Global Guideline

Online Research

ESOMAR
WORLD RESEARCH

GLOBAL RESEARCH
BUSINESS NETWORK
APRC • EFAMRO • ARIA

ESOMAR, der Weltverband für Sozial-, Meinungs- und Marktforschung, ist die wichtigste Organisation für die Förderung, das Voranbringen und die Aufwertung von Marktforschung. www.esomar.org

GRBN, das Global Research Business Network, verbindet 38 Forschungsverbände und über 3.500 Forschungsunternehmen auf fünf Kontinenten miteinander. www.grbn.org

Official Translation Partner:
Language Connect

INHALTSANGABE

1 EINFÜHRUNG UND UMFANG

Im Jahr 2011 hat ESOMAR in Zusammenarbeit mit CASRO eine Richtlinie für die Durchführung von Online-Forschung veröffentlicht. 2015 fand die Veröffentlichung der ESOMAR/GRBN Richtlinie für hochwertige Online-Stichproben statt. Forscher werden aufgefordert, beim Entwerfen und Durchführen von Online-Umfragen sowohl das letztgenannte Dokument als auch diese Richtlinie zu konsultieren.

Obwohl zahlreiche technische und methodologische Probleme der Online-Forschung bereits im vergangenen Jahrzehnt gelöst worden sind, verlangen die fortlaufenden Entwicklungen in der Technologie und in den Arten und der Vielfalt von digitalen Daten, die online erfasst werden können, eine kontinuierliche Überprüfung und Aktualisierung der fachlichen und ethischen Handlungsempfehlungen.

Diese ESOMAR/GRBN Richtlinie für Online-Forschung hat einen globalen Fokus und erklärt, wie eine Auswahl fundamentaler Prinzipien der Markt-, Sozial- und Meinungsforschung im Kontext der aktuellen, rechtlichen Rahmenbedingungen und regulatorischen Umfelder weltweit angewandt werden sollten. Aus diesem Grund ist das vorliegende Dokument eher als eine grundsätzliche Erklärung von Prinzipien denn als Katalog existierender Vorschriften anzusehen. Das Ziel ist es, Forscher, insbesondere diejenigen in kleinen und mittelgroßen Forschungsorganisationen, dabei zu unterstützen, sich mit rechtlichen, ethischen und praktischen Überlegungen in Bezug auf die Nutzung neuer Technologien bei der Durchführung von Online-Forschung auseinanderzusetzen.

Diese Richtlinie dient nicht als Ersatz für eine gründliche Lektüre und das vollständige Verstehen des ICC/ESOMAR Internationalen Kodex für die Markt- und Sozialforschung, der von mehr als 60 lokalen Verbänden weltweit übernommen wurde, noch die individuellen Kodizes der 38 Verbände, die das GRBN bilden. Vielmehr möchte sie als eine Interpretation der grundlegenden Prinzipien dieser Kodizes im Kontext der Online-Forschung angesehen werden.

Ebenso ist es von grundlegender Bedeutung, dass Forscher die nationalen und lokalen Datenschutzvorschriften und die selbstregulatorischen Vorgaben der Marktforschung jedes Landes einhalten, in denen eine Erfassung oder Verarbeitung von Daten geplant wird, da es je nach Land zu Unterschieden in der Umsetzung grundlegender Prinzipien kommen kann. Die in diesem Dokument bereitgestellten Handlungsrichtlinien sind als minimaler Standard anzusehen und müssen im Kontext eines spezifischen Forschungsprojektes möglicherweise mit zusätzlichen Maßnahmen versehen werden. Möglicherweise sehen Forscher die Notwendigkeit, einen lokalen Rechtsberater des Rechtssystems zu konsultieren, in dem die Forschung durchgeführt wird, um komplette Einhaltung dieser Vorschriften sicherzustellen.

Forscher müssen auf die Bedenken von Kunden sensibel reagieren und dürfen nicht aus den Augen verlieren, dass Marktforschung nur erfolgreich sein kann, wenn die Öffentlichkeit ihr Vertrauen schenkt. Forscher müssen Aktivitäten und technologische Praktiken vermeiden, die zu einer Untergrabung des öffentlichen Vertrauens in die Marktforschung führen könnten. Dies umfasst die Anwendung stichhaltiger, methodologischer Prinzipien und Handlungsweisen in Bezug auf das Forschungsdesign, besonders in Hinblick auf das angemessene Fragebogendesign, die angemessene Fragebogenlänge und die angemessene Belastung für die Teilnehmer. Ebenso muss sorgfältig darauf geachtet werden, dass eine Unterscheidung zwischen Forschung und kommerziellen Aktivitäten stattfindet, wie beispielsweise Direktmarketing oder gezielten Werbemaßnahmen. In Fällen, in denen Forscher Aktivitäten nachgehen, die zwar Forschungstechniken einsetzen, aber nicht ausschließlich für Forschungszwecke bestimmt sind, dürfen diese Aktivitäten nicht als Markt-, Meinungs- oder Sozialforschung bezeichnet werden.

In diesem Dokument wird das Wort „muss“ verwendet, um verbindliche Anforderungen zu kennzeichnen. Wir benutzen das Wort „muss“, um ein Prinzip oder eine Handlungsweise zu

beschreiben, das bzw. die von Forschern zwingend befolgt werden muss. Das Wort „sollte“ wird genutzt, wenn es um die Durchführung geht. Diese Nutzung soll Forschern zu verstehen geben, dass sie die Wahl haben, ein Prinzip oder eine Handlungsweise je nach Forschungsdesign unterschiedlich umzusetzen.

2 DEFINITIONEN

„Active Agent“-Technologien sind Technologien, die das Verhalten von Forschungsteilnehmern im Hintergrund erfassen und typischerweise gleichzeitig mit anderen Aktivitäten mitlaufen. Diese beinhalten:

Tracking-Software, die das tatsächliche Online-Verhalten eines Forschungsteilnehmers einfangen können, wie beispielsweise besuchte Webseiten, abgeschlossene Online-Transaktionen, ausgefüllte Online-Formulare, Klickraten oder Eindrücke von Werbeanzeigen, Online-Einkäufe und GPS-Informationen für digitale Geräte mit Internetverbindung. Diese Art von Software ist ebenso in der Lage, Informationen aus der E-Mail-Adresse des Forschungsteilnehmers und anderen, auf dem Gerät gespeicherten Dokumenten – beispielsweise auf einer Festplatte – zu erfassen. Einige dieser Technologien wurden als „Spyware“ eingestuft, insbesondere dann, wenn der Download oder die Installation oder die Datenerfassung ohne die volle Kenntnis und vorherige Einwilligung des Teilnehmers geschieht.

Software, die auf ein Digitalgerät (Computer, Tablet, Smartphone usw.) heruntergeladen und ausschließlich dafür genutzt wird, potenzielle Forschungsteilnehmer über die Möglichkeiten zur Teilnahme an Umfragen in Kenntnis zu setzen, Inhalte von Umfragen herunterzuladen oder Fragen aus einer Umfrage zu stellen. Diese verfolgt das Verhalten der Forschungsteilnehmer nicht, während sie im Internet surfen und alle gesammelten Daten stammen direkt aus dem Input der Nutzer.

Aktive Forschung bedeutet die Datenerfassung über eine direkte Interaktion mit dem Forschungsteilnehmer (z. B. eine Umfrage, eine Fokusgruppe oder andere Forschungsmethoden, entweder persönlich oder über andere Kommunikationswege, wie beispielsweise das Telefon, Post oder im Internet, einschließlich E-Mail, SMS oder andere elektronische Mittel).

Business-to-Business-Forschung (B2B) bedeutet die Datenerfassung von oder über juristische Personen, wie beispielsweise Unternehmen, Schulen, Wohltätigkeitsorganisationen und so weiter.

Business-to-Consumer-Forschung (B2C) bedeutet die Datenerfassung von oder über Einzelpersonen oder Haushalte.

Cloud-Computing bedeutet den Einsatz von Gruppen von Remoteservern und Computernetzwerken, die eine zentralisierte Datenspeicherung und den Online-Zugriff auf Computerdienstleistungen oder -ressourcen bieten. Cloud-Computing umfasst drei allgemeine Einsatzmodelle: öffentlich, privat oder eine Mischung aus beiden.

Kommerzielle Aktivität sind alle Aktivitäten mit einem anderen Zweck außer Forschung, einschließlich Direktmarketing und gezielte Werbemaßnahmen.

Einwilligung beschreibt die aus freien Stücken geäußerte und informierte Zustimmung einer Person zur Erfassung und Weiterverarbeitung seiner/ihrer personenbezogenen Angaben.

Cookies sind Textdateien, die kleine Informationsmengen enthalten, die auf das Gerät eines Nutzers heruntergeladen werden, während dieser eine Webseite besucht. Cookies werden bei jedem nachfolgenden Besuch gelesen oder zur ursprünglichen Webseite zurückgesandt, die diesen Cookie erkennt.

Cookies sind hilfreich, da sie es einer Webseite ermöglichen, das Gerät eines Nutzers zu erkennen und so die Webseitennavigation zu erleichtern. Dies umfasst Dinge wie die

Fähigkeit, sich an Benutzereinstellungen zu erinnern und die Nutzererfahrung im Allgemeinen verbessern. Forscher können Cookies für zahlreiche unterschiedliche Zwecke nutzen, einschließlich, aber nicht beschränkt auf, um eine bessere Umfrageerfahrung anzubieten, zur Qualitätskontrolle, für Validierungen, um die Teilnahme an der Umfrage möglich oder einfacher zu machen, um abgeschlossene Umfragen oder andere abgeschlossene Aktivitäten nachzuverfolgen oder um Betrug zu entdecken und/oder zu verhindern. Cookies können in den Browsereinstellungen abgelehnt oder gelöscht werden.

Datenverantwortlicher bezieht sich auf die Person oder Organisation, deren Verantwortlichkeit darin besteht festzulegen, wie personenbezogene Angaben weiterverarbeitet werden. Zum Beispiel wäre ein Forschungskunde der Datenverantwortliche für die erfassten Daten seiner Kunden oder Konsumenten, ein Anbieter von Forschungspanels wäre der Datenverantwortliche für die erfassten Daten seiner Online-Panel-Mitglieder und ein Forschungsunternehmen wäre der Datenverantwortliche für die erfassten Daten von Teilnehmern einer Mehrthemenumfrage.

Datenverarbeiter bezieht sich auf eine Partei, die Arbeitsgänge (einschließlich Analyse) mit personenbezogenen Angaben im Namen von oder unter Anleitung des Datenverantwortlichen erhält, protokolliert, verwaltet oder durchführt. Wie bereits erwähnt wäre ein Forschungsunternehmen im Falle von Mehrthemenumfragen sowohl Datenverantwortlicher als auch Datenverarbeiter**.**

Geräte-ID (Geräteidentifikation) ist eine eindeutige Nummer, die einem Smartphone oder einem ähnlichen, handgehaltenen Gerät zugeordnet werden kann. Ein solches Gerät verfügt normalerweise über mehrere Geräte-IDs, die jeweils zu einem anderen Zweck eingesetzt werden. Einige Geräte-IDs werden dazu genutzt, um Dienstleistungen, wie zum Beispiel Wi-Fi oder Bluetooth, zu aktivieren oder um spezifische Geräte eindeutig für den Betrieb in einem Mobilfunknetz zu identifizieren. Andere Geräte-IDs, wie beispielsweise die UDID von Apple oder die Android-ID von Android, werden von Apps, Entwicklern und anderen Unternehmen genutzt, um Geräte und deren Nutzer über mehrere mobile Dienstleistungen hinweg zu identifizieren, nachzuverfolgen und zu analysieren.

Digitaler Fingerabdruck (auch bekannt als Geräte-Fingerabdruck, Maschinen-Fingerabdruck oder Browser-Fingerabdruck) sind Informationen, die über ein Digitalgerät (Computer, Tablet, Smartphone usw.) zum Zweck der Identifikation erfasst werden. Digitale Fingerabdrücke können genutzt werden, um individuelle Forschungsteilnehmer oder Geräte komplett oder teilweise zu identifizieren, falls Cookies deaktiviert worden sind. Typischerweise nutzen sie die Konfigurationsinformationen des Internetbrowsers zusammen mit anderen, zur Verfügung stehenden Parametern des Digitalgerätes. Diese Informationen werden in eine einzelne Zeichenkette integriert, die den digitalen Fingerabdruck enthält. Digitale Fingerabdrücke werden auch in Anwendungsbereichen außerhalb der Forschung angewandt und haben sich für die Entdeckung von Diebstählen von Online-Identitäten und die Vorbeugung von Kreditkartenbetrug als nützlich erwiesen.

In einigen Rechtssystemen zählen digitale Fingerabdrücke möglicherweise zu personenbezogenen Angaben und müssen daher auch als solche behandelt werden, einschließlich der Notwendigkeit für die Einwilligung.

Es ist wichtig zu beachten, dass sich der einem Digitalgerät zugeordnete digitale Fingerabdruck verändern kann, da sich die Komponenten eines digitalen Fingerabdrucks im Verlauf der Zeit ebenso ändern können.

In der Marktforschung wird der Begriff Geräte-ID hin und wieder anstelle des digitalen Fingerabdrucks verwendet. Jedoch hat der Begriff Geräte-ID eine andere Bedeutung (siehe Geräte-ID).

Kostenlose Preisverlosung oder kostenloses Gewinnspiel bezieht sich auf einen Wettbewerb oder eine Auslosung mit zufällig vergebenen Preisen. Teilnehmer müssen

weder eine Gebühr zahlen noch eine sonstige Aktivität außer der Teilnahme selbst unternehmen, um eine Chance auf den Gewinn zu haben. Obwohl hierfür manchmal auch der Begriff „Lotterie“ verwendet wird, wird dieser in einigen Rechtssystemen als ein sehr spezifischer, rechtlicher Begriff behandelt und ist häufig für private Einrichtungen, wie beispielsweise Forschungsagenturen, verboten.

Standortdaten („Geolocation“) bezeichnen die Identifikation der realen, geografischen Lage eines Objektes, wie zum Beispiel eines Digitalgerätes (Computer, Tablet, Smartphone usw.). Standortdaten beziehen sich entweder auf die Praxis der Festlegung des Standortes oder auf den tatsächlich festgelegten Standort.

Incentive bezieht sich auf alle Anreize, die einem Teilnehmer angeboten werden, um die Teilnahme an einer Forschungsstudie zu fördern.

Datenschutzgesetze sind nationale oder lokale Gesetze oder Vorschriften, deren Umsetzung einen Effekt auf den Schutz personenbezogener Angaben haben und die im Einklang mit den in diesem Dokument dargelegten Prinzipien stehen**.**

Local Shared Objects (LSOs), häufig auch Flash-Cookies genannt (aufgrund von deren Ähnlichkeit mit HTTP-Cookies), sind Datenbestandteile, die Webseiten mit Adobe Flash möglicherweise auf dem Gerät oder Computer eines Nutzers speichern.

Marktforschung, einschließlich Sozial- und Meinungsforschung, bedeutet die systematische Sammlung und Interpretation von Informationen über Einzelpersonen oder Organisationen mithilfe der statistischen und analytischen Methoden und Techniken der angewandten Sozial- und Verhaltenswissenschaften, um Einsichten zu erlangen oder Entscheidungsfindungen zu unterstützen.

Online-Forschung bedeutet die Nutzung von Computernetzwerken, hauptsächlich dem Internet, in allen Phasen des Marktforschungsprozesses, einschließlich der Problemerarbeitung, dem Forschungsdesign, der Datenerfassung oder der Datenanalyse.

Paradaten sind Daten über den Prozess, mit dem die Umfragedaten erfasst worden sind. Beispiele sind das Datum und die Uhrzeit der Durchführung der Umfrage, die Zeitdauer der Umfrage und sowie die Teilnehmerbewegung in der Umfrage.

Passive Forschung bedeutet Datenerfassung über Beobachtung, Messung oder Aufzeichnung der Handlungen und Verhaltensweisen eines Teilnehmers.

Personenbezogene Angaben (manchmal auch als „Personally Identifiable Information“, d. h. Informationen zur Identifizierung von Personen, oder als „PII“ bezeichnet) sind alle Informationen, die einer identifizierten oder identifizierbaren, natürlichen Person zugeordnet werden. Bei einer identifizierbaren Person handelt es sich um eine Einzelperson, die direkt oder indirekt, insbesondere durch eine Identifikationsnummer oder über ihre physischen, physiologischen, mentalen, ökonomischen, kulturellen oder sozialen Eigenschaften, identifiziert werden kann. In einigen Forschungsarten können solche Datensätze auch Situationen umfassen, in denen Einzelpersonen aufgrund von Fotografien, Video- oder Tonaufnahmen identifizierbar sind, sowie aufgrund anderer, personenbezogener Angaben, die während der Forschung erfasst werden.

PII bedeutet „Personally Identifiable Information“ (oder Informationen zur Identifizierung von Personen). Siehe personenbezogene Angaben.

Private Cloud bezieht sich auf ein Cloud-Computing-System, in dem spezielle Ausrüstung eines bestimmten Rechenzentrums dem Unternehmen des Forschers zugeordnet wird.

Öffentliche Cloud ist ein Cloud-Computing-System, in dem ein Dienstleistungsanbieter der allgemeinen Öffentlichkeit Ressourcen über das Internet zur Verfügung stellt, beispielsweise Applikationen und Speicherplatz.

Forschungsteilnehmer bezeichnet alle Personen, deren personenbezogene Angaben für Forschungszwecke erfasst werden. Dies kann entweder mit aktiven oder passiven Methoden geschehen.

Forscher ist eine Einzelperson oder ein Unternehmen, die bzw. das ein Marktforschungsprojekt durchführt oder als Berater für ein solches Projekt agiert, einschließlich aller Mitarbeiter von Kundenorganisationen und alle genutzten Unterlieferanten.

Sensible Daten sind alle Informationen über die Rasse oder Ethnie, die Gesundheit oder das Sexualleben, das Strafregister, die politische Meinung, religiöse oder philosophische Glaubensausrichtungen oder Gewerkschaftsmitgliedschaften einer identifizierbaren Einzelperson. In unterschiedlichen Rechtssystemen werden möglicherweise noch weitere Zusatzinformationen als sensibel bezeichnet. In den USA gelten beispielsweise auch persönliche, gesundheitsbezogene Informationen, das Einkommen oder sonstige, finanzielle Informationen, finanzielle Identifikatoren und von der Regierung herausgegebene Dokumente oder Identitätsdokumente für Finanzdienstleistungen als sensibel.

Social-Media-Forschung bedeutet Forschung, in der Social-Media-Daten entweder allein oder in Kombination mit Daten aus anderen Quellen genutzt werden.

Spyware ist eine Software, die sich ohne Kenntnis des Nutzers Zugriff auf einen Computer oder auf Informationen über eine Person oder Organisation verschafft und diese Informationen möglicherweise und ohne die Einwilligung des Nutzers an eine andere Instanz weiterschickt.

Unterauftragsvergabe bedeutet die Weitergabe von Verantwortlichkeiten an ein Drittunternehmen oder eine Drittperson für die Durchführung eines Teils eines Forschungsprojektes, einschließlich Auslagerung („Outsourcing“) und Auslandsverlagerung („Offshoring“).

Zählpixel sind in eine Webseite oder E-Mail eingebettete und für den Nutzer unaufdringliche (und normalerweise unsichtbare) Objekte. Zählpixels erlauben es dem Betreiber einer Webseite oder dem Absender eine E-Mail zu erkennen, ob ein Nutzer die Seite oder E-Mail angesehen hat. Häufige Einsatzgebiete sind die Nachverfolgung von E-Mails und das Page-Tagging für Webanalysen. Alternative Namen sind Web-Beacon, Tracking-Bug, Tag, Page Tag oder Web Bug.

Übertragung bezieht sich im Zusammenhang mit Daten auf jede Art der Offenlegung, Kommunikation, Kopieanfertigung oder Bewegung von Daten von einer Partei zu einer anderen, unabhängig vom genutzten Medium, einschließlich, aber nicht beschränkt auf, Bewegungen innerhalb eines Netzwerks, physische Übertragungen, Übertragungen von einem Medium oder Gerät auf ein anderes oder über ferngesteuerten Zugriff auf die Daten.

Grenzüberschreitende Übertragungen personenbezogener Angaben sind die Bewegung personenbezogener Angaben über Ländergrenzen hinweg und mithilfe jeder möglichen Art und Weise, einschließlich des Zugriffs auf Daten von außerhalb des Landes, in dem diese erfasst wurden. Dies kann auch die Nutzung von Cloud-Technologien für die Datenerfassung und -speicherung umfassen**.**

3 TEILNEHMER: BEZIEHUNGEN UND VERANTWORTLICHKEITEN

3.1 Abgrenzung von Markt-, Sozial- und Meinungsforschung von anderen Aktivitäten der Datenerfassung

Forscher müssen sicherstellen, dass Forschungszwecke eindeutig von anderen, außerhalb der Forschung stattfindenden Online-Aktivitäten abgegrenzt werden. Zusätzlich dürfen sie es

nicht zulassen, dass von ihnen erfasste, personenbezogene Angaben für irgendeinen anderen Zweck außer der Marktforschung verwendet werden. Um Forschungsteilnehmern diese Unterscheidung eindeutig zu kommunizieren, müssen Forscher die Forschungsdienstleistung und die Organisation oder das Unternehmen, das diese erbringt, auf eine Art und Weise präsentieren, die sich eindeutig von Nichtforschungsaktivitäten unterscheidet.

Diese Bedingung hindert Forscher nicht an deren Mitarbeit an Aktivitäten außerhalb des Forschungsbereiches, vorausgesetzt der Zweck der Datenerfassung von personenbezogenen Angaben wird nicht fehlinterpretiert und personenbezogene Angaben werden nicht für irgendeinen anderen Zweck verwendet, außer es wurde von jedem Teilnehmer eine informierte Einwilligung eingeholt. Sie schränkt ebenso wenig das Recht der Organisation ein damit zu werben, dass das Unternehmen neben Marktforschung auch andere Aktivitäten betreibt, vorausgesetzt diese beiden Handlungen werden eindeutig voneinander abgegrenzt und separat und in Übereinstimmung mit den geltenden Gesetzen, Vorschriften und lokalen Verhaltensregulierungen der Branche durchgeführt.

3.2 Benachrichtigung, Ehrlichkeit, Zustimmung und der freiwillige Charakter von Forschung

Forscher müssen von jedem Forschungsteilnehmer eine informierte Einwilligung einholen, bevor mit der Erfassung und Verarbeitung jeglicher personenbezogener Angaben begonnen werden kann. Sie müssen absolute Transparenz hinsichtlich der Informationen walten lassen, deren Erfassung sie planen, sowie hinsichtlich des Zwecks dieser Erfassung, wie diese Daten geschützt werden, mit wem sie möglicherweise geteilt werden und auf welche Art und Weise dies geschehen kann. Diese Informationen sollten eindeutig, präzise und auffallende Weise präsentiert werden. Dies beinhaltet, ist aber nicht beschränkt auf, die Nutzung der Best Practices für Datenschutzrichtlinien, die auffällige Platzierung von Links zu den Datenschutzrichtlinien in Fragebögen und Panel-Webseiten und Kommunikation während der Prozesse der Datenerfassung und -nutzung. Teilnehmer dürfen niemals getäuscht, belogen, betrogen oder genötigt werden. Die Teilnahme an Forschungsstudien ist immer freiwillig und Teilnehmern muss es erlaubt sein, deren Teilnahme jederzeit abzubrechen und die Löschung derer personenbezogener Angaben zu verlangen, sofern diese nicht pseudonymisiert vorliegen.

Diese Richtlinie erkennt ebenso an, dass in einigen Situationen die Einholung der Einwilligung möglicherweise nicht realisierbar ist. Siehe 3.2.1 für weitere Informationen.

Wenn es zu einem beliebigen Zeitpunkt während der Forschungsstudie zu wesentlichen Veränderungen im Forschungsplan kommen sollte (beispielsweise eine zusätzliche Erfassung passiver Daten, wie dem Standort oder identifizierbarer Daten, die mit Forschungsdienstleistungen nutzenden Kunden geteilt werden), dann müssen die Teilnehmer darüber informiert werden, damit diese eine informierte Entscheidung über ihre weitere Teilnahme treffen können. Im Falle eines Access Panels oder einer Forschungsgemeinde oder wenn eine Forschungsstudie mehrere Phasen der Datenerfassung umfasst oder sich über mehrere Monate oder länger erstreckt, sollten Forscher die Einwilligung in regelmäßigen Abständen erneut einholen, indem die Teilnehmer an die Datenerfassung, die Gründe hierfür und die beabsichtigte Nutzung erinnert werden. Zeitpunkte, zu denen die Einwilligung erneut eingeholt werden sollte, sind unter anderem wesentliche Veränderungen bei der Datenerfassung oder der Anwendung der Daten, eine Veränderung innerhalb der Forschungsorganisation oder bei dessen Eigentumsverhältnissen oder eine Veränderung der geltenden Gesetze und Vorschriften.

Und schließlich müssen Forscher die geltenden Gesetze, Vorschriften und lokalen Verhaltensregulierungen der Branche einhalten.

3.2.1 Passive Daten

Neue Technologien machen es heutzutage möglich, eine große Vielfalt personenbezogener Angaben ohne direkte Interaktion mit den Einzelpersonen zu erfassen, deren Daten erhoben werden.

Beispiele beinhalten, sind aber nicht beschränkt auf, Daten aus Internetsuchen, von Treuekarten und Scannern in Ladengeschäften, Standortdaten aus internetfähigen Geräten und einige Datenarten aus sozialen Netzwerken. Während sich die mobile Technologie immer weiter entwickelt, kann auf viele dieser Datenquellen auch von und über Mobilgeräte zugegriffen werden.

In Situationen, in denen Forscher webseitenübergreifende Daten aus Internetsuchen von Panel-Mitgliedern oder mobilen Applikationen erfassen, muss dem Teilnehmer eine detaillierte Beschreibung über die spezifischen, erhobenen Daten und die hierfür genutzte(n) Methode(n) bereitgestellt und dessen explizite Einwilligung eingeholt werden, bevor solche Daten erfasst werden können. Dies gilt insbesondere für solche Arten von mobilen Apps, die Standortdaten abfragen, passiv mithören und/oder das Betriebssystem von Mobilgeräten ausmessen.

In Fällen, in denen personenbezogene Angaben aus öffentlichen Räumen, wie beispielsweise Webseiten und Seiten sozialer Netzwerke, erfasst werden, muss die Einwilligung direkt eingeholt oder explizit in den Nutzungsbedingungen der Plattform bereitgestellt werden. Dies trifft nicht auf die Veröffentlichungen in sozialen Netzwerken zu, die den Namen des Verfassers beinhalten, da dies eine verringerte Datenschutzerwartung impliziert.

Einige Verbände, einschließlich CASRO und ESOMAR, verfügen über Richtlinien für bestimmte soziale Netzwerke, die für weitere Informationen zu Rate gezogen werden sollten. Eine kombinierte ESOMAR/GRBN Richtlinie für soziale Netzwerke ist derzeit in Bearbeitung, die Veröffentlichung wird für Anfang 2016 erwartet.

In Fällen, in denen Drittanbieter für die Erfassung von Daten genutzt werden, sind Forscher trotzdem dazu verpflichtet sicherzustellen, dass diese Daten rechtmäßig erhoben wurden.

Da es je nach Land zu Unterschieden in der Umsetzung grundlegender Prinzipien kommen kann,1 müssen Forscher die nationalen und internationalen Datenschutzvorschriften und die selbstregulatorischen Vorgaben der Marktforschung jedes Landes einhalten, in denen eine Erfassung oder Verarbeitung von Daten geplant wird.

In Fällen, in denen Forscher ohne Einwilligung Kommentare an eine Drittpartei weitergeben, muss sichergestellt werden, dass ausschließlich depersonalisierte Daten weitergegeben werden. Dies ist mithilfe bestimmter Techniken, wie beispielsweise der Datenmaskierung, möglich.

Bei der Durchführung aller Forschungsprojekte müssen Forschungsunternehmen eine eindeutige und einsehbare Datenschutzrichtlinie über deren Datenerfassungen und Datenschutzmaßnahmen bereitstellen, einschließlich der Kontaktinformationen des Forschungsunternehmens.

Weiterhin ist der Forscher dem Datenschutz und der Sicherheit aller personenbezogenen Angaben verpflichtet, unabhängig davon, wie diese in seinen Besitz gekommen sind. Dies beinhaltet die Anonymisierung der Daten durch das Forschungsunternehmen vor der Weiterleitung an Drittparteien und das Abschließen eines Vertrages mit dem Empfänger der Daten, in welchem der Letztgenannte zustimmt, keinerlei Versuche zu unternehmen, die

[1] In zahlreichen Rechtssystemen ist es notwendig die Einstimmung einzuholen, um personenbezogene Angaben zu erfassen, zu verarbeiten und zu teilen. Möglicherweise lassen einige Rechtssysteme zu Forschungszwecken Ausnahmen zu, wenn die Einholung der Einwilligung nachweislich nicht machbar ist und die dem Kunden bereitgestellte Analyse in Form von anonymisierten Daten geschieht.

Einzelpersonen rückwirkend zu identifizieren oder diese Daten für Nichtforschungszwecke zu verwenden.

3.2.2 Sensible Daten

Obwohl es sich bei der Online-Methodologie im Vergleich zu anderen um eine weniger aufdringliche Art der Datenerfassung handelt und Forschern die Möglichkeit gibt, sensible Themen leichter anzusprechen als in Face-to-Face- oder Telefoninterviews (die die Präsenz eines Interviewers benötigen), müssen Forscher trotz allem vorsichtig sein, wenn sie Teilnehmer mit sensiblen Themen konfrontieren – entweder aufgrund der gesetzlichen Bestimmungen oder wegen der Gefahr den Teilnehmer zu verletzen oder zu ängstigen.

Forscher müssen sicherstellen, dass der Zweck für die in der Umfrage gestellten sensiblen Fragen erklärt und die ausdrückliche Einwilligung des Teilnehmers eingeholt wird. Außerdem muss erklärt werden, dass die Datenverarbeitung auf einem anonymen und vertraulichen Weg geschieht, dass jede Frage eine „Ich bevorzuge es, nicht zu antworten"-Option oder eine andere Option enthält, die es dem Teilnehmer erlaubt, sensible Fragen nicht zu beantworten, wenn sie dies nicht möchten und es muss sichergestellt werden, dass die Fragen notwendig, relevant und eindeutig sind. Wenn dieses Schutzmaßnahmen aufgrund des Forschungsdesigns nicht angewandt werden können, müssen die Teilnehmer hierauf aufmerksam gemacht werden und deren ausdrückliche Einwilligung hierzu geben.

In einigen Ländern ist es möglicherweise notwendig, die Bevollmächtigung für die Erfassung sensibler, personenbezogener Angaben von der zuständigen, nationalen Behörde einzuholen.

3.3 Sicherstellen, dass Teilnehmer nicht zu Schaden kommen

Forscher müssen alle angemessenen Vorkehrungen treffen, um sicherzustellen, dass Teilnehmer an Online-Forschungsstudien weder zu Schaden kommen noch durch deren Teilnahme nachteilig beeinträchtigt werden. Dies beinhaltet jede Art von Schädigung, z. B. finanziell, physisch oder emotional. Dementsprechend sollten sie die spezifischen Forschungsanforderungen sorgfältig erwägen, die lokal geltenden, gesetzlichen Bestimmungen/Einschränkungen und Vorschriften zu Rate ziehen und die konkreten Auswirkungen prüfen, die die Umfrage möglicherweise auf die Teilnehmer haben könnte. In jedem Fall müssen Forscher faire Behandlungsprinzipien anwenden. Diese beinhalten:

Vermeidung irreführender Aussagen, die für den Teilnehmer verletzend oder belästigend sein würden (z. B. unzutreffende Informationen über den Inhalt der Forschungsstudie, die wahrscheinliche Länge des Interviews oder die Möglichkeit zu einem späteren Zeitpunkt eventuell noch einmal online oder auf eine andere Art und Weise befragt zu werden;

Vermeidung irreführender oder unaufgeforderter Datenerfassung und -verarbeitung (z. B. geheim gehaltene, automatisierte Systeme, die personenbezogene Angaben aus Online-Umgebungen/Mobilgeräten sammeln), wenn Nutzer Datenschutz oder die Aufforderung zur Einwilligung für bestimmte Handlungen erwarten); und

Beantwortung aller Nachfragen von Teilnehmern an die Marktforschungsagentur/den Forscher.

Der Forscher muss sicherstellen, dass weder personenbezogene Angaben zurückverfolgt noch die Identitäten von Einzelpersonen über Kreuzanalysen (deduktive Aufdeckung), kleine Stichproben oder auf irgendeine andere Art und Weise über die Forschungsergebnisse erschlossen werden können. Beispiele umfassen unter anderem das Verbinden von Zusatzinformationen, wie beispielsweise geografische Daten oder die Fähigkeit, einen spezifischen Forschungsteilnehmer zu identifizieren.

3.4 Datenschutz und Privatsphäre

Forscher müssen die universellen Grundsätze für den Datenschutz von personenbezogenen Angaben befolgen. Diese Grundsätze besagen, dass alle erfassten und gespeicherten, personenbezogenen Angaben folgende Merkmale aufweisen müssen:

Erfassung für spezifische Forschungszwecke und keine Nutzung in irgendeiner Art und Weise, die mit diesen Zwecken unvereinbar ist;

Adäquat, relevant und nicht übertrieben in Hinblick auf den Forschungszweck, für welchen diese erfasst und/oder weiterverarbeitet werden;

Von den Antwortdaten separate Speicherung, falls möglich; und

Keine längere Aufbewahrung als für den Zweck notwendig, zu dem die Information erfasst und weiterverarbeitet wurde.

Forscher müssen ebenso alle geltenden nationalen und lokalen Gesetze und Vorschriften einhalten.

3.4.1 Datenschutzrichtlinien

Datenschutzgesetze und -vorschriften verlangen normalerweise, dass Forschungsunternehmen eine Datenschutzrichtlinie auf deren Webseiten veröffentlichen. Diese Datenschutzrichtlinien müssen Forschungsteilnehmer darüber informieren, welche personenbezogenen Angaben erfasst, wie diese genutzt und verwaltet (gespeichert und abgerufen) und geteilt werden und unter welchen Bedingungen diese für eine Drittpartei offengelegt werden. Datenschutzrichtlinien müssen ebenso beschreiben, wie weitere Informationen zu diesem Thema erhalten und eine Beschwerde eingereicht werden kann. Sie müssen ebenso in allen Online-Forschungsstudien, relevanten Webseiten und elektronischen Kommunikationsmitteln verfügbar gemacht werden (dies geschieht üblicherweise über einen Link).

Teilnehmer müssen außerdem über die der Datenerfassung zugrunde liegenden Gesetze informiert werden. Wenn Daten in mehreren Ländern erfasst werden, muss der Forscher die Gesetze der Länder einhalten, in denen die Forschung durchgeführt wird. In Fällen, in denen es Forschern möglich ist, Kenntnis über das Wohnsitzland der Teilnehmer zu erlangen, müssen die gesetzlichen Bestimmungen dieses Landes unter Beachtung der Tatsache eingehalten werden, dass es zu beträchtlichen Unterschieden zwischen verschiedenen Rechtssystemen kommen kann.

3.4.2 Datensicherheit

Forscher müssen sicherstellen, dass Sicherheitsprotokolle angewendet werden, um vor Risiken wie Verlust, unautorisiertem Zugriff, Zerstörung, Nutzung, Modifikation und Offenlegung zu schützen. Dementsprechend müssen Forscher strenge Maßnahmen für die Datensicherheit ergreifen.

Es existieren unterschiedliche Standards und Rahmenbedingungen, die für die Entwicklung der notwendigen Sicherheitsstandards und -richtlinien im Einsatz sind. Weitere Informationen erhalten Forscher in der Norm ISO 27001: Informationstechnologie – Sicherheitstechniken – Informationssicherheitsmanagementsysteme – Anforderungen oder der ESOMAR Datenschutz-Checkliste.

3.4.3 Benachrichtigung bei Sicherheits- oder Datenschutzverletzungen

Forscher müssen alle relevanten Gesetze und Vorschriften in bezüglich Benachrichtigungen bei Sicherheits- oder Datenschutzverletzungen und Protokollanforderungen einhalten. Sollten solche Gesetze und Vorschriften nicht vorhanden sein, dann müssen Forscher alle betroffenen Parteien und ohne unangemessene Verzögerung über Sicherheits- oder Datenschutzverletzungen informieren, einschließlich Kunden, Forschungsteilnehmer und

Unterlieferanten. Diese Benachrichtigung sollte eine Beschreibung der Arten von Daten beinhalten, die von der Verletzung betroffen sind, sowie alle Maßnahmen, die die Einzelpersonen ergreifen sollten, um sich vor möglicherweise aus der Verletzung entstehendem Schaden zu schützen.

3.4.4 Grenzüberschreitende Übertragungen

Bevor personenbezogene Daten vom Land der Erfassung in ein anderes Land übertragen werden, muss der Forscher sicherstellen, dass diese Datenübertragung legal ist und alle angemessenen Maßnahmen ergreifen, um den Datenschutz und die Datensicherheit zu garantieren. Dies ist der Fall, wenn sich ein Daten erfassender Server in einem Drittland befindet. Dieses Prinzip trifft ebenso bei der Nutzung von Cloud-Technologie zu, wenn sich die Cloud-Server in einem Drittland befinden (siehe Abschnitt 7.7).

3.5 Teilnehmerwerbung via E-Mail und SMS

Lokale und nationale Gesetze können sich in Bezug auf deren Auslegung über die Handhabung von E-Mails und SMS unterscheiden. In einigen Ländern ist die Nutzung automatisierter Systeme zum Senden von SMS untersagt, außer es wurde die ausdrückliche Einwilligung eingeholt.[2] Forscher dürfen keinerlei Vorwände benutzen, um E-Mail-Adressen oder Mobilfunknummern von potenziellen Teilnehmern zu erhalten. Dies beinhaltet die Nutzung öffentlicher Domänen, die Nutzung von Technologien oder Techniken ohne die Kenntnis der Einzelperson oder die Datenerfassung unter dem Deckmantel einer anderen Aktivität als Forschung.

Forscher dürfen keine unaufgeforderten E-Mails oder SMS nutzen, um Forschungsteilnehmer zu rekrutieren oder eine heimliche Datenerfassung durchzuführen. In diesem Fall bedeutet „unaufgefordert“, dass die Teilnehmer keine Einwilligung gegeben oder eine angemessene Erwartungshaltung dahingehend haben, möglicherweise solche E-Mails oder SMS zu erhalten.

Einzelpersonen, die für Forschungszwecke via E-Mail oder SMS kontaktiert werden, müssen auf angemessene Weise bereits eine solche Kontaktaufnahme für Forschungszwecke via E-Mail oder SMS erwarten. Es kann von einer solchen Zustimmung ausgegangen werden, wenn ALLE folgenden Bedingungen existieren UND es keinerlei Einschränkungen oder Verbote auf rechtlicher Ebene in lokalen Gesetzen und/oder Vorschriften gibt:

- Es besteht eine substanzielle, bereits bestehende Beziehung zwischen den kontaktierten Einzelpersonen und dem Forscher, dem die E-Mail-Adressen oder Mobilfunknummern bereitstellenden Kunden oder dem die E-Mail-Adressen oder Mobilfunknummern bereitstellenden Stichprobenanbieter (letzterer wird auch in der E-Mail- oder SMS-Einladung als solcher identifiziert oder verlinkt).

- In Fällen, in denen per E-Mail oder SMS Eingeladene ausdrücklich der Online- oder mobilen Forschung mit dem Forscher oder Stichprobenanbieter zugestimmt haben, oder im Fall einer vom Kunden bereitgestellten Verbraucherliste, die E-Mail- oder SMS-Kommunikationen nicht abgelehnt haben und für Forschungszwecke kontaktiert werden können.

[2] Auch hier unterscheiden sich die Gesetze und/oder Vorschriften hinsichtlich der Nutzung von automatisierten Systeme für das Wählen von Telefonen oder das Senden von Nachrichten an Mobiltelefone je nach Rechtssystem. In einigen Rechtssystemen gibt es Ausnahmen für Forschungszwecke, während in anderen eine Einwilligung erforderlich ist. Ein spezifisches Rechtssystem sollte separat erwähnt werden: in den USA verlangt der „Telephone Consumer Protection Act“ (TCPA) eine Einwilligung, um ein Mobiltelefon mit automatisierten Systemen für das Wählen von Telefonen oder das Senden von Nachrichten kontaktieren zu dürfen.

- E-Mail- oder SMS-Einladungen an potenzielle Forschungsteilnehmer kommunizieren den Namen des Stichprobenanbieters, Forschers oder Kunden deutlich, oder enthalten einen entsprechenden Link, beschreiben die bestehende Beziehung mit der Einzelperson und bieten die Möglichkeit, zukünftige Kontaktaufnahmen via E-Mail oder SMS abzulehnen.

- Die Liste der E-Mail-Stichproben oder Mobilfunknummern schließt auf angemessene und zeitnahe Weise alle Einzelpersonen aus, die vorher die Entfernung für zukünftige Kontaktaufnahmen via E-Mail oder SMS gefordert haben.

- Teilnehmer auf der E-Mail- oder Mobilgeräteliste wurden nicht über unaufgeforderte E-Mail- oder SMS-Einladungen rekrutiert.

Forscher müssen außerdem Folgendes beachten:

- Wenn Forscher von Kunden oder Stichprobenanbietern E-Mail-Listen oder Listen mit Mobilfunknummern erhalten, dann müssen sie zusammen mit dem Kunden oder Stichprobenanbieter prüfen, ob die aufgelisteten Einzelpersonen auf angemessene Art und Weise erwarten, per E-Mail oder SMS kontaktiert zu werden.

- Forscher dürfen bei der Rekrutierung von Teilnehmern keine gefälschten oder irreführenden Absender-E-Mail-Adressen verwenden.

- Forscher müssen Teilnehmern die Möglichkeit bieten, sich bei jedem Forschungsprojekt gegen eine Teilnahme zu entscheiden. Dies trifft ebenso zu, wenn ein Teilnehmer die Entfernung von einer Stichprobenquellenliste für Blindstudien fordert (d. h. in denen der Sponsor der Studie in der E-Mail- oder SMS-Anwerbung nicht angegeben oder verlinkt wird, aber dem Teilnehmer die Offenlegung dieser Information während oder nach der Befragung angeboten wird).

- Forscher müssen auch dann alle zutreffenden Bedingungen dieses Abschnittes erfüllen, wenn andere Technologien zur Nachrichtenübermittlung genutzt werden, wie beispielsweise mobile Applikationen (mobile Apps) für Benachrichtigungen, die ähnliche Eigenschaften und Fähigkeiten wie SMS-Nachrichten aufweisen.

Eine bewährte Verfahrensweise für Forscher ist die Aufbewahrung von Kopien oder Protokollen von E-Mails und anderen Dokumenten, die von Forschungsteilnehmern erhalten worden sind und in denen sie dem Zugriff auf und der Nutzung von deren personenbezogenen Angaben zustimmen oder diese einschränken.[3]

3.6 Incentives

Die Regeln für Gewinnspiele und kostenlose Preisverlosungen sollten in Zusammenhang mit den folgenden Regeln für Incentives gelesen werden.

In Fällen, in denen Incentives zur Teilnahmeförderung an Online-Forschungsprojekten eingesetzt werden, müssen Forscher sicherstellen, dass die Teilnehmer eindeutig darüber informiert werden:

- wer die Incentives verwaltet;

- um was es sich bei den Incentives handelt;

[3] In einigen Ländern handelt es sich hierbei um eine gesetzliche Bestimmung, einschließlich in allen Mitgliedsstaaten der Europäischen Union, Argentinien, Australien, Kanada, Neuseeland und den USA (für Forscher, die an dem US-EU Safe Harbor-Abkommen teilnehmen).

- wann Teilnehmer die Incentives erhalten; und

- ob der Erhalt an Bedingungen geknüpft ist, z. B. die Erledigung einer bestimmten Aufgabe oder das erfolgreiche Bestehen von Qualitätskontrollen (beispielsweise bei einer Online-Panel-Forschungsstudie).

Forscher müssen ebenso sicherstellen, dass Incentives verhältnismäßig und kein Bestechungsgeschenk sind oder als solches wahrgenommen werden. Incentives müssen für die Zielgruppe und die Art der Forschung angemessen sein. Wenn sich beispielsweise eine Online-Forschungsstudie auf das Fahrverhalten von Teilnehmern konzentriert, dann wäre es unangemessen alkoholische Getränke als Incentive anzubieten.

Forscher müssen sicherstellen, dass die für die Verwaltung der Incentives erfassten Daten nicht für andere Zwecke genutzt werden, z. B. für den Aufbau einer Datenbank. Sie dürfen ohne die ausdrückliche Erlaubnis der Teilnehmer keinerlei identifizierbaren Teilnehmerinformationen, die als Teil des Incentive-Prozesses gesammelt worden sind, an Kunden (einschließlich interner Kunden, wenn die Durchführung innerhalb der Forschungsabteilung des Kunden geschieht) und/oder eine andere Drittpartei weitergeben.

Forscher müssen die lokalen Gesetze und Vorschriften in Bezug auf Incentives kennen. In einigen Ländern gelten beispielsweise folgende Regelungen:

- Die Nutzung von durch Kunden bereitgestellte Incentives und/oder Rabattangebote, bei denen Teilnehmer Geld ausgeben müssen, um aus dem Incentive Nutzen ziehen zu können (beispielsweise Preisermäßigungen auf Waren und Dienstleistungen, die von den Teilnehmern bezahlt werden müssen, um einen Vorteil zu erhalten) sind für Online-Forschungsprojekte verboten, da solche Aktivitäten zum Direktmarketing zählen (da die von den Kunden bereitgestellten Incentives und Ermäßigungen als Art der Kundenwerbung angesehen werden).

- Incentives müssen von einer spezifischen Art sein (d. h. nicht monetär).

Bei Online-Forschungsprojekten über Ländergrenzen hinweg und sich über mehrere Länder erstreckend, muss der Prozess des Anbietens von Incentives alle relevanten Gesetze aller beteiligten Länder einhalten.

3.6.1 Gewinnspiele und kostenlose Preisverlosungen (auch als Lotterie bekannt)

Gewinnspiele und kostenlose Preisverlosungen sind eine besonders beliebte Art von Incentive in der Online-Forschung. Bei deren Nutzung muss der Forscher alle geltenden, lokalen Gesetze und Vorschriften kennen, die sich je nach Land unterscheiden können, und sich der erheblichen Risiken der Nutzung dieses Ansatzes ohne das notwendige, detaillierte Wissen bewusst sein. In einigen Ländern gelten beispielsweise folgende Regelungen:

- Teilnehmer dürfen nichts weiter tun als der Teilnahme an Online-Forschungsprojekten zuzustimmen, um die Teilnahmeberechtigung für die kostenlose Preisverlosung oder das Gewinnspiel zu erhalten. Dies beinhaltet, dass keinerlei Antworten auf Forschungsfragen gegeben oder Umfragen ausgefüllt werden müssen usw., die möglicherweise Teil eines Forschungsprojektes sind, besonders wenn von der Einzelperson eine unverhältnismäßig große Menge an Daten bereitgestellt werden muss, da dies als die „Übertragung des Geldwertes“ der Person ausgelegt werden kann. In solchen Fällen würde dies genauso interpretiert werden wie eine für die Teilnahme notwendige Zahlung und würde daher als bezahlte Lotterie gesetzlichen Kontrollen unterliegen.

- Irgendeine Art von Kenntnis, die möglicherweise für die Teilnahme an der kostenlosen Preisverlosung/dem Gewinnspiel notwendig ist, um diese als solche zu klassifizieren, z. B. das Stellen einer Frage, die eine bestimmte Menge an Wissen verlangt, auch wenn diese recht einfach ist (z. B. Wer ist der Präsident der Vereinigten Staaten von Amerika?), bevor die Teilnahme akzeptiert wird.

- Die nicht komplette Durchführung von Forschungsaktivitäten oder -projekten führt nicht zu einer Disqualifikation der Teilnehmer in Bezug auf die Teilnahme einer kostenlosen Preisverlosung oder eines Gewinnspiels.

Forscher dürfen Preise aus kostenlosen Preisverlosungen/Gewinnspielen nicht einbehalten, außer Teilnehmer haben die in den Regeln dargelegten Kriterien eindeutig nicht erfüllt, die die Grundlage der kostenlosen Preisverlosung/des Gewinnspiels bilden (z. B. Regeln, die die Teilnahme von Familienmitgliedern von für die Preisverlosung oder das Gewinnspiel verantwortlichen Mitarbeitern eindeutig von der Teilnahme an der Verlosung ausschließen).

Forscher müssen sicherstellen, dass den Teilnehmern zum Zeitpunkt der Bitte nach Einwilligung alle relevanten Informationen über kostenlose Preisverlosungen/Gewinnspiele eindeutig kommuniziert werden. Spezifische Anforderungen variieren je nach Land, beinhalten aber die folgenden Arten von Informationen:

- der letzte Tag, an dem eine Teilnahme möglich ist;

- die Art des Preises;

- ob ein Preis gegen Bargeld getauscht werden kann;

- wie und wann die Gewinner über die Ergebnisse benachrichtigt werden;

- wie und wann die Gewinner und die Ergebnisse bekannt gegeben werden;

- die Qualifikations- und Disqualifikationskriterien; und

- alternative Wege der Teilnahme.

Alle Regeln müssen eindeutig und unmissverständlich sein, damit sie von Teilnehmern leicht verstanden werden können und nicht irreführend sind. Dies beinhaltet die Gewinnchancen, den Wert der angebotenen Preise und so weiter. Zusätzlich muss beachtet werden:

- Solche Regeln dürfen weder unzumutbar noch übermäßig einschränkend sein.

- Forscher müssen eindeutig zwischen Geschenken unterscheiden, die allen oder den meisten Teilnehmern an der kostenlosen Preisverlosung/dem Gewinnspiel angeboten werden, und Preisen, die nur die Gewinner erhalten.

- Forscher müssen sicherstellen, dass es für alle kostenlosen Preisverlosungen/Gewinnspiele eine alternative, kostenfreie Teilnahmemöglichkeit gibt und dass die Gewinnchancen für alle Arten der Teilnahme gleich hoch sind.

- Forscher müssen sicherstellen, dass die Gewinner von kostenlosen Preisverlosungen/Gewinnspielen auf eine Art und Weise ausgewählt werden, die eine faire Anwendung der Gesetze des Zufalls garantiert. Der Prozess, über den Gewinner ausgewählt werden, muss von einem eindeutigen Überwachungsprotokoll untermauert werden und alle Verlosungen müssen unabhängig voneinander stattfinden. In einigen Ländern ist es möglicherweise notwendig, unabhängige Beobachter einzubeziehen, um

sicherzustellen, dass alle Teilnehmer zum Zeitpunkt der Gewinnziehung die gleiche Gewinnchance haben.

- Und schließlich müssen Forscher sicherstellen, dass Kunden über deren Verpflichtungen und potenzielle Verpflichtungen in Bezug auf alle kostenfreien Preisverlosungen/Ziehungen/Gewinnspiele informiert werden, die in deren Namen durchgeführt werden. Forscher sollten zusammen mit den Kunden Handlungsansätze für die Abmilderungen dieser Verpflichtungen besprechen (z. B. die Einbeziehung einer Haftpflicht- und Freistellungsverfügung).

Forscher müssen vor der Durchführung einer solchen Unternehmung immer erst die nationalen Verbandsrichtlinien überprüfen.

4 KUNDEN: BEZIEHUNGEN UND ERANTWORTLICHKEITEN

4.1 Unterauftragsvergabe

Forscher müssen Kunden vor Arbeitsbeginn darüber informieren, falls ein Teil der Arbeit an einen Unterlieferanten außerhalb der eigenen Organisation des Forschers vergeben wird. Auf Anfrage muss dem Kunden auch die Identität dieser Unterlieferanten mitgeteilt werden.

In Fällen, in denen die Identität eines Unterlieferanten, der für die Beschaffung von Stichproben zuständig ist, berechtigterweise als urheberrechtlich geschützte Information angesehen werden kann, muss der Stichprobenanbieter folgende Informationen bereitstellen:

- eine Beschreibung der Art der Stichprobenquellen, die genutzt werden sollen; und
- eine Schätzung des Prozentsatzes der Stichprobe, die voraussichtlich aus Panel- bzw. Nicht-Panel-Quellen stammen werden.

Forscher müssen außerdem sicherstellen, dass die mit einem Unterlieferanten geteilten, personenbezogenen Angaben auf solche beschränkt werden, die für die Durchführung der Unteraufträge notwendig sind; dass der Unterlieferant die notwendigen Datensicherheitsverfahren anwendet, um die Daten zu schützen; und dass die Verantwortlichkeiten des Unterlieferanten in Bezug auf diesen Datenschutz eindeutig protokolliert und vereinbart werden.

4.2 Schutz von personenbezogenen Angaben

Forscher müssen sicherstellen, dass die persönliche Identität von Teilnehmern nicht für Kunden offengelegt wird. Außer geltende Datenschutzgesetze und/oder -vorschriften stellen höhere Anforderungen, ist es dem Forscher nur dann erlaubt, Informationen zur Identifizierung von Personen an den Kunden weiterzugeben, wenn die folgenden Bedingungen erfüllt werden:

- der Forschungsteilnehmer hat seine ausdrückliche Einwilligung erteilt;
- es handelt sich ausschließlich um Forschungszwecke; und
- es werden aufgrund der Bereitstellung dieser Informationen keinerlei Marketing- oder Verkaufsaktivitäten an den Teilnehmer weitergeleitet.

Weiterhin ist es von grundlegender Bedeutung, dass Forscher eine schriftliche Garantie von deren Kunden erhalten, dass diese keinerlei Versuche unternehmen werden, die Identität von Teilnehmern in Erfahrung zu bringen, außer die oben genannten Bedingungen wurden erfüllt.

4.3 Transparenz, Falschdarstellung und Fehlerbehebung

Alle Forschungsprojekte müssen eine präzise, transparente und objektive Berichterstattung aufweisen. Sollten nach der Lieferung Fehler entdeckt werden, muss der Kunde unmittelbar kontaktiert und Korrekturen sofort vorgenommen werden.

Weitere Informationen über die Anforderungen an die Berichterstattung finden Sie in Abschnitt 6 dieses Dokumentes – „Methodologische Qualität“.

5 DIE BREITE ÖFFENTLICHKEIT: BEZIEHUNGEN UND VERANTWORTLICHKEITEN

5.1 Aufrechterhaltung des öffentlichen Vertrauens

Forscher müssen nachprüfen, dass in den von Stichprobenanbietern oder Kunden bereitgestellten Stichproben ausschließlich Einzelpersonen vertreten sind, die auf angemessene Weise eine Kontaktaufnahme für die Teilnahme an Forschungsstudien via E-Mail oder SMS erwarten. Andere Technologien zur Nachrichtenübermittlung, wie beispielsweise mobile Applikationen (mobile Apps) für Benachrichtigungen, können ähnliche Eigenschaften und Fähigkeiten wie SMS-Nachrichten aufweisen. Siehe Abschnitt 3.5 für weitere Informationen.

5.2 Veröffentlichung von Ergebnissen

Wenn ein Kunde plant, die Ergebnisse eines Forschungsprojektes zu veröffentlichen, dann sind sowohl der Kunde als auch der Forscher verantwortlich dafür sicherzustellen, dass die veröffentlichten Ergebnisse nicht irreführend sind. Daher werden Kunden nachdrücklich dazu aufgefordert, sich mit dem Forscher über das Format und die Inhalte der Veröffentlichung der Ergebnisse zu beraten.

Forscher müssen auf Anfrage ebenso in der Lage sein, ausreichend technische Informationen für die Validitätsprüfung der veröffentlichten Ergebnisse zur Verfügung zu stellen. Dies beinhaltet relevante Informationen über den Hintergrund der Studie, die Stichprobenquelle, die Methode der Datenerfassung, die Formulierungen aller genutzten Fragen, alle angewandten Gewichtungsmethoden und alle Tabellen oder sonstige Analyseergebnisse, über die in der Veröffentlichung Bericht erstattet wurde.

Forscher dürfen nicht erlauben, dass deren Namen mit der Verbreitung von Ergebnissen eines Marktforschungsprojekts in Verbindung gebracht werden, außer diese werden auf angemessene Art und Weise von den Daten unterstützt.

6 METHODOLOGISCHE QUALITÄT

Wenn die Nutzer von Online-Forschung darauf vertrauen sollen, dass die Ergebnisdaten ihren Zweck erfüllen, dann müssen Forscher diesen Nutzern angemessene Informationen darüber verfügbar machen, wie die Forschung durchgeführt wurde, einschließlich aller Einschränkungen in der Methodologie, die möglicherweise zu nicht von den Daten unterstützten Schlussfolgerungen führen könnten. Diese Informationen sollten Folgendes beinhalten:

- Stichprobengröße, - quelle und -verwaltung;
- Stichprobendesign und -auswahl;
- die Methode der Datenerfassung;
- alle möglicherweise angewandten Arten von Datenbereinigung, Gewichtung oder Anpassung nach der Feldarbeit; und

- für Online-Forschungen in Ländern mit geringer Internetverbreitung müssen Schritte eingeleitet werden, um sicherzustellen, dass die Ergebnisse die Zielpopulation der Studie repräsentieren.

Nachfolgend finden Sie die Mindestanforderungen. Für weitere Informationen ziehen Sie bitte die ESOMAR/GRBN Richtlinie für hochwertige Online-Stichproben zu Rate.

6.1 Stichquelle und -verwaltung

Die wichtigsten Kategorien der Online-Stichprobenbeschaffung sind:

- Online-Panels: ein Stichprobenanbieter hat ein Panel oder mehrere Panels entwickelt, aus dem oder denen eine Stichprobe erstellt wird;

- River-Stichprobe oder dynamisch generierte Stichprobe: aus einer Verkehrsquelle aus dem Internet;

- Listen-Stichproben: beispielsweise Verbraucherlisten, Mitglieder eines Berufsverbandes, Studenten einer bestimmten Universität usw.

In jedem Fall muss der Stichprobenanbieter in der Lage sein, dem Forscher Details über die Rekrutierung der Stichprobe und eine Beschreibung des Stichprobenrahmens bereitzustellen, sowie zu erklären, wie gut die Stichprobe die Zielpopulation abdeckt, deren Repräsentation beabsichtigt wurde. (Wenn die Stichprobe beispielsweise „national repräsentativ“ ist, dann müssen die präzise, für die Stichprobe verwendete Definition von „national repräsentativ“, sowie die demographischen, geografischen oder sonstigen Gruppen, die wahrscheinlich in der Stichprobe unterrepräsentiert sind, bereitgestellt werden.) Zusätzlich sollten Forscher in deren Berichten gegebenenfalls die Fertigstellungs- und Abbruchsraten, sowie die Antwortraten einschließen (z. B. im Fall von Listen-Stichproben), um die potenzielle Schweigeverzerrung zu bewerten zu können.

Der Stichprobenanbieter muss ebenso in der Lage sein, Informationen über die Verfahren bereitzustellen, die genutzt wurden, um die Qualität der gegebenen Antworten und der erfassten Daten zu garantieren. Dies beinhaltet:

- für die Validierung der Stichprobenquellen unternommene Schritte;

- die Verfahren, die für die „Eingliederung“ potenzieller Teilnehmer in Panels, Communities oder Listen genutzt wurden;

- Bereinigung und Aktualisierung von Verfahrensweisen;

- alle Arten der Überwachung der individuellen Performance während der Teilnahme an Umfragen oder die Qualitätskontrollen, die genutzt wurden, um „Satisficing“-Verhalten oder Betrug zu minimieren, sowie alle Maßnahmen, die bei Entdeckung solcher Verhaltensweisen zum Einsatz kamen;

- Verfahren der Teilnehmerbetreuung;

- die Verwaltung von Prämien;

- ob und wie neue Quellen in den Stichprobenrahmen integriert wurden;

- und alle Verfahrensweisen, die zur Maximierung der Stichprobenkonsistenz für die Nachverfolgung von Projekten angewandt wurden.

6.2 Stichprobenauswahl und -design

Um sicherzustellen, dass abgeschlossene Interviews die Zielpopulation und die Zielsetzung des Forschungsdesigns repräsentieren, muss der Forscher alle genutzten Quoten oder jede Zielgruppenauswahl dokumentieren, einschließlich der Stichprobenmischung, der Nutzung von Stichproben-Routing-Technologien und der den Teilnehmern angebotenen Incentives.

6.3 Datenerfassung

Forscher müssen außerdem angemessene Informationen über die Art und Weise der Datenerfassung mit dem Nutzer der Forschung teilen. Im Falle eines Fragebogens sollten die folgenden Informationen bereitgestellt werden:

- die mittlere oder durchschnittliche Dauer des Fragebogens;
- die Wortwahl der Fragestellungen und alle Filter oder Anweisungen für die Umfrageteilnehmer;
- die Anfangs- und Enddaten der Datenerfassung;
- ob der Fragebogen dazu entwickelt wurde, auch von Teilnehmern über Smartphones oder Tablets ausgefüllt zu werden und falls nicht, ob diese Einzelpersonen von der Stichprobe ausgeschlossen wurden oder an der Umfrage teilgenommen haben, auch wenn diese nicht für deren Gerät optimiert worden ist; und
- alle Notwendigkeiten, besondere Aufgaben durchzuführen, wie beispielsweise das Herunterladen einer Software oder das Teilen sensibler Informationen oder personenbezogener Angaben.

6.4 Datenbereinigung und -gewichtung

Der Forscher muss dokumentieren, auf welche Art und Weise die Daten bereinigt und ob abgeschlossene Interviews aus den Daten entfernt wurden und falls ja, warum. Außerdem müssen die entsprechenden Informationen über Gewichtungen und andere Anpassungen beinhaltet sein. Wenn Imputation genutzt wurde, dann muss eindeutig dargestellt werden, welche Variablen vervollständigt wurden, in welchem Ausmaß dies geschehen ist und welche Imputationsmethoden genutzt wurden.

7 WEITERE HANDLUNGSRICHTLINIEN

7.1 Datenerfassung von Kindern

Die Datenerfassung von Kindern erfordert die Einwilligung eines Elternteils oder Erziehungsberechtigten. Nationale Vorschriften, die die Altersgrenze festlegen, ab der eine solche Einwilligung nicht mehr notwendig ist, weichen sehr stark voneinander ab. Forscher müssen sich über die nationalen Gesetze und selbstregulatorischen Richtlinien in den Rechtssystemen informieren, in denen die Daten erfasst werden, um festzulegen, ob eine elterliche Einwilligung notwendig ist oder ob kulturelle Befindlichkeiten eine bestimmte Handlungsweise erforderlich machen.

Bei der Kontaktaufnahme mit einem potenziellen Forschungsteilnehmer, von welchem vernünftigerweise erwartet werden kann, dass es sich um ein Kind handelt, muss der Forscher vor allen anderen personenbezogenen Angaben zuerst nach dessen Alter fragen. Wenn das angegebene Alter unter der national festgelegten Definition eines Kindes liegt, dann darf dieses Kind nicht darum gebeten werden, weitere personenbezogene Angaben zu teilen, bis eine angemessene Einwilligung vorliegt. Der Forscher darf das Kind um die Bereitstellung der Kontaktdetails seiner Eltern oder Erziehungsberechtigten bitten, um auf diese Weise die Einwilligung einzuholen.

Bei der Bitte um Einwilligung muss der Forscher ausreichende Informationen über die Art des Forschungsprojektes bereitstellen, damit der Elternteil oder Erziehungsberechtigte in der Lage ist, eine informierte Entscheidung über die Teilnahme des Kindes zu treffen. Dies beinhaltet:

- den Namen und die Kontaktdaten des Forschers/der Organisation, der/die die Forschung durchführt;
- die Art der Daten, die von dem Kind erfasst werden sollen;
- eine Erklärung zur Nutzung der Daten;
- eine Erklärung, warum das Kind um seine Teilnahme gebeten wurde und die wahrscheinlichen Vorteile oder möglichen Auswirkungen;
- eine Beschreibung des Verfahrens für das Geben und Überprüfen einer Einwilligung; und
- die Bitte um die Kontaktadresse oder Telefonnummer eines Elternteils oder Erziehungsberechtigten für die Überprüfung der Einwilligung.

Der Forscher sollte ebenso die Identität des Erziehungsberechtigten und seine oder ihre Beziehung zu dem Kind protokollieren.

Es sollte Eltern empfohlen werden, die Identität ihres Kindes während seiner/ihrer Teilnahme an der Umfrage vertraulich zu halten, nachdem dieser Teilnahme zugestimmt worden ist und, falls notwendig, zur Unterstützung des Kindes bereitzustehen und ihm/ihr bei Bedarf beim Ausfüllen der Umfrage zu helfen.

Es muss besondere Sorgfalt in Bezug auf das Forschungsthema (einschließlich wichtiger Elemente wie sensible Themen, die für junge Teilnehmer oder die Eltern beunruhigend sein könnten) walten gelassen werden, wie auch auf das Design des Forschungsfragebogens (angepasst auf die spezifischen Eigenschaften des Kindes – Alter, Maß an Verständnis, sowohl den Elternteil/Erziehungsberechtigten als auch das Kind darüber informierend, dass die Beantwortung bestimmter Fragen nicht verpflichtend ist usw.).

Vorherige Einwilligung durch einen Elternteil oder Erziehungsberechtigten ist nicht notwendig für:

- die Erfassung der E-Mail-Adresse eines Kindes oder Elternteils, wenn diese ausschließlich dafür genutzt wird, um über die Datenerfassung zu informieren und die Einwilligung einzuholen; oder
- die Erfassung des Alters des Kindes zum Zwecke der Vorauswahl und des Ausschlusses. Wenn diese Vorauswahl zur Entscheidung führt, dass sich das Kind für das Interview qualifiziert, dann muss von dem Elternteil oder Erziehungsberechtigten die Einwilligung eingeholt werden, um das Interview durchzuführen.

7.2 Online-Technologien für Identifikation und Tracking

Eine Reihe von Technologien, die für Online-Marketingaktivitäten genutzt werden, finden auch in der Forschung Anwendung, zum Beispiel das Online-Tracking. Die Nutzung dieser Technologien für Forschungszwecke ist eine Form der passiven Datenerfassung, die normalerweise Folgendes beinhaltet:

- Verbesserung der Integrität von Online-Stichproben;
- Vorbeugung von Betrug; oder

- Anwendungen in der Forschung, einschließlich, aber nicht beschränkt auf, Messungen des Online-Publikums und der Inhalte sowie dem Testen von Werbeanzeigen. In diesen und ähnlichen Fällen ist die Einwilligung des Teilnehmers erforderlich.

7.2.1 Spezifische Technologien und Anforderungen für die Nutzung in der Forschung

Diese beinhalten:

- Cookies;
- Local Shared Objects (auch Flash-Cookies genannt);
- Zählpixel; und
- digitale Fingerabdrücke und Geräte-ID.

Da einige dieser Technologien auch für Marketingaktivitäten, wie beispielsweise für das so genannte Online Behavioural Targeting genutzt werden, hat deren Nutzung zur Überprüfung von Gesetzgebern, Aufsichtsbehörden und privaten Gruppen geführt, die sich besorgt über das Potenzial gezeigt haben, das die Überwachung der Online-Aktivitäten von Einzelpersonen ohne deren Wissen in sich trägt.

Wo immer dies möglich ist, muss eine Einwilligung eingeholt und darüber informiert werden, wie personenbezogene Daten erfasst, genutzt und protokolliert werden. Dies ist von besonderer Wichtigkeit in Fällen, in denen ein Forscher einen Forschungsteilnehmer darum bittet, eine Software auf sein oder ihr Gerät herunterzuladen. „Active Agent"-Technologien dürfen nur mit der ausdrücklichen Einwilligung des Forschungsteilnehmers eingesetzt werden.

Außer in Fällen, in denen die direkte Einwilligung oder eine andere, existierende Vereinbarung (wie beispielsweise die Nutzungsbedingungen) eine anderweitige Handhabung erlauben, gilt Folgendes:

- Daten dürfen nur in zusammengefasster Form als Bericht weitergegeben oder geteilt werden und es muss ein Vertrag mit dem Empfänger dieser Daten abgeschlossen werden, in welchem der Letztgenannte zustimmt, keinerlei Versuche zu unternehmen, die Einzelpersonen rückwirkend zu identifizieren (siehe 4.2);
- personenbezogene Angaben dürfen niemals mit Drittparteien geteilt werden (einschließlich Kunden); und
- Daten müssen anonymisiert werden, sobald sie nicht mehr gebraucht werden. Sollte eine Anonymisierung nicht möglich sein, dann müssen diese Daten mithilfe der allgemein anerkannten Best Practices abgesichert werden.

In Fällen, in denen Online-Tracking- und Identifikationstechnologien zur Forschung eingesetzt werden, darf dies nur zu Forschungszwecken geschehen und die vorrangigen Prinzipien der Marktforschungen müssen Anwendung finden (siehe Abschnitt 3.1 für weitere Erläuterungen). Außerdem müssen Forscher die geltenden Gesetze, Vorschriften und lokalen Verhaltensregulierungen der Branche einhalten.

7.3 Mobile Forschung

Im Allgemeinen wird mobile Marktforschung als eine Methode betrachtet, die von der in dieser Richtlinie behandelten Online-Forschung abzugrenzen ist. Sowohl ESOMAR als auch GRBN haben speziell für die mobile Marktforschung geltenden Richtlinien veröffentlicht.

Jedoch entscheidet sich ein erheblicher Teil der für Online-Forschungsstudien kontaktierten Teilnehmer dafür, mithilfe eines Mobilgerätes, wie zum Beispiel eines Smartphones oder Tablets, zu antworten. Dies hat zur Folge, dass Forscher die Grenzen von Smartphones bei der Entwicklung von Online-Umfragen berücksichtigen sollten (z. B. Bildschirmgröße und Downloadgeschwindigkeiten).

7.4 Social-Media-Forschung

Die Entstehung der sozialen Medien in den vergangenen Jahren hat die Art und Weise verändert, in der hunderte Millionen Menschen weltweit Informationen über sich selbst mit anderen teilen. Das Konzept von Verbrauchern, die im Internet ihre eigenen Inhalte erschaffen, ist heute allgegenwärtig. Dies hat für Forscher neue Gelegenheiten zum Beobachten, Interagieren und Sammeln von Informationen geschaffen. Es wurden bereits zahlreiche Techniken entwickelt, um soziale Medien wirksam einzusetzen, beispielsweise Community Panels, Online-Communities für die Marktforschung, Crowdsourcing, Co-Creation, Netnographie, Blog-Analysen und Web Scraping. Zudem ist es wahrscheinlich, dass in Zukunft noch mehr solcher Techniken entstehen, während sich das Internet immer weiter entwickelt.

Forscher müssen deren Beobachtungen mithilfe der gleichen grundlegenden, ethischen und fachbezogenen Prinzipien durchführen, die auch für Face-to-Face-, E-Mail- und Telefonforschung gelten.

Daten aus sozialen Medien beinhalten häufig Informationen zur Identifizierung von Personen. Viele Vorschriften in diesem Bereich wurden in einer Zeit entwickelt, in der es für eine Person noch nicht möglich war, mit vielen anderen über öffentlich zugängliche Online-Plattformen zu kommunizieren. Aktualisierungen in Gesetzen zum Schutz der Privatsphäre und persönlicher Daten befinden sich noch in Arbeit und bleiben häufig hinter praktischen Veränderungen zurück, die sich bereits gemeinhin durchgesetzt haben.

Nichtsdestoweniger ist es die Aufgabe von Forschern, die existierenden, lokalen Vorschriften oder Branchenkodizes des Rechtssystems zu konsultieren, in dem die Forschung geplant wird. Ziehen Sie für weitere Informationen bitte Abschnitt 3.2.1 zu Rate.

7.5 Neue Arten von personenbezogenen Daten

Forscher müssen anerkennen, dass Fotos, Audio- und Videoaufnahmen zu den personenbezogenen Angaben gehören und auch als solche behandelt werden müssen. In Fällen, in denen eine digitale Abbildung das eindeutig sichtbare Gesicht einer Einzelperson enthält, so dass eine Identifizierung dieser Person möglich ist, gilt diese Abbildung als personenbezogene Angabe. Dementsprechend müssen alle in einem Forschungsprojekt gesammelten, verarbeiteten und gespeicherten Fotos, Video- und Audioaufnahmen als personenbezogene Angaben behandelt und entsprechend geschützt werden. Diese dürfen nur mit einem Kunden oder Nutzer der Forschungsarbeiten geteilt werden, wenn der Teilnehmer seine Einwilligung hierfür gibt. In diesem Falle ist eine Weitergabe nur für Forschungszwecke erlaubt. Informationen, die auf angemessene Weise anonymisiert wurden (wie beispielsweise durch Verpixelungs- oder Stimmmodifizierungstechnologien), damit diese Personen nicht mehr als identifizierbar gelten, dürfen mit Kunden oder Nutzern von Forschungsarbeiten geteilt werden.

Lesen Sie auch die ESOMAR Datenschutz-Checkliste für weitere Informationen.

7.6 Business-to-Business-Forschung

Eine beachtliche Anzahl von Forschungsprojekten beinhaltet die Datenerfassung von juristischen Personen, wie beispielsweise Unternehmen, Schulen und Wohltätigkeitsorganisationen. Solche Forschungsstudien umfassen häufig die Erfassung von Informationen über die Organisation selbst, wie beispielsweise Einnahmen, Mitarbeiteranzahl, Branche, Standort und so weiter.

In jedem dieser Fälle genießen die teilnehmenden Organisationen das gleiche Maß an Schutz vor Identitätsoffenlegung in Berichterstattungen wie alle Einzelpersonen in anderen Arten von Forschung auch.

An dieser Stelle sollte auch erwähnt werden, dass zahlreiche nationale Datenschutzgesetze auch die Anrede und die Kontaktinformationen des Arbeitsplatzes einer Einzelperson zu den personenbezogenen Angaben zählen. Einige Datenschutzgesetze gehen noch einen Schritt weiter und wenden diese Vorschriften sowohl auf natürliche als auch juristische Personen an (d. h. Einzelpersonen und Rechtspersonen). Jedoch haben Rechtspersonen im Gegensatz zu Forschungsteilnehmern keine gesetzlichen Zugriffsrechte auf deren Angaben.

7.7 Cloud-Speicherung

Die Entscheidung, personenbezogene Angaben in der Cloud zu speichern, sollte sorgfältig überdacht werden. Forscher müssen die Sicherheitskontrollen und standardmäßigen Geschäftsbedingungen des Anbieters von Cloud-Speichermöglichkeiten überprüfen und in der Lage sein, zusätzliche Kontrollmechanismen in Kraft zu setzen, falls die Kontrollen des Anbieters nicht ausreichend sind. Beispielsweise sollten Forscher personenbezogene Angaben sowohl verschlüsseln, während sich diese in Bewegung (Übertragung in die/aus der Cloud) und als auch im Ruhezustand (auf den Cloud-Servern des Anbieters gespeichert) befinden.

Forscher müssen ebenso die physischen Standorte berücksichtigen, an denen personenbezogene Angaben gespeichert werden, und festlegen, ob die Nutzung der Cloud-Speicherung als grenzüberschreitende Übertragung gilt. In Fällen, in denen personenbezogene Angaben von einem Rechtssystem in ein anderes übertragen werden, muss dies auf eine Art und Weise geschehen, die die Datenschutzanforderungen beider Rechtssysteme erfüllt, d. h. sowohl das Ursprungs- als auch des Ziellandes. Aus diesem Grund muss der Forscher alle geltenden nationalen und lokalen Gesetze und Vorschriften überprüfen und verstehen, um eine Entscheidung über die angemessenen Maßnahmen treffen zu können.

Forscher sollten ernsthaft in Erwägung ziehen, personenbezogene Angaben eher einer privaten Cloud anstelle einer öffentlichen Cloud zu speichern. In einer privaten Cloud werden dem Unternehmen des Forschers spezielle Ausrüstungen zugeordnet und der Forscher weiß immer, an welchem Standort sich die personenbezogenen Angaben befinden.

Im Gegensatz dazu kann es bei einer öffentlichen Cloud der Fall sein, dass Daten über zwei oder mehr Rechenzentren oder zwei oder mehr Länder oder Kontinente verteilt werden, was wiederum zu Problemen bei der Einhaltung sowohl der geltenden Vorschriften von Datenschutzgesetzen, als auch der Verträge führen kann, die mit den Datenverantwortlichen abgeschlossen wurden und in denen festgelegt worden ist, an welchem Standort personenbezogene Angaben gespeichert werden müssen (siehe die ESOMAR Datenschutz-Checkliste für weitere Informationen).

Und schließlich empfiehlt es sich auch noch, dass Forscher den Abschluss einer Cyber-Haftpflichtversicherung in Betracht ziehen. Viele Anbieter von Cloud-Speicherdiensten bieten für den Fall, dass sie selbst Sicherheitsverletzungen oder Sicherheitsbeeinträchtigungen für personenbezogene Daten verursachen, nur geringe Entschädigungen an. Dies bedeutet, dass die Organisation des Forschers ein beträchtliches Risiko finanzieller Schäden oder Verluste aufgrund schwerwiegender Datenschutzverletzungen auf sich nimmt, die zur Schädigung der betroffenen Einzelpersonen führen.

7.8 Anonymisierung und Pseudonymisierung

Ein wichtiger Teil der Verantwortlichkeit eines Forschers in Bezug auf den Datenschutz ist die Anonymisierung der Daten vor deren Freigabe an einen Kunden oder auch die breite Öffentlichkeit. Anonymisierung ist eine Schutzmaßnahme, die entweder das Löschen oder

die Modifizierung persönlicher Identifikatoren beinhaltet, um Daten in eine Form zu bringen, in der die Identifikation von Einzelpersonen nicht mehr möglich ist. Beispiele sind das Unkenntlichmachen von Abbildungen, um Gesichter zu verbergen, oder das Berichten von Ergebnissen in Form von zusammengefassten Statistiken, um es so unmöglich zu machen eine Einzelperson zu identifizieren.

Pseudonymisierung ist das Bearbeiten personenbezogener Daten auf eine Art und Weise, in der es noch möglich ist, Einzelpersonen aus einem Datensatz zu identifizieren, beispielsweise mithilfe eines einzigartigen Identifikators wie einer Ausweisnummer, oder über Hash-Algorithmen, bei gleichzeitiger, separater Speicherung der personenbezogenen Daten zum Zwecke der Überprüfung.

Bei der Anwendung solcher Techniken sollten Forscher die lokalen, nationalen Gesetze und selbstregulatorischen Kodizes überprüfen, um festzulegen, welche Elemente entfernt werden müssen, um den rechtlichen Anonymisierungs-/Pseudonymisierungsstandards für solche Daten gerecht zu werden.

7.9 Nutzung statischer und dynamischer Identifikationsnummern

In der Vergangenheit wurden statische Identifikatoren von Forschungsteilnehmern (statische Identifikationsnummern) von Forschungskunden und Stichprobenanbietern genutzt, um die Kontrolle und Zuordnung von Forschungsteilnehmern innerhalb spezifischer Studien zu unterstützen, sowohl bei Längsschnitt- als auch Ad-hoc-Studien. Diese Technik hat dabei geholfen, Informationen über jeden Teilnehmer zu konsolidieren und wurde zu einem nützlichen Ansatz, um sicherzustellen, dass die Teilnehmer in einer einzelnen Längsschnittstudie einzigartig sind und die Ausschlussfristen der Forschungsstudie eingehalten werden. Zusätzlich zur Verbesserung der Qualitätskontrolle und der Überwachung der Ausschlussfristen und Stichprobenauswahl, sowie der Möglichkeit einzelne Forschungsteilnehmer für Studien präzise identifizieren zu können, benötigen einige Forscher die statischen Identifikationsnummern ebenso zur Unterstützung von deren Datenanalysen.

Die Nutzung dynamischer Identifikationsnummern (variable Identifikationsnummern für jede Nutzung) wurde von einigen Stichprobenanbietern als Methode beworben, um die Identitätssicherung von deren individuellen Mitgliedern zu unterstützen und die Möglichkeit zu verhindern oder zu reduzieren, dass skrupellose Kunden die Daten von Forschungsteilnehmern zusammen mit anderen, während der Teilnehmerinterviews erfassten Daten (Paradaten) nutzen, um zusätzliche Einsichten zu gewinnen oder zu versuchen, die tatsächliche Identität des Teilnehmers zu enthüllen.

Forscher sollten die Nutzung jeder Art von Identifikationsnummer und die Bedenken in Bezug auf Datenschutz und Forschungsqualität für deren spezifische Studie sorgfältig abwägen. Rechtliche und vertragliche Bestimmungen sollten angewandt werden, um die Erfassung und Nutzung der durch die Studie erhaltenen Informationen innerhalb der vertraglichen Grenzen zu kontrollieren, die in den zwischen allen Parteien (Forschungsteilnehmer, Stichprobenanbieter, Forscher, Endkunde) abgeschlossenen Vereinbarungen festgelegt wurden.

7.10 Nutzung und Kontrollen von Paradaten

Es wird empfohlen, dass die Nutzung von Paradaten in einer beidseitigen, rechtlichen Vereinbarung zwischen dem Stichprobenanbieter und dem Kunden festgelegt wird, um die Erfassung, Nutzung und weitere Übertragung dieser Daten in dem nachfolgenden Forschungsprozess anzuleiten, einzuschränken und zu schützen.

7.11 Inakzeptable Handlungsweisen

Nachfolgend finden Sie eine Liste inakzeptabler Handlungsweisen, die von Forschern strengstens verboten oder verhindert werden müssen. Die Durchführung einer oder mehrerer der folgenden Handlungen durch Forscher gilt als Nutzung von Spyware:

- Herunterladen von Software ohne die Einwilligung des Forschungsteilnehmers;
- Herunterladen von Software ohne die Bereitstellung einer kompletten, eindeutigen, präzisen und sichtbaren Mitteilung und Bekanntgabe über die Arten von Informationen, die erfasst werden, sowie die nachfolgende Nutzung dieser Informationen.
- Die Nutzung von Keyloggern (dt. „Tasten-Protokollierern“) ohne die vorherige Einwilligung des Teilnehmers;
- Die Installation von Software, die die Einstellungen des Computers des Teilnehmers über das Maß hinaus verändert, das für die Durchführung der Forschungsstudie notwendig ist;
- Die Installation von Software, die Anti-Spyware-, Antivirus- oder Antispam-Software ausschaltet oder die Kontrolle über den Computer oder das Gerät des Teilnehmers ergreift oder übernimmt;
- Nicht alle angemessenen Anstrengungen unternehmen, um sicherzustellen, dass die Software nicht zu Konflikten mit den wichtigsten Betriebssystemen oder zu fehlerhaften oder unerwarteten Reaktionen von sonstigen, installierten Software führt.
- Die Installation von Software, die in einer zweiten Software versteckt wurden, die wiederum heruntergeladen werden kann oder deren Deinstallation schwierig ist; oder die Installation einer Software, die Werbeinhalte anbietet, um auf diese Weise Werbewirkungsforschung zu betreiben;
- Die Installation von Softwareaktualisierungen ohne eine Benachrichtigung der Nutzer und der Möglichkeit für Teilnehmer, sich gegen eine solche Aktualisierung zu entscheiden;
- Das Verändern der Art der Identifikations- und Trackingtechnologien ohne eine Benachrichtigung der Nutzer;
- Das Versäumnis, die Nutzer über Änderungen in den Datenschutzpraktiken in Zusammenhang mit Softwareaktualisierungen zu informieren;
- Das Nachverfolgen von Inhalten von Teilnehmer-E-Mails;
- Das Nachverfolgen von Verhaltensweisen ohne die vorherige Einwilligung durch den Teilnehmer in dem Fall, dass dessen Browser in einen Privatmodus gesetzt wurde.
- Das Erfassen personenbezogener Daten ohne die vorherige Einwilligung, wenn sich der Teilnehmer auf einer verschlüsselten Webseite befindet (d. h. auf einer SSL-Webseite).

8 REFERENZEN

- ESOMAR Datenschutz-Checkliste
- ESOMAR/GRBN Richtlinie für hochwertige Online-Stichproben
- Global Research Business Network
- ICC/ESOMAR Internationaler Kodex für Markt- und Sozialforschung
- ISO 20252:2012 – Markt-, Meinungs- und Sozialforschung
- ISO 26362:2009 – Access Panels in der Markt-, Meinungs- und Sozialforschung
- ISO 27001 – Informationstechnologie – Sicherheitstechniken – Informationssicherheitsmanagementsysteme – Anforderungen

9 DAS PROJEKTTEAM

- Reg Baker, Co-Vorsitzender, Berater des ESOMAR Professional Standards Committee, Marketing Research Institute International
- Peter Milla, Co-Vorsitzender, Technischer Berater bei CASRO, Peter Milla Consulting
- Mario Callegaro, Senior-Wissenschaftler im Bereich Umfrageforschung, Google
- Melanie Courtright, stellvertretende Vorsitzende – Global Client Services, Research Now
- Brian Fine, Vorstandsvorsitzender, Quality Online Research
- Phillipe Guilbert, Generaldirektor, Toluna
- Debrah Harding, Geschäftsleiterin, Market Research Society
- Kathy Joe, Leiterin Internationale Standards & Regierungsangelegenheiten, ESOMAR
- Jackie Lorch, Vizepräsidentin – Global Knowledge Management, SSI
- Bruno Paro, Geschäftsleiter, Netquest
- Efrain Ribeiro, Forschungsleiter, Lightspeed Research
- Alina Serbanica, Senior-Vizepräsidentin – Interactive Services, Ipsos