Ethik Richtlinien für Nutzerstudien

Inhalt

1. Einleitung

Diese Richtlinien basieren teilweise auf dem „PD-Net Ethics Primer V1.2“ (http://pd-net.org). Das Original ist Teil des Ethikprozesses, der beschrieben wurde in: Marc Langheinrich, Albrecht Schmidt, Nigel Davies, and Rui José (2013): A Practical Framework for Ethics – the PD-Net Approach to Supporting Ethics Compliance in Public Display Studies. In: Proceedings of the Second International Symposium on Pervasive Displays (Mountain View, CA, June 4-5, 2013). PerDis 2013. ACM, New York, NY.

Ethische Richtlinien für Experimente am Menschen geben Hinweise darauf, wie man mit Menschen und ihren Daten richtig umgeht. Während sich die Informatik typischerweise nicht so mit Experimenten beschäftigt wie beispielsweise die Medizin oder die Psychologie (d.h. direkt mit Individuen experimentiert), werden viele unserer Studien letztendlich Informationen sammeln und speichern, die mit Individuen in Verbindung gebracht werden können oder nicht. Diese Informationen können das physische und psychische Wohlbefinden der Testpersonen beeinträchtigen oder sogar gefährden, wenn sie für unvorhergesehene Zwecke verwendet oder an unberechtigte Dritte weitergegeben werden.

2. Ethischer Prozess

Die Teilnehmer einer Nutzerstudie sollten grundsätzlich eine schriftliche Teilnehmerinformation, und ggf. eine zusätzliche Datenschutzerklärung erhalten. Außerdem müssen die Teilnehmer meistens eine Einverständniserklärung unterschreiben. Die folgende Liste beschreibt die Schritte, die alle Nutzerstudien, Feldversuche, Interviews etc. durchlaufen sollten.

1. **Ethik-Arbeitsblatt** (in diesem Ordner) vor dem geplanten Studienbeginn ausfüllen
2. **Teilnehmerinformation und evtl. Einverständniserklärung** vorbereiten
3. Optional **Datenschutzerklärung** vorbereiten

3. Übersicht Ethischer Grundsätze

Studien und Beobachtungen sollten den 10 unten aufgeführten Grundprinzipien folgen [1].

1. Maximieren Sie den möglichen Nutzen und minimieren Sie mögliche Schäden.
2. Einholung der freiwilligen informierten Zustimmung
3. Sicherstellung des Widerrufsrechts
4. Offenlegung von Nachteilen durch die Teilnahme an der Forschung
5. Gewährleistung von Datenschutz und Privatsphäre
6. Begrenzung der Offenlegung
7. Nach dem Prinzip des minimalen Eindringens
8. Angemessene Anreize bieten
9. Besondere Bestimmungen für Experimente mit Kindern und anderen gefährdeten Personen
10. Vermeidung von Täuschung

Hier benutze Fachbegriffe

- Die **Forschungsteilnehmer** können aktive oder passive Subjekte von Prozessen wie Beobachtung, Untersuchung, Experiment oder Test sein. Sie können Mitarbeiter oder Kollegen im Forschungsprozess sein oder einfach Teil des Kontextes sein, z.B. wenn Passanten Teil des Kontextes sind, aber nicht Gegenstand einer Studie auf dem Campus sind (angepasst an:[1]).

- **Personenbezogene Daten (PII)** sind Daten, die - mit vertretbarem Aufwand - mit einer Person verknüpft werden können. D.h. eine Person kann - mehr oder weniger sicher - von allen anderen Personen unterschieden werden. Beispiele für PII sind z.B. der Vor- und Nachname, eine Privatadresse oder andere Adressen, eine E-Mail-Adresse und eine Telefonnummer. Auch ein scheinbar zufälliger Identifikator, wie beispielsweise eine IP-Adresse oder eine Bluetooth-MAC-Adresse, kann zu PII werden, wenn diese wiederum mit anderen PII, wie beispielsweise einer physikalischen Adresse, verknüpft werden können. Die für die Verknüpfung erforderlichen Informationen können sich in einer öffentlichen Datenbank befinden (z.B. gelbe Seiten, Telefonbuch) oder mit vertretbarem Aufwand aus einer anderen Datenbank bezogen werden. Beachten Sie bitte, dass dies auch von der Anzahl der potenziell in Frage kommenden Nutzer Nutzer abhängt: Wenn an einem Experiment nur Mitglieder einer bestimmten Abteilung beteiligt sind, kann die Kenntnis auch eines relativ harmlosen Datenpunkts wie "Körpergröße" bereits PII darstellen.

- **Anonymisierung, Pseudonymisierung und Identifizierbarkeit (ab[4]): "**Anonymisierung" bedeutet Daten, die eine Person nicht identifizieren; "anonymisiert" bedeutet Daten, die anonymisiert wurden; "pseudonymisiert" und "verschlüsselt" bedeutet Daten, bei denen offensichtliche Identifikatoren (z.B. Namen und Adressen) durch indirekte Identifikatoren (z.B. Nummern) im Hauptdatensatz ersetzt wurden und die indirekten Identifikatoren dann mit den offensichtlichen Identifikatoren in einem separaten Datensatz (bekannt als "Schlüssel") gehalten werden. Der Schlüsselbegriff, der allen oben genannten Definitionen im Rahmen des europäischen Datenschutzrechts zugrunde liegt, ist die "Identifizierbarkeit" einer Person aus den Daten. Damit das europäische Datenschutzrecht die Forschung über personenbezogene und sensible personenbezogene Daten verbindlich macht, muss man sich fragen: Wird die Person entweder sofort aus den Daten identifiziert oder wenn diese Daten mit anderen Daten in den Händen einer anderen Person kombiniert werden? Diese Kombination erstreckt sich nur auf vorhersehbare Verknüpfungen von Daten. Daher werden Daten, die anonym und ohne Identifikatoren erhoben werden, außerhalb des europäischen Datenschutzrechts liegen; Daten, die pseudonymisiert oder verschlüsselt sind, werden im Rahmen des Gesetzes behandelt, da es möglich ist, die beiden getrennten Datensätze wieder einzuführen und Personen zu identifizieren; Daten, die als identifizierbare Daten erfasst und dann anonymisiert

wurden, unterliegen dem Datenschutzrecht, wenn sie identifizierbare Daten enthalten (vor allem zum Zeitpunkt der Datenerhebung, die die Offenlegung von Informationen durch den Forscher an den Forschungsteilnehmer erfordern, einschließlich des Zwecks der Verarbeitungs- und Kontaktdaten).

- **Sensible Informationen (aus[5]).** Zu den sensiblen Daten gehören Daten, die "die ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit und die Verarbeitung von Daten über Gesundheit oder Sexualleben" (Artikel 10 der Verordnung 45/2001; Artikel 8 der Richtlinie 95/46/EG) offenlegen. Die Verarbeitung dieser Informationen ist grundsätzlich verboten, es sei denn, die betroffene Person hat ausdrücklich zugestimmt. Die Verarbeitung und Speicherung sensibler Daten erfordert ein deutlich höheres Sicherheitsniveau.

4. Erklärung der Grundsätze

Keinen Schaden zufügen

Eines der grundlegendsten Prinzipien der ethischen Forschung ist das Schadensprinzip. Sie geht auf den Bericht Belmont von 1979 zurück[7], in dem ethische Grundprinzipien festgelegt sind, die allen Arten der Verhaltensforschung am Menschen zugrunde liegen sollten. Der Bericht nennt drei Grundprinzipien: Autonomie, Nützlichkeit und Gerechtigkeit. Das letzte Prinzip (Gerechtigkeit) besagt einfach, dass sowohl die Risiken als auch der Nutzen der Forschung gleichmäßig verteilt werden sollten. Dies kann z.B. bei der Auswahl von Teilnehmern relevant werden. Das Leistungsprinzip verpflichtet den Forscher dann, das Wohlbefinden aller ausgewählten Teilnehmer zu sichern, d.h. "den möglichen Nutzen zu maximieren und mögliche Schäden zu minimieren". In der Praxis muss jede Studie explizit mögliche Risiken für die Teilnehmer auflisten und erläutern, wie ihre negativen Auswirkungen gemildert werden (z.B. unfreiwillige Weitergabe personenbezogener Daten). Diese Informationen müssen auch potenziellen Teilnehmern vor der Einschreibung mitgeteilt werden, was das erste der drei Prinzipien, Autonomie, unterstützt und im nächsten Punkt erläutert wird.

Informierte Einverständniserklärung

Das erste der drei Belmont-Grundsätze, Autonomy, besagt, dass jedem Teilnehmer der Respekt, die Zeit und die Gelegenheit gegeben werden sollte, seine eigenen Entscheidungen zu treffen, um "sicherzustellen, dass er frei und im Bewusstsein möglicher negativer Folgen tätig ist". Dieses Prinzip wird durch ein so genanntes Informierte Einverständniserklärung-Verfahren umgesetzt. Die Zustimmung zur Teilnahme an der Forschung ist ein Prozess und keine Veranstaltung[3]. Forscher sollten planen und beschreiben, wie die Zustimmung zunächst eingeholt und wie sie während der gesamten Studie überprüft wird. Um eine sinnvolle Einwilligung zu erteilen, müssen die Teilnehmer auch die Ziele der Forschung, die durchzuführende Studie/Experiment, die gesammelten Daten und die Verwendung dieser Daten verstehen. Während die schriftliche Zustimmung bevorzugt wird, kann die mündliche Zustimmung in einigen Situationen sinnvoller sein, z.B. bei Walk-Up-Interviews an öffentlichen Orten. Beachten Sie, dass der Grundsatz der Einwilligung nach Aufklärung auch den Grundsatz der Offenlegung von Nachteilen und der Gewährleistung des Widerrufsrechts beinhaltet (siehe unten). Eine detaillierte Beschreibung des Aufklärungsverfahrens finden Sie im Leitfaden zur Einholung der informierten Zustimmung.

Recht auf Widerruf

Im Rahmen des oben beschriebenen Verfahrens der informierten Einwilligung müssen potenzielle Teilnehmer über das Recht informiert werden, die Teilnahme an der Studie zu verweigern, und dass sie ihre Einwilligung zur Teilnahme jederzeit ohne Vergeltung widerrufen können[8]. Dazu sollte auch das Recht gehören, sich rückwirkend, d.h. im Lichte der Erfahrungen aus der Untersuchung oder als Ergebnis einer Nachbesprechung, zurückzuziehen. Eine solche Anfrage sollte zur Zerstörung der eigenen Daten der Teilnehmer führen. Es ist zu beachten, dass das bedingungslose Widerrufsrecht von Forschern wiederholt in Frage gestellt wurde[9][10], da es nicht nur Forscher daran hindern könnte, Studienteilnehmer zur Fortsetzung der Teilnahme zu ermutigen, sondern auch zu einer vorherigen Entlassung von potenziellen Abbrüchen aus dem Pool der Studienteilnehmer führen könnte. Wie im obigen Grundsatz der Einwilligung nach Aufklärung beschrieben, sollten die Forscher von während der gesamten Studie einen kontinuierlichen Dialog mit den Teilnehmern suchen, um sicherzustellen, dass die Teilnehmer zwar über den Austritt angemessen informiert werden, aber ausreichend ermutigt werden, fortzufahren.

Offenlegung von Nachteilen

Die Offenlegung möglicher Nachteile durch die Teilnahme ist ein wesentlicher Bestandteil der Einholung der Einwilligung potenzieller Studienteilnehmer. Als Teil des Ethik-Arbeitsblattes Worksheet müssen die Forscher explizit die Risiken für die Untersuchung von Probanden auflisten, die sich aus der Teilnahme ergeben könnten. Diese Informationen müssen den Teilnehmern in den Einwilligungsunterlagen ausdrücklich mitgeteilt werden.

Privatsphäre

Die Datenerhebung, -speicherung und -nutzung von personenbezogenen Daten (PII) im Allgemeinen muss dem EU-Rechtsrahmen (d.h. der Richtlinie 1995/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) sowie den individuellen nationalen Rechtsvorschriften zum Datenschutz entsprechen. Die gesetzlichen Anforderungen an die Verarbeitung von PII umfassen typischerweise die folgenden Aspekte, die grob nach den OECD-Richtlinien von 1980[11] modelliert sind:

1. Die betroffenen Personen sollten benachrichtigt werden, wenn ihre Daten erhoben werden;
2. Die Zweckbestimmung der Daten darf nur für den angegebenen Zweck und nicht für andere Zwecke verwendet werden;
3. Einwilligungsdaten sollten nicht ohne die Zustimmung der betroffenen Person weitergegeben werden;
4. Die sicherheitsrelevanten Daten sollten vor jeglichem Missbrauch geschützt werden;
5. Die betroffenen Personen sollten darüber informiert werden, wer ihre Daten sammelt;
6. Die betroffenen Personen sollten Zugang zu ihren Daten haben und Korrekturen an ungenauen Daten vornehmen können; und
7. Die betroffenen Personen sollten über ein Verfahren verfügen, um die Datensammler für die Einhaltung der oben genannten Grundsätze zur Rechenschaft zu ziehen.

Die Grundsätze der Benachrichtigung, Einwilligung und Offenlegung werden durch das Einwilligungsverfahren abgedeckt (Einholung der Einwilligung in Kenntnis der Sachlage). Dem Zweckprinzip wird durch den konsequenten Einsatz von Ethischen Arbeitsblättern Rechnung getragen, die die individuellen Studienziele explizit beschreiben. Die Sicherheit wird durch die ausdrückliche Angabe der Datenspeicherungs- und Verarbeitungsbedingungen für jede einzelne Studie im Ethik-Arbeitsblatt gewährleistet. Der Zugang und die Rechenschaftspflicht werden

durch die Aufnahme von Zugangs- und Inspektionsmethoden in das Informationsblatt gewährleistet, das im Rahmen der Einwilligung nach Aufklärung verwaltet wird (z.B. die Kontaktdaten des für die Studie verantwortlichen Hauptprüfers und - falls zutreffend - eines lokalen institutionellen Prüfungsausschusses).

Darüber hinaus verlangen die europäischen Datenschutzgesetze das Prinzip der Verhältnismäßigkeit/Datenminimierung - siehe unten das " Minimales Eindringprinzip".

Begrenzung der Offenlegung

Personenbezogene Daten, die im Rahmen einer Studie erhoben werden, werden nur den direkt an der Forschung beteiligten Forschern auf der Grundlage des "need to know" zur Verfügung gestellt. Das Ethik-Arbeitsblatt fordert die Forscher auf, alle Mitglieder des Konsortiums, die an der Durchführung einer bestimmten Studie beteiligt sind, sowie alle externen Forscher ausdrücklich aufzulisten.

Minimales Eindringprinzip

Das Prinzip des "minimalen Eingriffs" oder der "Datenminimierung" bedeutet, dass man die Erfassung personenbezogener Daten auf das beschränken sollte, was direkt relevant und notwendig ist, um einen bestimmten Zweck zu erreichen. Die Daten sollten auch nur so lange aufbewahrt werden, wie es zur Erfüllung dieses Zwecks erforderlich ist. Dieser Grundsatz ergibt sich aus Artikel 6 Absatz 1 Buchstaben b) und c) der Richtlinie 95/46/EG, wonach personenbezogene Daten "für bestimmte, ausdrückliche und rechtmäßige Zwecke erhoben" und "angemessen, relevant und nicht übermäßig im Verhältnis zu den Zwecken, für die sie erhoben und/oder weiterverarbeitet werden", sein müssen. Dies wird auch oft als Verhältnismäßigkeitsprinzip bezeichnet, d.h. "ob die von der zu bewertenden Maßnahme eingesetzten Mittel geeignet und hinreichend wahrscheinlich sind, ihre Ziele zu erreichen"[12]. Für die Forschung bedeutet dies, dass Forscher nur Informationen sammeln sollten, die die Daten liefern, die für die Bearbeitung aktueller Forschungsfragen erforderlich sind. Das Ethik-Arbeitsblatt fordert die Forscher auf, explizit anzugeben, welche Daten in einer Studie erhoben werden sollen (Frage 3.6), und verlangt eine Begründung über die Eignung dieser Daten (und der verwendeten Studienmethoden) für den angegebenen Forschungszweck (Frage 3.4).

Angemessene Anreize

Die Nutzung von Anreizen (Teilnehmervergütungen) zur Rekrutierung und Bindung von Probanden ist in der Regel eher harmlos. Allerdings, wenn die Studienteilnehmer in einer Abhängigkeitsbeziehung mit dem Forscher stehen (z.B. Studenten in einem Kurs), oder wenn die Abneigung des Teilnehmers gegen die Studie stark sein kann (z.B. hohes Risiko, erniedrigende Forschung, grundsätzliche Abneigung)[13]. Anreize sollten nur eine angemessene Vergütung für die Zeit und den Aufwand der Teilnehmer umfassen, z.B. für die Teilnahme an wöchentlichen Treffen. Bei Bedarf können kleine Anreize in Form von Gutscheinen für Online-Shops wie Amazon.com oder iTunes gewährt werden, oder alle Teilnehmer nehmen an einer Verlosung kleinerer Preise teil.

Vermeidung von Täuschung

Der Akt der Täuschung der Studienteilnehmer wird häufig in psychologischen Experimenten eingesetzt, um sicherzustellen, dass die Studienteilnehmer nicht versehentlich ihr "natürliches" Verhalten ändern, um dem Experimentator zu gefallen und/oder sich in einem besseren Licht erscheinen zu lassen. Berüchtigte Beispiele für irreführende Experimente sind das Stanley-Milgram-Experiment von 1974[14] oder Zimbardos Stanford-Gefängnis-Experiment von 1971[15]. Heute ist Täuschung bei der Forschung am Menschen in der Regel nicht mehr

akzeptabel. Die Verwendung von Täuschung gefährdet die Integrität des Prozesses der informierten Zustimmung und kann den Teilnehmern potenziell schaden.

Die Anwendung der Täuschung erfordert daher eine eingehende Begründung, warum die Täuschung für die Studie notwendig ist, und die Maßnahmen zum Schutz der Studienteilnehmer.

Gefährdete Teilnehmer

Gefährdete Teilnehmer sind Personen, die nicht in der Lage sind, ihre eindeutige Einwilligung nach Aufklärung zu erteilen, wie z.B. Kinder, Menschen mit kognitiven Störungen oder Menschen mit kulturellen oder intellektuellen Schwierigkeiten in Sprache und Verständnis. Experimente, die die Teilnahme schutzbedürftiger Teilnehmer anstreben, müssen gerechtfertigt sein. Die Zustimmung der Eltern oder anderer geeigneter Erziehungsberechtigter ist einzuholen.

5. Schriftlichen Teilnehmerinformation

Allgemeine Hinweise

- Das **Sprachniveau** ist dem Alter und dem Leselevel der Teilnehmerpopulation angemessen.
- Die Sprache sollte **allgemein verständlich** sein, also keine komplizierten Fachbegriffe, ohne Erklärungen beinhalten
- Die Teilnehmer erhalten eine **Kopie des Informationsschreibens**, das sie für sich behalten können.

Die schriftliche Teilnehmerinformation sollte die folgenden Punkte abdecken:

- **Titel/Name der Studie:** Präziser Name der Studie, der die untersuchte Problemstellung beschreibt
- **Kurze Beschreibung der Studie:** 3-4 Sätze, die die Studie beschreibt. Diese sollte die benutzten Methoden und eine Problembeschreibung beinhalten.
- **Dauer der Nutzerstudie:** Wie lange wird die Nutzerstudie dauern (inkl. Start- und Enddatum)?
- **Ort der Nutzerstudie:** Sind Präsenztermine für die Nutzerstudie nötig?
- **Evtl. Vergütungen** für die Teilnahme oder die Erstattung von Ausgaben
- **Relevante Ein- und Ausschlusskriterien**
- **Gegebenenfalls die Anzahl der Teilnehmer:** z.B. wenn dies die Vertraulichkeit beeinträchtigen könnte
- **Studienleitung:** Wer ist für die Durchführung der Studie verantwortlich? Nennen Sie hier auch die Institution (z.B. Max Mustermann, Bundeswehr Universität München). Geben Sie hier auch eine Kontaktmöglichkeit mit der Studienleitung an (z.B. E-Mail Adresse)
- **Freiwillige Teilnahme:** jederzeit ist ein zurücktreten oder nicht beantworten von Fragen möglich - alles ohne negative Folgen.
- **Vorhersehbare Risiken, Schäden oder Unannehmlichkeiten**
- **Potenzielle Vorteile** - einschließlich der Information, dass es keinen direkten Nutzen gibt
- **Aufbewahrung und Verwendung** (z.B. Löschung) der Daten während und nach Abschluss der Recherche.
- **Verfahren zur Wahrung der Vertraulichkeit:** z.B. Verwendung von studienspezifischen ID-Nummern, Pseudonymen, etc.
- **Vorhersehbare Einschränkungen der Vertraulichkeit** - z.B. für die Teilnahme an Fokusgruppen, die Recherche mit Schlüsselinformanten oder die Berichtspflicht
- **Gesammelte Daten:** Auflistung aller Daten, die während der Studie von den Teilnehmern erfasst werden. Dies kann auch einen Verweis auf die optionale Datenschutzerklärung der Studie beinhalten.

- **Verwendung von Audio- und Videoaufzeichnungen** sollten als separate Optionen aufgeteilt werden, denen die Teilnehmer zustimmen können (oder nicht).
- **Hinweis auf die Veröffentlichung der Daten:** Erwähnen Sie inwieweit die gesammelten Daten veröffentlich werden.
- Informationen darüber, **wer Zugang zu den Daten hat**
- **Zusammenfassung der Forschungsergebnisse** und ein Mechanismus zur Bereitstellung der Zusammenfassung angeboten werden.

6. Inhalt der Einverständniserklärung

- **Name/Titel der Studie**
- **Name, Vorname und Geburtsdatum des Teilnehmers**
- **Optional: Vergütung**
- **Einzelne Punkte, zu denen das Einverständnis des Teilnehmers abgefragt wird:** Erhalt und Inhalt der Teilnehmerinformation, Video oder Audioaufnahmen, Evtl. Erhalt und Inhalt der Datenschutzerklärung, Teilnahme an der Studie, Erhebung der Daten, Speicherung der Daten, Veröffentlichung der (anoymisierten) Daten
- **Freiwillige Teilnahme:** jederzeit ist ein zurücktreten oder nicht beantworten von Fragen möglich - alles ohne negative Folgen.
- **Evtl. Konsequenzen für Studienabbruch/Widerruf**: Wenn Daten anonymisiert oder entkoppelt sind, können sie nicht entnommen werden; ebenso ist es fast unmöglich, Daten aus einer Fokusgruppen-Diskussion zu entnehmen).
- **Ort, Datum und Unterschrift des Teilnehmers**

7. Inhalt der Datenschutzerklärung

- **Kontaktdaten des Anbieters:** Name, Anschrift und Kotaktmöglichkeit zur Studienleitung
- **Was sind personenbezogene Daten?** Siehe Beispiel Datenschutzerklärung
- **Erklärung des Zwecks der Datenerhebung**: Beschreibung der Studie und der Problemstellung
- **Beschreibung der Daten, während der Studie erhoben werden:** Methodik und detailierte Auflistung aller erhobenen Daten
- **Speicherdauer:** Wie lange werden die Daten gespeichert?
- **Erhebungsdauer:** Studiendauer.
- **Information über Übermittlung an Dritte und deren Zweck**: Geben Sie hier an, ob und inwiefern Daten an Dritte übermittelt werden
- **Rechte des Benutzers:** siehe Beispiel Datenschutzerklärung
- **Datum der Erstellung**

Anhang

Beispiel Probandeninformation

Vielen Dank, dass Sie sich für die Teilnahme an dieser Studie interessieren.

Die Nutzer-Studie dient zu der Evaluation verschiedener Bedrohungsszenarien im Bezug den Authentifizierungsvorgang auf dem persönlichen Smartphone.

Das Thema der Studie lautet dementsprechend:

„User Centered Attacks: Wie sicher ist dein Smartphone wirklich?“

Hierbei werden Daten in Form von anonymisierten demographischen Daten (z.B.: Alter, Geschlecht, Beschäftigung, Selbsteinschätzung der Smartphone-Nutzung), anonymisierten Smartphone-Nutzungsdaten (z.B.: Ausgeführte Apps und Touchinteraktionen) und mehrerer anonymisierten Nutzerfeedbacks (z.B.: Online-Fragebögen und direktes Feedback über die App) gesammelt.

Anbei finden Sie die Datenschutzerklärung, die alle gesammelten Daten auflistet.

Während der Studie wird nur die Studienleitung Zugriff zu den Daten haben. Im Rahmen wissenschaftlicher Abhandlungen können diese anonymisiert veröffentlicht werden. Die Anonymisierung erfolgt durch die zufällige Zuteilung von TeilnehmerIDs.

Unter anderen zur Kontaktaufnahme wurde zu Beginn der Studie um die Angabe Ihrer E-Mail-Adresse gebeten. Diese wird vertraulich behandelt und nach Beendigung der Auswertung der Studie nicht weiterverwendet oder gespeichert.

Sie können ihre Teilnahme an der Studie jederzeit, ohne jegliche Nachteile, zurückziehen. Bitte kontaktieren Sie uns für weitere Informationen.

Max Mustermann

Email: Max.Mustermann@campus.lmu.de

Beispiel Einverständniserklärung

Ich, _____
(Name, Vorname)

Geburtsdatum _____

Gewünschte Vergütung: (Bitte entsprechendes ankreuzen)

☐ **Barauszahlung des Betrags**

☐ **MMI – Punkte** – Geben Sie ihre Matrikelnr. an: _____

erkläre, dass ich die Probandeninformation zur Studie:

„User Centered Attacks: Wie sicher ist dein Smartphone wirklich?“

und diese Einverständniserklärung zur Studienteilnahme erhalten habe.

✓ Ich wurde für mich ausreichend schriftlich über die wissenschaftliche Untersuchung informiert (Probandeninformation).

✓ Ich habe die Datenschutzerklärung erhalten, durchgelesen und verstanden.

✓ Ich erkläre mich bereit, dass im Rahmen der Studie Daten über mich gesammelt und anonymisiert aufgezeichnet werden. Es wird gewährleistet, dass meine personenbezogenen Daten nicht an Dritte weitergegeben werden. Bei der Veröffentlichung in einer wissenschaftlichen Abhandlung wird aus den Daten nicht hervorgehen, wer an dieser Untersuchung teilgenommen hat. Meine persönlichen Daten unterliegen dem Datenschutzgesetz.

✓ Im Rahmen der Studie werden Daten bezüglich meiner Smartphone-Nutzung, Feedbackdaten, sowie demographische Daten gesammelt. Diese werden ohne weitere personenbezogenen Daten gespeichert. Ich bin mit diesem Vorgehen einverstanden.

✓ Da die Daten anonymisiert gespeichert werden und meiner Person nicht mehr zugeordnet werden können, kann ich weder deren Löschung noch eine Einsichtnahme verlangen.

_____
(Unterschrift)

✓ Ich weiß, dass ich jederzeit meine Einverständniserklärung, ohne Angabe von Gründen, widerrufen kann, ohne dass dies für mich nachteilige Folgen hat.

✓ Bei weiteren Fragen kann ich jederzeit die Studienleiter kontaktieren.

✓ Mit der vorstehend geschilderten Vorgehensweise bin ich einverstanden und bestätige dies mit meiner Unterschrift.

_____ _____
(Ort, Datum) (Unterschrift)

Beispiel Datenschutzerklärung

Kontaktdaten des Anbieters

Max Mustermann Max.Mustermann@campus.lmu.de

Gruppe Usable Security and Privacy,
Forschungsinstitut Cyber Defence (CODE)
Bundeswehr Universität München
Cascada Bürogebäude
Carl-Wery-Str. 18-22
D-81739 München, Deutschland

Was sind personenbezogene Daten?

Nach der gesetzlichen Definition sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Unter personenbezogenen verstehen wir also Daten insbesondere Informationen zu Ihrer Identität wie beispielsweise Ihren Namen, E-Mail-Adresse, Telefon- bzw. Handynummer oder Postanschrift.

Erklärung des Zwecks der Datenerhebung

Die vorliegende App (SecureAuth) wird ausschließlich zur Datenerhebung und Datenverarbeitung einer wissenschaftlichen Studie an der Gruppe Usable Security and Privacy des Forschungsinstitut Cyber Defence (CODE) der Bundeswehr Universität München verwendet.

Diese Studie dient zur Einschätzung der persönliche Risikobewertung im Bezug auf unautorisierte Zugriffe auf das persönliche Smartphone. Hierfür wird bei den persönlichen Smartphones der Teilnehmer zu Beginn der Studie eine App installiert. Anschließen nutzen die Teilnehmer ihr Smartphone wie gewohnt und werden durch die App regelmäßig um Feedback zu den Situationen, in denen Sie ihr Smartphone entsperren, gebeten.

Hierfür wird bei jeder Entsperrung ein Foto mit der Selfie-Kamera gemacht, welches von dem Teilnehmer entsprechend der Gefahrensituation bewertet wird. Diese Fotos werden nur vom Teilnehmer gesehen und verlassen das Smartphone zu keinem Zeitpunkt.

Zusätzlich zu diesen Feedbacks werden im Rahmen der Nutzerstudie auch Touch-Daten, GPS-Daten und Nutzungsdaten anonymisiert gespeichert. Diese Daten werden anschließend ausgewertet, um sowohl den Kontext der Authentifizierung zu bestimmen als auch das entstandene Sicherheitsrisiko zu bewerten (z.b. Schmierspuren einer Passworteingabe können durch anschließende Touch-Interkationen verwischt werden.

Nach Beendigung der Studie werden alle Daten in einem persönlichen Treffen an die Studienleitung übermittelt. Außerdem beinhaltet die Teilnahme an der Studie das Ausfüllen zweier Online-Fragebögen, jeweils zu Beginn und zum Ende der Studie.

Beschreibung der Daten, die während der Studie erhoben werden

Grundsätzlich erhoben werden nur Daten, welche sowohl auf Basis aktueller rechtlicher Grundlagen als auch und unter Einwilligung der StudienteilnehmerInnen legitim sind. Erste Daten zur Demographie, Smartphone-Nutzung, Meinungen und Erfahrungen der Teilnehmer werden durch **2 Online-Umfragen** gesammelt. Folgende Daten werden **zusätzlich** durch die **SecureAuth-App** erhoben und zu Beendigung der Studie an die Studienleitung weitergeleitet:

- Zufällig generierte UserID der App
- Smartphone Modell und Android Version
- Erkennen von Touch Interaktionen (Koordinaten, Zeitpunkt und Art der Touch Interaktionen)
- Erkennen und Aufzeichnen von Aktivierungen des Bildschirms (Zeitpunkt)
- Nach einer Entsperrung ausgeführten Apps (Paketname der App, Zeitpunkt der Nutzung)
- Bewertung der Authentifizierungssituationen durch den Nutzer (Feedback zu Selfies)

- GPS-Daten (Aufenthaltsort) zum Zeitpunkt jeder Entsperrung des Bildschirms

Hierbei wollen wir speziell hervorheben, dass alle die Koordinaten und Zeitpunkte aller Touch-Punkte gespeichert werden, eben auch solche, die durch Eingabe von Passwörtern etc. entstehen.

Speicherdauer

Personenbezogene Daten werden für maximal 3 Monate gespeichert. Anschließend werden die Daten anonymisiert, also ohne Bezug auf Ihre Person, unbegrenzt gespeichert. Diese anonymisierten Daten sind dann nicht mehr löschbar.

Erhebungsdauer

Die maximale Erhebungsdauer im Rahmen des Forschungsvorhabens beträgt maximal 20 Tage. Die erhobenen Daten werden nach Ablauf der Studiendauer im Rahmen eines persönlichen Treffens direkt an die Studienleitung übertragen. Hierbei wird auch die „SecureAuth"- App gelöscht und von Ihrem Smartphone entfernt.

Information über Übermittlung an Dritte und deren Zweck

Alle Daten, die Sie uns übermittelt haben, werden selbstverständlich vertraulich behandelt. Wir stellen Ihre Daten grundsätzlich nicht anderen zur Nutzung zur Verfügung, es sei denn, wir sind zur Preisgabe dieser Daten verpflichtet, beispielsweise aufgrund gerichtlicher Verfügung.

Rechte des Benutzers

Der Nutzer hat die vom Europäischen Richtlinien- und Verordnungsgeber gewährten folgenden Rechte, im Bezug auf seine Personenbezogenen Daten (nicht die anonymisierten Daten):

- Recht auf Bestätigung: Recht, eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden.
- Recht auf Auskunft: Recht, jederzeit unentgeltliche Auskunft über die zu seiner Person gespeicherten personenbezogenen Daten und eine Kopie dieser Auskunft zu erhalten.
- Recht auf Berichtigung: Recht, die unverzügliche Berichtigung sie betreffender unrichtiger personenbezogener Daten oder die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.
- Recht auf Löschung (Recht auf Vergessen werden): Recht, zu verlangen, dass die sie betreffenden personenbezogenen Daten unverzüglich gelöscht werden, soweit die Verarbeitung nicht erforderlich ist.
- Recht auf Einschränkung der Verarbeitung: Recht, die Einschränkung der Verarbeitung zu verlangen, wenn eine der folgenden Voraussetzungen gegeben ist:
- Recht auf Datenübertragbarkeit: Recht, die personenbezogenen Daten, welche durch die betroffene Person einem Verantwortlichen bereitgestellt wurden, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
- Recht auf Widerspruch: Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, jederzeit gegen die Verarbeitung sie betreffender personenbezogener Daten, die aufgrund von Art. 6 Abs. 1 Buchstaben e oder f DS-GVO erfolgt, Widerspruch einzulegen.
- Recht auf Widerruf einer datenschutzrechtlichen Einwilligung: Recht, eine Einwilligung zur Verarbeitung personenbezogener Daten jederzeit zu widerrufen.

Um eines oder mehrere dieser Rechte in Anspruch zu nehmen, kontaktieren Sie bitte die unter 1. angegebene Kontaktperson.

Datum der Erstellung

Dieses Dokument wurde am 24.06.2019 von Max Mustermann erstellt.

Referenzen

[1] British Educational Research Association (bera): Revised Ethical Guidelines for Educational Research, 2004. Available from http://www.bera.ac.uk/files/guidelines/ethica1.pdf

[2] Mackay, Wendy E.: Ethics, Lies and Videotape... In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (Denver, Colorado, United States, May 07 - 11, 1995. ACM Press/Addison-Wesley Publishing Co., New York, NY, pp.138-145. DOI: 10.1145/223904.223922

[3] UofT Research Ethics Board (REB): Guide for Informed Consent. University of Toronto, Canada, April 2010.

[4] Caroline Gans-Combe (ed.): Data Protection and Privacy Ethical Guidelines (Version 5). European Commission, September 18, 2009

[5] The European Data Protection Supervisor (EDPS): Data Protection Glossary. The EDPS Website. See http://www.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/Glossary

[6] Eléonore Pauwels: Ethics for Researchers. Facilitating Research Excellence in FP7. See ftp://ftp.cordis.europa.eu/pub/fp7/docs/ethics-for-researchers.pdf

[7] National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research: The Belmont Report - Ethical Principles and Guidelines for the Protection of Human Subjects of Research. U.S. Department of Health, Education, and Welfare, 1979. See http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.htm

[8] World Medical Association: WMA Declaration of Helsinki - Ethical Principles for Medical Research Involving Human Subjects. 18th WMA General Assembly, Helsinki, Finland, 1964. See http://www.wma.net/en/30publications/10policies/b3/index.html

[9] Sarah J. L. Edwards: Research participation and the right to withdraw. Bioethics. 2005 April; 19(2):112-30. DOI: 10.1111/j.1467-8519.2005.00429.x

[10] Stefan Eriksson and Gert Helgesson: Potential harms, anonymization, and the right to withdraw consent to biobank research. European Journal of Human Genetics (2005) 13, 1071–1076. doi:10.1038/sj.ejhg.5201458; published online 29 June 2005. See http://www.nature.com/ejhg/journal/v13/n9/abs/5201458a.html

[11] Organization for Economic Co-Operation and Development: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. See http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html

[12] Christopher Kuner: Proportionality in European Data Protection Law And Its Importance for Data Processing by Companies. Privacy & Security Law Report, Vol. 07, No. 44, 11/10/2008, pp. 1615ff.

[13] Ruth W. Grant and Jeremy Sugarman: Ethics in Human Subjects Research: Do Incentives Matter? Journal of Medicine and Philosophy, 29(6): 717–738, 2004. See http://www.waisman.wisc.edu/EVENTS/ethics/sprin06-sem2-incentives-compensation.pdf

[14] Stanley Milgram: Obedience to Authority. New York: Harper & Row, 1974

[15] Philip G. Zimbardo: The power and pathology of imprisonment. Congressional Record. (Serial No. 15, 1971-10-25). Hearings before Subcommittee No. 3, of the Committee on the Judiciary, House of Representatives, Ninety-Second Congress. Washington, DC: U.S. Government Printing Office.