Forschungsteilnehmer keinen Schaden oder negative Konsequenzen als direkte Folge ihrer Teilnahme an einem Marktforschungsprojekt erleiden?*

Der Forscher muss sicherstellen, dass auch nicht durch geschickte Kreuztabellierung, das Herunterbrechen auf kleinste Stichproben oder auf andere Weise aus den Forschungsdaten die Identität einer Einzelperson ermittelt werden kann. Beispiele sind auch das Zuspielen von Hilfsinformationen wie z.B. ein geografisches Gebiet oder die Möglichkeit einen ganz bestimmten Angestellten in einer Kundenzufriedenheitsstudie zu identifizieren.

3. *Wird beim Einsatz von Unterauftragnehmern oder sonstigen Dienstleistern sichergestellt, dass nur so die personenbezogenen Daten weitergegeben werden, welche zur Erfüllung ihrer Aufgaben notwendig sind? Gibt es vertragliche Vereinbarungen, die ein vergleichbares Datenschutzniveau bei ihnen sicherstellen?*

Wenn ein Unterauftragnehmer genutzt wird, dann darf dieser nur solche personenbezogene Daten erhalten, die zur Erfüllung seines Auftrags erforderlich sind. Dabei muss vertraglich und durch klare Instruktionen die Verantwortung kommuniziert werden, welche die Unterauftragnehmer haben, solange sie im Besitz der Daten sind. Alle Unterauftragnehmer müssen den gleichen Regeln und Bestimmungen folgen wie die Forschungsorganisation selbst. Personenbezogene Daten dürfen nicht ohne die vorherige Zustimmung oder Beauftragung durch den Forschungskunden an Unterauftragnehmer oder andere Dritte weitergegeben werden.

Dies setzt voraus, dass den Forschungsteilnehmern versichert wird, dass die Daten vertraulich erhoben und gehalten werden und nur in aggregierter Form analysiert und berichtet werden. Wenn die Forschungsteilnehmer die Einwilligung zur Weitergabe ihrer personenbezogenen Daten geben, dann müssen sie darüber informiert werden, wer ihre Daten erhält und wie sie genutzt werden[1].

5.2 Information und Zustimmung

4. *Erteilt jede Teilnehmerr, dessen personenbezogenen Daten erhoben werden, dazu seine Zustimmung?*

Gemäß den OECD Prinzipien zum Schutz der Privatsphäre soll jedes personenbezogene Datum durch gesetzeskonforme und faire Methoden erheben werden und – soweit angemessen – mit dem Wissen und / oder der Zustimmung des Forschungsteilnehmers. In der Regel nennen nationale Gesetze eine Anzahl gesetzeskonformer und fairer Begründungen zur Datenerhebung. Meist hat der Marktforscher jedoch die Pflicht zur Einholung der Zustimmung.

[1] Anmerkung des Übersetzers: In Deutschland ist eine Weitergabe personenbezogener Daten an den Auftraggeber grundsätzlich verboten.

In manchen Fällen liegt die Verantwortung zur Einholung der Zustimmung bei anderen. Beispiele sind Panels, die durch einen Dritten zur Verfügung gestellt werden oder wenn eine Kundendatenbank genutzt wird. In diesen und ähnlichen Fällen muss sich der Marktforscher die Zusicherung einholen, dass die Zustimmung ordnungsgemäß erteilt wurde.

Die Zustimmung muss sein:

- Frei, d.h. freiwillig und jederzeit widerrufbar
- Spezifisch, d.h. sie bezieht sich auf einen oder mehrere definierte Erhebungszweck(e)
- Informiert, d.h. in vollem Bewusstsein aller relevanten Folgen einer gegebenen Zustimmung.

Die Zustimmung muss auch klar durch eine Erklärung oder Handlung des Forschungsteilnehmers ausgedrückt sein. Vorher muss der Forschungsteilnehmer entsprechend informiert sein. Zusammenfassend soll die Information die folgenden Punkte umfassen: (a) Wie die personenbezogenen Daten genutzt werden; (b) welche Daten erhoben werden; (c) der Name, die Adresse und die Kontaktinformationen der Stelle, welche die Daten erhebt und – sofern dieser abweicht – die verantwortliche Stelle und (d) ob die Daten Dritten zugänglich gemacht werden.

Forscher sollen sich sorgfältig überlegen, welche Methode der Zustimmung sie wählen. Diese werden in der Regel als „opt out“, „opt in“, implizit, informiert oder explizit bezeichnet. Die verwendete Methode soll dokumentiert werden.

Allgemein gilt: Je sensibler die erhobenen Daten sind, je aufdringlicher und je weniger offensichtlich die Datenerhebung stattfindet, desto höher ist die Anforderung, die an die Zustimmung zu stellen ist. In manchen Gesetzen wird für die Erhebung sensibler Daten die vorherige explizite Zustimmung durch die betroffenen Personen gefordert.

Es gibt Fälle, in denen Forscher personenbezogene Daten unabsichtlich erheben oder erhalten, oder sie bekommen Daten von Personen, die keine Forschungsteilnehmer sind. Beispiele sind u.a. Informationen, die Befragte von sich aus geben, vom Kunden zur Verfügung gestellte Listen mit mehr als der erforderlichen Information oder Personen, die zufällig auf Fotos oder Videos erfasst sind, jedoch keine Forschungsteilnehmer sind. Forscher sollten diese Informationen so behandeln wie andere personenbezogene Daten auch. Solche Daten sollten unverzüglich anonymisiert oder gelöscht werden. Dies gilt besonders, wenn die Personen, deren Daten erfasst wurden, über den Speicherort oder die Nutzung der Daten nicht informiert werden können. In manchen Gesetzen ist es verpflichtend, solche Daten zu löschen oder sie exakt so zu behandeln wie andere Informationen, die absichtlich erhoben wurden.

5. *Besteht Klarheit über den Zweck bzw. die Zwecke, für den bzw. für welche die Daten erhoben und gehalten werden?*

Die Marktforschungsbranche hat seit langem zwischen Marktforschung auf der einen Seite und der Datenerhebung für andere Zwecke wie Werbung, Verkaufsförderung, Adressgewinnung, Direktmarketing oder Direktverkauf auf der anderen Seite unterschieden. Diese Unterscheidung ist ein wichtiger Bestandteil zur Differenzierung der Zielsetzung und zur Förderung eines positiven Images bei Gesetzgebern, Behörden und der allgemeinen Öffentlichkeit. In den letzten Jahren stiegen die Möglichkeiten der Erhebung personenbezogener Daten durch das Aufkommen neuer Technologien wie z.B. Online-Tracking oder herunterladbare mobile Apps. In jedem Fall ist es wesentlich bevor irgendwelche Daten erhoben werden, dass die möglichen Forschungsteilnehmer über den Zweck bzw. die Zwecke informiert werden, die mit diesen Daten verfolgt werden und auch über mögliche Folgen einschließlich einem weiteren Kontakt zur Qualitätssicherung.

Wenn personenbezogene Daten zu Marktforschungszwecken erhoben werden, ist die Transparenz gegenüber dem Forschungsteilnehmer wichtig. Der Forschungsteilnehmer muss hinreichend über die beabsichtigte Nutzung und über jede etwaige Weitergabe der Daten informiert werden. Ist es beispielsweise beabsichtigt, die Antworten der Befragung mit einem Kundenprofil zu verknüpfen, dann sollte das dem Forschungsteilnehmer vor der Datenerhebung mitgeteilt werden.

Datenschutzerklärungen müssen regelmäßig daraufhin überprüft werden, ob sich die Arten der erhobenen Daten und ihre beabsichtigte Nutzung geändert haben. Es muss weiter sichergestellt sein, dass die eingegangenen Verpflichtungen noch den aktuellen Geschäftsabläufen, den in der Forschungsorganisation genutzten Technologien und den aktuellen gesetzlichen Erfordernissen entsprechen. Jede vorgeschlagene Nutzung personenbezogener Daten muss daraufhin analysiert werden, ob sie den Datenschutzgesetzen des jeweiligen Landes, dem ICC/ESOMAR Code, den ESOMAR Richtlinien sowie den Zusagen entsprechen, welche den Forschungsteilnehmern gemacht wurden.

6. *Besteht Klarheit über die Art der zu erhebenden Daten?*

Personenbezogene Daten sind in der Rechtsprechung teilweise sehr breit definiert. Daher ist es erforderlich, alle möglichen personenbezogenen Daten, die unter Umständen erhoben werden, bei der Abfassung der Teilnehmerinformation zu berücksichtigen. Personenbezogene Daten können u.a. folgendes beinhalten: Name, Adresse, Email-Adresse, Telefonnummer, Mobiltelefonnummer, Geburtstag, Identifikationsnummern von mobilen Geräten, IP-Adressen, Fotos, Ton- und Filmaufnahmen, von Behörden zugeteilte Identifikationsnummern wie Führerschein-, Ausweis- oder Sozialversicherungsnummern, von der Forschungsorganisation zugeteilte Teilnehmernummer, Nutzernamen von sozialen Medien sowie Daten, die einem Cookie oder in einem Tracking Pixel bzw. einer angehängten Datei gespeichert sind. Dabei ist auch zu berücksichtigen, dass ein einzelnes Datum u.U. noch kein personenbezogenes Datum gemäß den jeweiligen Gesetzen ist, dass es aber in Kombination mit anderen Daten (z.B. Postleitzahl, Geschlecht, Arbeitsstätte oder Schule, sowie Position und Gehalt) geeignet sein kann, eine bestimmte Person zu identifizieren.

Weiter sind alle Empfänger der personenbezogenen Daten zu berücksichtigen. Marktforscher, Forschungsorganisationen, dritte Dienstleister und / oder Endkunden können in der Lage sein, im Laufe eines Forschungsprojekts personenbezogene zu erheben oder zu nutzen.

7. *Wird deutlich gemacht, wie die Daten erhoben werden, einschließlich passiver Methoden, die dem Forschungsteilnehmer u.U. nicht bewusst sind?*

In der Vergangenheit war die Befragung die wichtigste Methode in der Marktforschung zur Erhebung personenbezogener Daten. Wie weiter oben unter 5. erwähnt, ermöglichen nun neue Technologien, ein breiteres Spektrum personenbezogener Daten zu erheben, ohne dass diejenigen, deren Daten erhoben werden, dies wissen. Alle Forschungsteilnehmer müssen über die Arten von personenbezogener Daten sowie die Methode(n) ihrer Erhebung informiert werden, sei es durch eine aktive Methode wie die Befragung oder passiv wie durch mobile Apps oder das Nachverfolgen des Verhaltens durch Online-Cookies.

Forscher sollten auch darüber berücksichtigen, welche Daten oder welche Datenerhebungsmethode vom Forschungsteilnehmer nicht vorhergesehen werden können und darüber herausgehoben informieren. Dies kann durch „Kurzinformationen“ geschehen, welche über längere Datenschutzerklärungen gelegt werden, und die möglicherweise nicht erwartete oder als zudringlich empfundene Datenerhebungen beschreiben. Mobile Anwendungen, besonders solche, die den Standort bestimmen, „passiv zuhören“ und / oder das Betriebssystem des mobilen Geräts erfassen: Dies alles erfordert eine detaillierte Beschreibung und die ausdrückliche Einwilligung des Forschungsteilnehmers.

5.3 Datenintegrität / -sicherheit

8. *Sind Prozesse eingerichtet, die sicherstellen, dass alle erhobenen personenbezogenen Daten richtig, vollständig und aktuell sind?*

Qualitätsprüfungen sollten auf jeder Stufe des Forschungsprozesses stattfinden. Wenn Fragebögen oder Forschungsanwendungen entwickelt werden, sind diese vor der Feldarbeit zu testen, um die Gefahr von Fehlern bei der Datenerhebung zu minimieren. Während der Feldarbeit sollten die Interviews gemäß den anzuwendenden Qualitätsstandards laufend geprüft und validiert werden. Auch während der Produktions- und Berichtsphase sollten zusätzliche Qualitätsüberprüfungen erfolgen, um sicherzustellen, dass die Daten richtig sind und dass die Analysen, Folgerungen und Empfehlungen durch die Daten gestützt werden.

Forschungsorganisationen, welche Panels betreiben, sollten sicherstellen, dass die Panelteilnehmer ihr Profil jederzeit prüfen und aktualisieren können und sie sollten sie regelmäßig daran erinnern, dies auch zu tun. Stichproben, die aus den Panels gezogen werden, sollten aktuelle soziodemografische Informationen beinhalten. Eine gute Quelle für standardmäßige Verfahren in dieser Hinsicht ist die ISO 26362:2009 – Access Panels in der Markt-, Meinungs- und Sozialforschung.

9. *Ist sichergestellt, dass personenbezogene Daten nicht länger aufbewahrt werden, als es zur Erreichung des Forschungszwecks, für den die Daten erhoben und verarbeitet wurden, erforderlich ist? Sind Prozesse installiert, die den Personenbezug der Daten separat speichern oder löschen, sobald dieser nicht mehr erforderlich ist?*

Forscher sollten die Datenspeicherungsfristen so kurz wie möglichfestsetzen. Auf jeden Fall müssen sie den gültigen Gesetzen entsprechen. Die Länge der Fristen hängt auch ab von der Datenquelle sowie davon, ob die Daten von der verantwortlichen Stelle oder einem Datenverarbeiter gehalten werden. In letzterem Fall kann es sein, dass die Kunden die Datenaufbewahrungsfristen vertraglich festsetzen.

Bezüglich der Quelle der personenbezogenen Daten werden die Daten von Längsschnittstudien oder die Profildaten der Panelteilnehmer üblicherweise so lange aufbewahrt, wie der Panelteilnehmer aktiv ist. Im Gegensatz dazu sollten die personenbezogenen Daten von Nicht-Panelteilnehmern, die an einer Ad Hoc Forschung teilnehmen, nur wesentlich kürzer aufbewahrt werden. Dennoch ist es auch hier wichtig, die Daten nicht zu schnell zu löschen, weil während der Datenverarbeitung die Qualitätsprüfungen vorgenommen werden müssen, um die Genauigkeit und die Integrität der Daten gemäß den Datenschutzregeln sicherzustellen.

Bei der Verwendung personenbezogener Daten ist es ein bewährtes Verfahren, pseudonymisierte Identifikationsnummern zu verwenden. Die Stammdatei, welche die Namen, Adressen und / oder Telefonnummern mit der entsprechenden internen Identifikationsnummer verbindet, muss sicher gespeichert werden und es dürfen nur wenige Personen Zugang zu ihr haben, z.B. die mit der Stichprobenziehung oder dem Panelmanagement betrauten Personen. Auf diese Weise können Forscher, Datenverarbeiter und Codierer die Daten auf der Ebene der Panelteilnehmer analysieren, ohne die Namen, Adressen oder Telefonnummern der Teilnehmer zu sehen.

Wenn die Erhebungsdaten verarbeitet und als aggregierte, statistische Daten berichtet worden sind, sollten die personenbezogenen Daten der Teilnehmer zusammen mit den pseudonymisierten Identifikationsnummern gelöscht werden, so dass die Organisation keinerlei personenbezogene Daten mehr gespeichert hat.

10. *Sind Prozesse eingerichtet, mit denen Anfragen von Einzelpersonen zu den möglicherweise über sie erhobenen personenbezogenen Daten beantwortet werden können? Beinhalten diese Prozesse auch Verfahren zur Feststellung der Identität der anfragenden Personen? Sehen diese Verfahren eine angemessene Reaktionszeit vor, die es erlaubt, falsche Daten zu korrigieren oder zu löschen?*

Es sollten formelle Verfahren entwickelt, eingerichtet und kommuniziert werden, mit denen Personen geantwortet werden kann, die Zugang zu den über sie bei der Organisation gespeicherten personenbezogenen Daten wünschen. Dabei ist es wichtig, die Identität der anfragenden Personen zu überprüfen, damit nicht personenbezogener Daten anderer Personen an sie kommuniziert werden.

Sobald die Identität der anfragenden Person als zutreffend festgestellt wurde und diese Person ein gesetzliches Recht hat, die angefragten Daten zu erhalten, sollen sich Forscher bemühen, die Anfrage so schnell wie möglich zu beantworten, z.B. abhängig von den jeweils gültigen Gesetzen innerhalb von 10 bis 30 Tagen. Wenn das Forschungsinstitut dazu länger braucht, ist u.U. eine Fristverlängerung möglich, wenn dies zusammen mit nachvollziehbaren Begründungen kommuniziert wird. So kann zusätzliche Zeit erforderlich sein für Nachfragen oder wenn die Daten auf unterschiedlichen Datenbanken verteilt sind.

Obwohl Datenschutzgesetze Ausnahmen vorsehen können, bei denen die Organisation sich weigern muss, die personenbezogenen Daten der betreffenden Person zugänglich zu machen, sind diese Ausnahmen für zu Marktforschungszwecken erhobenen personenbezogene Daten in der Regel nicht zutreffend. So kann es sein, dass das

zutreffende Gesetz es Organisationen erlaubt, den Zugang zu Daten zu verweigern, die unter die Beziehung zwischen Anwalt und Mandant fallen. Ein weiteres Beispiel ist, dass die Organisation die Daten an eine Strafverfolgungs- oder Sicherheitsbehörde weitergegeben hat. Hier kann es sein, dass die Behörde anweist, die Daten und / oder die Tatsache ihrer Weitergabe geheim zu halten.

11. *Gibt es für jeden Datenbestand Sicherheitsprotokolle, welche vor der Gefahr des Verlusts, des unberechtigten Zugangs, der Nutzung, Veränderung oder Veröffentlichung schützen?*

Die Erfüllung dieser Verantwortung beginnt mit der Entwicklung und der Implementierung eine Sicherheitsstrategie zum Schutz personenbezogener und sonstiger vertraulicher Daten. Ein anerkannter Sicherheitsstandard auf dem eine gründliche Sicherheitsstrategie aufgebaut werden kann, ist die ISO 27001.

Die notwendigen Sicherheitsvorkehrungen beinhalten u.a.:

- Physische Maßnahmen wie abgeschlossene Archive, Zugangsbeschränkungen für bestimmte Büros, Alarmsysteme, Videoüberwachung
- EDV-technische Maßnahmen wie Passwörter, Verschlüsselung und Firewalls
- Organisatorische Maßnahmen wie Hintergrundüberprüfungen, Regeln zur Mitnahme von Computern vom Arbeitsplatz, Beschränkung des Zugangs auf die notwendigen Informationen, Ausbildungsmaßnahmen und Vereinbarungen mit Kunden und Auftragnehmern.

Die Sicherheitsstrategie soll auch vorschreiben, wie nach einer möglichen Verletzung des Datenschutzes personenbezogener Daten vorgegangen wird. Wenn die Daten durch eine andere Stelle erhoben und zur Verfügung gestellt wurden, ist diese unverzüglich zu informieren. Teilnehmer, deren Daten offengelegt wurden, müssen ebenfalls benachrichtig werden, wenn die Offenlegung für sie ein gewisses Risiko darstellt (z.B. Identitätsdiebstahl). Weiter müssen geeignete Maßnahmen ergriffen werden, um gegen dieses Risiko zu schützen.

12. *Gibt es eine klare Erklärung, wie lange personenbezogene Daten aufbewahrt werden?*

Wie schon in der Antwort auf Frage 9 dargelegt, kann sich die Dauer, in der personenbezogene Daten aufbewahrt werden, je nach Forschungsprojekt abhängig von einer Reihe von Einflussgrößen unterscheiden.

Obwohl es sinnvoll ist, generelle Informationen zu den Aufbewahrungsfristen in die Datenschutzerklärung mit aufzunehmen, kann es manchmal unpraktikabel sein, exakte Aufbewahrungsfristen für verschiedene Studienarten zu kommunizieren. Daher sollte geprüft werden, ob Datenhaltungsfristen in die Informationen einbezogen werden können, die bei der Teilnehmerrekrutierung, bei der Einleitung zum Fragebogen oder bei der Zustimmungserklärung der jeweiligen Studie verwendet werden. In jedem Fall sollte die Forschungsorganisation darauf vorbereitet sein, auf Nachfrage die Datenhaltungsfristen eines jeden Projekts mitteilen zu können.

5.4 Weitergabe von Daten

13. *Gibt es definierte Regeln und Vorgehensweise zur Nutzung und Offenlegung personenbezogener Daten?*

In den Datenschutzgesetzen des jeweiligen Landes sind die Regeln und Vorgehensweisen klar umrissen. Die Bedeutung dieser Regeln sollte mit den daraus folgenden Vorgehensweisen schriftlich verständlich erklärt sein, so dass sichergestellt ist, dass das Personal die für die Handhabung personenbezogener Daten richtigen Regeln und Vorgehensweisen einrichten kann und auch damit vertraut ist. Diese werden z.B. auch beinhalten, dass prinzipiell die Zustimmung des Befragten erforderlich ist, bevor solche Daten

weitergegeben werden. Dies gilt auch für die Weitergabe an Kunden und Forscher beim Kunden[2].

14. *Sind die Bedingungen, unter denen personenbezogene Daten weitergeben werden, klar und unzweideutig?*

Forschungsteilnehmer müssen wissen, was mit ihren personenbezogenen Daten geschieht, und dies muss entweder mündlich erläutert werden oder mit einem Schriftstück, dem die Forschungsteilnehmer zugestimmt haben. Diese Zustimmung ist zu Beweiszwecken zu dokumentieren.

15. *Ist das Personal sich dieser Regeln bewusst und ist es ausgebildet, diese Regeln richtig anzuwenden?*

Die Datenschutzstrategie beschreibt die Vorgehensweise des Unternehmens bei der Erhebung und Verarbeitung von Daten. Es ist ebenso wichtig, standardisierte Vorgehensweisen zu entwickeln, damit sichergestellt wird, dass die Datenschutzzusagen, welche den Teilnehmern gemacht werden, auch eingehalten werden.

Die Ausbildung des Personals zum Datenschutz sollte einen Überblick über die einschlägigen Gesetze, die Standesregeln, die firmeneigenen Datenschutzregeln sowie die diesbezüglichen Standardprozeduren beinhalten. Diese Trainings sollt mindestens einmal pro Jahr wiederholt werden. Die Teilnahme soll dokumentiert werden.

Die Personen, die mit den Teilnehmern in direktem Kontakt stehen, sollten die Richtlinien und die Vorgehensweise ihres Unternehmens überblicksweise erklären können. Sie sollten auch wissen, bei wem sie nachfragen können, wenn sie mit Fragen konfrontiert werden, die sie nicht beantworten können.

Die Aufsichtspflicht und die Verantwortlichkeit sollten klar definiert sein. Darüber hinaus ist muss es eine gewisse Kontrolle geben, dass die definierten Vorgehensweisen auch befolgt werden.

5.5 Grenzüberschreitende Übertragung personenbezogener Daten

16. *Ist bei einer Übertragung personenbezogener Daten von dem Gebiet einer Rechtsordnung in das Gebiet einer anderen Rechtsordnung gewährleistet, dass die Anforderungen an den Datenschutz beider Rechtsordunen (Quelle und Ziel) erfüllt werden?*

Ein solcher Datentransfer wird häufig als „grenzüberschreitende Übermittlung personenbezogener Daten“ bezeichnet. Solches geschieht, wenn die Daten über Grenzen hinweg erhoben werden oder wenn die Verarbeitung der Daten in einem anderen Land stattfindet als dem, in dem sie erhoben wurden. Ein Beispiel dafür ist, wenn ein Unternehmen einen in einem anderen Land ansässigen Marktforscher beauftragt und ihm dazu seine Kunden- oder Nutzerdaten zur Verfügung stellt. Jedes Land hat seine eigenen Regeln, wie solche Daten behandelt und geschützt werden müssen. Marktforscher müssen diese Regeln befolgen. Obwohl dies zunächst als schwierig erscheinen mag, so hilft es doch, wenn man sich vergegenwärtigt, dass die zu beachtenden Regeln in drei Themen behandelt werden können:

- Es muss sichergestellt sein, dass die grenzüberschreitende Datenübertragung den gültigen nationalen Gesetzen entspricht. Die üblichsten Voraussetzungen, um einen angemessenen Datenschutz für den grenzüberschreitenden Datentransfer zu gewährleisten, ist entweder die Zustimmung der Betroffenen oder die Nutzung geeigneter vertraglicher Bestimmungen und, soweit von den gültigen Gesetzen gefordert, die vorherige Genehmigung durch die nationale Datenschutzbehörde oder einer anderen für den Datenschutz zuständigen Behörde zu diesen vertraglichen Bestimmungen. Als zusätzliche Sicherheitsmaßnahme sollten soweit möglich vor der Übertragung der Personenbezug der Daten entfernt werden, so dass nur eine pseudonymisierte Identifikationsnummer die individuellen Daten mit der jeweiligen Identität der Befragten verbindet.

[2] Anmerkung des Übersetzers: In Deutschland ist es aufgrund der Standesregeln der deutschen Verbände, die auch von ESOMAR anerkannt sind, grundsätzlich verboten, personenbezogene Daten an Kunden weiterzugeben.

- Es kann Beschränkungen für Datenverarbeiter geben, die nicht die verantwortliche Stelle sind, z.B. wenn sie eine Studie durchführen und dabei vom Kunden zur Verfügung gestellte Stichproben nutzen. Selbst wenn der Marktforscher sichergestellt hat, dass die grenzüberschreitende Übertragung alle Regeln für einen solchen Datentransfer erfüllt, sollten er sich dennoch bewusst sein, dass er als Datenverarbeiter, der im Auftrag einer verantwortlichen Stelle (z.B. dem Marktforschungskunden) tätig ist, die personenbezogenen Daten u.U. nicht übertragen darf, weil die verantwortliche Stelle dies nicht erlauben kann. Dies kann die Art und Weise beeinflussen, in der das Projekt durchgeführt wird. Darüber sollte es zwischen den beiden Parteien eine schriftliche Vereinbarung geben.
- Grenzüberschreitende Übertragung personenbezogener Daten kann schon bei der Datenerhebung erfolgen, z.B. dann wenn bei einer Online-Umfrage Daten von Forschungsteilnehmern aus mindesten einem anderen Land als dem Land des verantwortlichen Marktforschers erhoben werden. Das anzuwendende Datenschutzgesetz ist normalerweise das Gesetz des Landes, in dem der Marktforscher ansässig ist. Der Marktforscher muss jedoch sicherstellen, dass er auch die nationalen Gesetze all der Länder beachtet, in denen er Daten erhebt. Es wird empfohlen, dass (1) die Identität der forschenden Stelle (Firmenname, Postadresse etc.) einschließlich dem Land in den Anwerbungsunterlagen klar kommuniziert wird und (2) dass die online einsehbaren Datenschutzrichtlinien eine einfache und klare Bestimmung zu grenzüberschreitenden Datenübertragungen enthält, die bei der Studie angewendet werden, und (3) dass auch die bei der Panelanwerbung eingeholte Einwilligungserklärung einen Bezug zum grenzüberschreitenden Datenverkehr enthält.

5.6 Outsourcing und Untervergabe

17. *Gibt es klare Anforderungen einschließlich angemessener Aufsicht für jeden externen Datenverarbeiter oder anderen Unterauftragsnehmer?*

Wenn Daten, in welcher Form auch immer, an dritte Datenverarbeiter oder Unterauftragnehmer übertragen werden, muss es klare Anforderungen bezüglich der Regeln zum Schutz personenbezogener Daten geben, die an diese kommuniziert werden. Weitere Schutzmaßnahmen beim Transfer von Daten – seien sie personenbezogen oder aggregiert – wie die Nutzung bestimmter IT-Verfahren wie Verschlüsselung oder die Nutzung von FTP-Servern, sollten vorgesehen werden. Wenn irgendwelche Datenkopien als Backup bei Unterauftragnehmern oder außerhalb der Datenverarbeiter erstellt werden müssen, dann muss es klar definierte Prozesse geben, wie diese Daten während der Zeit, in der sie gespeichert sind, zu schützen sind und dass sie gelöscht werden müssen, sobald sie nicht mehr gebraucht werden.

5.7 Datenschutzpolitik

18. *Sind die Informationen über ihr Programm zum Schutz der Privatsphäre und der personenbezogenen Daten einfach und für die Forschungsteilnehmer leicht verständlich verfügbar?*

Viele Rechtssysteme erfordern, dass die Datenschutzregeln in einer für Forschungsteilnehmer leicht verständlichen Form verfügbar sind. Obwohl der erforderliche Inhalt je nach Land variiert, müssen sich die forschenden Stellen immer klar identifizieren und sie müssen dem Forschungsteilnehmern erläutern, welchem Zweck die Forschung dient, wie die personenbezogenen Daten erhoben und wie sie verarbeitet werden (gespeichert, genutzt, wie auf sie zugegriffen wird und wem sie zugänglich gemacht werden), wie weitergehende Informationen erlangt werden können und wie eine Beschwerde erfolgen kann.

Marktforscher müssen sicherstellen, dass ihre Datenschutzregeln leicht verständlich, für den Leser relevant, einfach zu finden, so kurz gefasst wie möglich und auf die Vorgehensweise der Firma zugeschnitten sind. Das beinhaltet, dass sie in möglichst vielen Sprachen zur Verfügung gestellt werden und dass sie regelmäßig überprüft und ggf. aktualisiert werden.

19. *Ist die Identität und die Verantwortlichkeit der verantwortlichen Stelle klar?*

Marktforscher müssen sicherstellen, dass ihre eigene Rolle und Verantwortlichkeiten für den Umgang mit personenbezogenen Daten den Forschungsteilnehmern transparent sind. Das beinhaltet, dass die verantwortliche Stelle benannt wird und dass offengelegt wird, ob ein

externer Datenverarbeiter genutzt wird. Die Teilnehmer dürfen nicht darüber im Unklaren gelassen werden, welche Stelle letztlich für den Umgang mit ihren Daten verantwortlich ist.

Manche nationalen Gesetze sehen es auch vor, dass eine bestimmte Person genannt werden muss, die für den Datenschutz im Unternehmen verantwortlich ist.

In den Fällen, in denen die Stichprobe vom Kunden zur Verfügung gestellt wurde und der Auftraggeber der Studie nicht genannt werden soll, weil dies eine Verzerrung der Ergebnisse zur Folge haben könnte, muss dem Teilnehmer zu Beginn des Interviews gesagt werden, dass der Name des Marktforschungskunden erst nach dem Ende des Interviews mitgeteilt wird. Da jedoch die Datenschutzgesetze vieler Länder bestimmen, dass die Teilnehmer ein gesetzliches Recht haben zu erfahren, wer ihre personenbezogene Daten weitergegeben hat, müssen sich die Marktforscher darauf einstellen, jederzeit auf Verlangen den Namen des Kunden mitzuteilen.

20. *Ist klar, dass die verantwortliche Stelle für die unter ihrer Kontrolle stehenden personenbezogenen Daten verantwortlich ist, ganz egal wo diese gespeichert sind?*

Wenn Marktforscher evtl. Teile der Datenverarbeitung an Unterauftragnehmer vergeben oder personenbezogene Daten an Stellen außerhalb ihres Landes übertragen, sollen sie der verantwortlichen Stelle die Details der vertraglichen Gestaltung sowie der Orte der Datenverarbeitung mitteilen können. Soweit erforderlich sollten sie auch die vorherige schriftliche Zustimmung der verantwortlichen Stelle einholen. Wenn das Marktforschungsunternehmen auch die verantwortliche Stelle ist, sollten sie in ihren Datenschutzerklärungen auf die Nutzung von externen Datenverarbeitern hinweisen und, wenn erforderlich, die betreffenden Länder oder Regionen auflisten. Marktforscher sollten sich der Tatsache bewusst sein, dass es manche Landesgesetze verbieten, Daten in Länder oder Regionen zu übertragen, die ein geringeres gesetzliches Datenschutzniveau aufweisen. Wenn der grenzüberschreitende Datentransfer innerhalb eines multinationalen Unternehmens stattfindet, dann ist dieser durch die meisten Landesgesetze gedeckt, auch wenn manche Gesetze es erfordern, dass die Inhaber der Daten darüber informiert werden, wo ihre Daten gespeichert sind.

6 SPEZIALPROBLEME

6.1 Erhebung von Daten von Kindern

Die vom Gesetzgeber definierten Altersgrenzen, ab denen keine Einwilligung der Eltern mehr erforderlich ist, variieren zwischen den Ländern erheblich. Marktforscher müssen die für das Land der Datenerhebung zuständigen Gesetze und Standesregeln daraufhin prüfen, ob die Zustimmung der Eltern erforderlich ist. Auch ist zu beachten, dass u.U. kulturell begründete Sensibilitäten eine besondere Vorgehensweise erfordern. Wenn es keine nationalen Regeln gilt, dann sollte die ESOMAR Richtlinie „Interviewing Children and Young People“ herangezogen werden.

Datenerhebung bei Kindern erfordert die nachprüfbare Erlaubnis des gesetzlichen Vertreters. Der Elternteil oder der gesetzliche Vertreter muss ausreichend über das Forschungsprojekt informiert werden, so dass er oder sie eine informierte Entscheidung über die Teilnahme des Kindes treffen kann. Der Marktforscher sollte die Identität des gesetzlichen Vertreters sowie die Art der Beziehung zum Kind aufzeichnen.

6.2 Business-to-Business Forschung

Viele Forschungsprojekte beschäftigen sich mit der Datenerhebung bei rechtlichen Einheiten wie Unternehmen, Schulen, Non-profit und ähnlichen Organisationen. Diese Forschung beinhaltet oft auch Daten wie den Umsatz, die Zahl der Beschäftigten, den Wirtschaftszweig oder den Sitz der Organisation.

Auf jeden Fall haben die teilnehmenden Organisationen das Recht auf das gleiche Niveau zum Schutz ihrer Identität wie ihn Einzelpersonen bei anderen Forschungsarten genießen.

Es ist sinnvoll sich zu vergegenwärtigen, dass in vielen nationalen Datenschutzgesetzen die Funktion und die Kontaktdaten am Arbeitsplatz als personenbezogene Daten gelten. Manche Datenschutzgesetze gehen so weit, dass sie alle Anforderungen in gleicher Weise auf

natürliche und auf juristische Personen, d.h. auf Einzelpersonen und auf rechtliche Einheiten anwenden.

6.3 Fotos, Ton- und Filmaufnahmen

Es gibt eine Reihe von Forschungsmethoden, bei denen Fotos, Ton- und / oder Filmaufnehmen erzeugt, gespeichert und weitergegeben werden. Zwei wichtige Beispiele sind die Ethnografie und das Mystery Shopping.

Marktforscher müssen sich der Tatsache bewusst sein, dass Fotos, Ton- und Filmaufnahmen personenbezogene Daten sind und als solche zu behandeln sind. Wenn Marktforscher Forschungsteilnehmer bitten, Informationen in dieser Form zur Verfügung zu stellen, sollten sie zugleich dazu Hinweise geben, wie die Erhebung nicht gewünschter Daten reduziert werden kann, besonders von Personen, die keine Forschungsteilnehmer sind.

Schließlich können bestimmte Arten der beobachtenden Forschung es erforderlich machen, dass Fotos, Ton- oder Filmaufnahmen im öffentlichen Raum gemacht werden, bei denen auch Personen erfasst werden, die nicht als Forschungsteilnehmer gewonnen wurden. In solchen Fällen müssen Marktforscher die Einwilligung der Personen einholen, deren Gesichter klar erkennbar und die identifizierbar sind. Ist dies nicht möglich, sollte das Bild verpixelt oder auf andere Weise unkenntlich gemacht werden. Zusätzlich sollten deutlich lesbare Schilder darauf hinweisen, dass das betreffende Gebiet unter Beobachtung ist. Die Kameras sollten so platziert werden, dass sie nur den Bereich erfassen, der beobachtet werden soll.

6.4 Datenspeicherung in der Cloud

Die Entscheidung, personenbezogene Daten in der Cloud zu speichern, sollte sorgfältig überlegt werden. Marktforscher müssen die Sicherheitskontrollen des Betreibers der Cloud und seine allgemeinen Geschäftsbedingungen bewerten. Viele Cloud-Betreiber bieten nur sehr geringe Schadersatzsummen für den Fall an, dass sie die Sicherheitsvorkehrungen verletzen oder personenbezogene Daten geoffenbart werden. Das wiederum bedeutet, dass die Forschungsfirma ein beträchtliches finanzielles Risiko eingeht, welches ernsthafte Verletzungen der Privatsphäre mit der Folge von Schäden für Einzelpersonen nach sich ziehen können.

Marktforscher sollten daher ausgleichende Kontrollen durchführen, um sich vor diesen Risiken zu schützen. So sollten sie die Daten verschlüsseln, die zur Cloud oder von ihr übertragen werden oder die auf den Servern des Cloud-Betreibers gespeichert sind. Marktforscher sollten sich auch überlegen, ob sie eine Haftpflichtversicherung gegen Internetrisiken abschließen.

Marktforscher müssen auch berücksichtigen, wo die Daten gespeichert werden, damit sie feststellen können, ob die Nutzung der Cloud-Technologie eine grenzüberschreitende Übertragung der Daten darstellt (vgl. Abschnitt 5.5 mit einer ausführlichen Diskussion dieser Problematik). Einige Cloud-Betreiber bieten länderspezifische Speicherorte an, was in manchen Fällen angezeigt sein kann.

Schließlich sollten Marktforscher personenbezogene Daten eher in einer privaten als in einer öffentlichen Cloud speichern. Eine private Cloud ordnet eine bestimmte Geräteausstattung einem Forschungsunternehmen zu. Der hauptsächliche Vorteil einer privaten Cloud ist, dass der Marktforscher zu jeder Zeit weiß, wo die personenbezogenen Daten gespeichert sind. Im Gegensatz dazu kann eine öffentlich Cloud dazu führen, dass die Daten in einem oder auch in mehreren Rechenzentren auf einem oder mehreren Kontinenten liegen. Dies kann sowohl den Datenschutzgesetzen als auch den Verträgen mit der verantwortlichen Stelle widersprechen, die oft den Speicherort der personenbezogenen Daten bestimmen.

6.5 Anonymisierung und Pseudonymisierung

Eine der wichtigsten Pflichten des Marktforschers ist es, den Personenbezug der Daten zu entfernen, bevor sie an den Kunden oder gar an die allgemeine Öffentlichkeit weitergegeben werden. Anonymisierung stellt eine Absicherung dar, die entweder die Löschung oder die Veränderung von identifizierenden Daten beinhalten, so dass die sich ergebenden Daten keine Identifizierung einzelner Personen mehr zulassen. Beispiele sind u.a. Bilder unkenntlich

zu machen oder Ergebnisse nur als zusammenfassende Tabellen zu berichten, um so sicherzustellen, dass keine bestimmte Einzelperson identifiziert werden kann.

Pseudonymisierung beinhaltet die Veränderung der personenbezogenen Daten in der Weise, dass die Einzelperson zwar noch durch eine Identifikationsnummer oder eine Rechenvorschrift identifiziert werden kann, dass die identifizierenden Daten aber getrennt zu Überprüfungszwecken gespeichert sind (s. Frage 9).

Wenn Marktforscher solche Techniken anwenden, sollten sie anhand der jeweiligen Landesgesetze überprüfen, welche Elemente entfernt werden müssen, um die gesetzlichen Standards der Anonymisierung bzw. Pseudonymisierung zu erfüllen.

7 LITERATURVERZEICHNIS

DLA Piper, Data Protection Laws of the World

EphMRA Adverse Event Reporting Guidelines 2014

ICC/ESOMAR International Code on Market and Social Research

ESOMAR Interviewing Children and Young People Guideline

ISO 26362:2009 – Access panels in market, opinion, and social research

ISO 20252 – Market, Opinion and Social Research

OECD Privacy Principles

8 DAS PROJEKTTEAM

Vorsitzende:

- Reg Baker, Berater des ESOMAR Professional Standards Committee und Marketing Research Institute International
- David Stark, Vice President, Integrity, Compliance and Privacy, GfK

Mitglieder des Projektteams:

- Debrah Harding, Managing Director, Market Research Society
- Stephen Jenke, Berater
- Kathy Joe, Director of International Standards and Public Affairs, ESOMAR
- Wander Meijer, Global COO, MRops
- Ashlin Quirk, General Counsel at SSI
- Barry Ryan, Director Policy Unit, Market Research Society
- Jayne Van Souwe, Principal, Wallis Consulting Group