GERMAN **UPA**
Berufsverband der Deutschen Usability
und User Experience Professionals

Keine Angst vorm Datenschutz

DSGVO-Basics für User Researcher

Stand Oktober 2022

Inhalt

Einleitung

Die Einführung der Datenschutz-Grundverordnung (DSGVO) hat die Rechte von Verbrauchern erheblich gestärkt. Aber bei denen, die mit personenbezogenen Daten arbeiten, hat es auch teilweise große Verunsicherung erzeugt. Welche Daten gelten genau als personenbezogen? Welche Konsequenzen hat dies für die Einwilligung der Nutzer? Wie kann ich Daten noch speichern? Dabei hilft uns die DSGVO, weil sie Dinge festschreibt, die Vertrauen zwischen Nutzern und Researchern fördert und damit Themen einfordert, die guter User Research schon immer berücksichtigt hat. Daher die gute Nachricht vorneweg: User Research ist weiterhin wie gehabt möglich, ein paar Dinge musst du allerdings in der Planung, Durchführung und Nachbereitung berücksichtigen.

Mit diesem Dokument versuchen wir von den Arbeitskreisen “User Research” und “Usable Security & Privacy” anhand bekannter Beispiele zu zeigen, an welchen Punkten die DSGVO auf das Thema User Research Bezug nimmt. Dann zeigt dir unsere Checkliste Schritt für Schritt, worauf du in den einzelnen Phasen achten musst. Definitionen der wichtigsten Begriffe und Antworten auf die häufigsten Fragen helfen dir schließlich, gut informiert in die nächste User-Research-Studie zu starten.

Die Autoren übernehmen keine Haftung, dass die dargestellten Inhalte in dem Artikel aktuell, richtig, vollständig und rechtmäßig sind und nicht in unzulässiger Weise in Rechtsgüter Dritter eingreifen. Die Ratschläge basieren auf den persönlichen Erfahrungen der Autoren und stellen keine verbindliche Rechtsberatung dar. Aufgrund der Besonderheiten des Themas empfiehlt sich im Einzelfall die Beratung durch einen spezialisierten Rechtsanwalt.

Dabei betrifft Datenschutz aber nicht nur rechtliche Fragestellungen. Die Ergebnisse von User Research basieren auf dem vertrauensvollen Austausch zwischen Researchern und Proband:innen - daher ist es in beiderseitigem Interesse dieses Vertrauen aufrechtzuerhalten. Die Anwendung der DSGVO stellt dieses Vertrauen sicher.

Als Teil der German UPA setzen wir uns ein für Wissensvermittlung im Bereich Usability und User Experience und wollen dazu beitragen, dass User Research auch in Zukunft ein wichtiger Bestandteil der menschzentrierten Gestaltung bleibt. Weiterhin wollen wir diejenigen, die sich erst neu mit dem Thema beschäftigen, darin ermutigen, User Research auszuprobieren und in ihre Prozesse zu integrieren.

DSGVO im Research Projekt

Im Folgenden wird nun durch den groben Ablauf von User-Research-Studien geführt und es werden die jeweiligen Herausforderungen und zu beachtenden Details erläutert.

Vorbereitung

Schon vor der Durchführung der Studie gilt es, vorausschauend verschiedene Aspekte des Datenschutzes zu beachten, beispielsweise welche Softwaretools oder Dienstleister eingesetzt werden. Mit diesen Überlegungen schließt man spätere Gefahren aus, etwa dass mit den Daten Dinge geschehen, die die Proband:innen nicht wussten und/oder zu denen sie nicht zugestimmt haben. Dies wäre ein Verstoß gegen die DSGVO.

Erstellung einer passenden Einwilligungserklärung

Mit dieser Sammlung an studienspezifischen Informationen lässt sich nun direkt eine Vorlage zu einer Erklärung erstellen, welche den Proband:innen vorgelegt werden kann zur Information und Einwilligung. Hierbei ist es wichtig, dass die Inhalte gut und verständlich geschrieben sind und dass die Proband:innen erfahren, was der Zweck der Erhebung ist, wie die Daten verarbeitet werden und ob/wer/wieso von Dritter Stelle Zugriff auf die Daten hat.

Stolperfalle: Ein NDA/Geheimhaltung hat nichts mit einer Einwilligungserklärung bzgl. Datenschutz zu tun.
Zu Beginn von Research Sessions wird oft “Papierkram” gemacht. Darunter häufig auch Geheimhaltungserklärungen für den Umgang mit Prototypen (die hier im Dokument nicht weiter erläutert wird). Die Einwilligungserklärung muss davon losgelöst sein (und hat auch andere Klauseln die nicht eine Geheimhaltung gehörten). D.h. Proband:innen müssten dann mehrfach unterzeichnen.

Stolperfalle: Wahl der Länge von Speicherfristen
Für die Einwilligungserklärung muss man die Speicherfrist benennen, also die Zeit wie lange die aufgezeichneten Daten gespeichert werden. Diese kann frei gewählt werden, muss sich aber an den Zweck der Erhebung und der Studie anlehnen. Nicht gültig sind dabei Zwecke die “unendlich” lange Zeiten implizieren. Üblich sind Zeiträume von 3, 6, 9 oder manchmal auch 12 Monaten. Bei den längeren Zeiträumen sollte eine aussagekräftige Erklärung möglich sein, wieso die Daten so lange vorgehalten werden müssen. Bei der Angabe von “unnötig” langen Zeiträumen ist trotz etwaiger Einwilligung der Proband:innen ein Verstoß von Datenschutzregularien möglich.

Stolperfalle: Besonders schützenswerte Zielgruppen / Daten
Es gibt Daten die bzgl. der Art oder der Zielgruppe einen besonderen Schutz genießen. Dies betrifft sowohl den Umgang mit den Daten als auch der Einwilligung der Proband:innen. Beispiele dafür sind Befragungen von Minderjährigen oder Menschen mit Behinderung. Auch bei medizinischen personenbezogenen Daten sind besondere Schutzmaßnahmen empfohlen. Aber auch jenseits der Zielgruppe können Inhalte – z. B. Gespräche über kritische Infrastruktur – besonderem Schutz unterliegen.

DSGVO im Research Projekt

Stolperfalle: Externe Tools
Wenn Daten in der Weiterverarbeitung in andere Tools geladen werden und dort analysiert werden, kann dies datenschutzrechtlich relevant bzw. kritisch sein. Schnell sind dort Daten in “unsicheren” Drittstaaten abgelegt (z. B. bei Cloud Online Tools aus den USA) oder werden automatisiert weitergegeben (über API Tools wie Zapier) / verarbeitet (über z. B. manche automatischen Transkript-Tools).

Stolperfalle: Dienstleister
Bei der Erhebung oder Verarbeitung der Daten durch externe Dienstleister ist dies in der Regel auch mit den Probanden explizit zu vereinbaren, um eine Transparenz zu schaffen, was mit ihren Daten passiert. Selbstverständlich solltest auch du klären und sicherstellen, dass die Daten dort in guten Händen sind. Hierzu gibt es auch rechtlich mit den Dienstleistern explizite Zusatzvereinbarungen, sog. Auftragsverarbeitungsverträge (AVV). In diesen sollte festgehalten werden, welche Daten zu welchem Zweck in welchem Zeitraum vom Dienstleister verarbeitet werden und wie der Dienstleister den Schutz der Daten sicherstellt.

Stolperfalle: Interne Befragungen
Werden betriebsinterne Proband:innen im Rahmen einer Studie befragt ist es empfehlenswert - und teilweise auch nötig - dies im Vorhinein mit der Arbeitnehmervertretung (z.B. der Betriebsrat) abzustimmen, da hier besondere Schutzrechte gelten können.

Stolperfalle: Erhebung von Daten, mit denen Leistungskontrollen möglich sind
Es gibt viele Metriken, die im Rahmen von Studien erhoben werden können, welche im beruflichen Kontext Rückschlüsse auf die Leistung von Einzelpersonen oder -gruppen zulassen. Dies gilt vor allem bei Erhebungen zu firmenspezifischer Software und lässt sich oft nur schwer vermeiden. Z.B. bei der Erhebung von Taktzeiten, Durchlaufzeiten oder der einfachen Bearbeitungszeit einer Aufgabe ist dies eine mögliche Leistungskontrolle. Im Rahmen des Arbeitnehmerschutzes sind derartige Befragungen mit der Arbeitnehmervertretung zu klären.

Best Practice: Wann brauche ich keine Einwilligung der Proband:innen?
Einer der Grundsätze der DSGVO ist die Datensparsamkeit. Je weniger personenbezogene Daten ich in meiner Studie erhebe, desto weniger kritisch ist die Bewahrung des Datenschutzes. Wenn ich im Rahmen einer Studie keine personenbezogenen Daten erhebe - und auch keine Möglichkeit gebe, fälschlicherweise welche einzugeben - dann kann ich die Studie ohne Datenschutzerklärung durchführen. Beispiele sind dabei oft reine, allgemeine Multiple-Choice oder Skalenbefragungen in denen zusätzlich auch vom System im Hintergrund keine weiteren Daten mitgeschrieben werden (wie z.B. IP-Adressen der Teilnehmer).

DSGVO im Research Projekt

Best Practice: Bulletpoint-Zusammenfassung
Die komplette, rechtssichere Erklärung zum Datenschutz ist häufig lang und teilweise kompliziert geschrieben, um bei eventuellen Rechtsstreitigkeiten möglichst eindeutig zu sein. Um den Proband:innen einen einfachen Zugang zu den erhobenen Daten und ihrer Verwendung zu geben, kann eine kurze, stichwortartige Zusammenfassung der wichtigsten Information vor dem kompletten Text sehr hilfreich sein.

Durchführung

Nun geht es los. Die Studie ist aufgesetzt, geplant und organisiert. Hierbei ist es natürlich wichtig, sich an die Planungen weitestgehend zu halten, um die in Ruhe getroffenen Maßnahmen zur Einhaltung der DSGVO auch umzusetzen.

Informieren
Hierzu gehört ein offener Umgang mit den Probanden:innen und eine transparente Kommunikation aller wichtigen Informationen. Je nach Situation kann es auch hilfreich sein, nochmal den Ablauf, Methode und Zweck zu erläutern. Solltest du aus methodischer Sicht manche der Punkte nicht zu detailliert ausführen wollen, stelle sicher, dass du am Ende nochmal alle Lücken füllst. Plane für diesen Schritt auch Zeit ein für Erklärungen und Rückfragen.

Einholung der expliziten Zustimmung für die Datenerhebung durch Probanden
Im Rahmen der Einführung musst du spätestens die Einwilligungserklärung vorlegen - wenn du personenbezogene Daten erhebst - und den Proband:innen Zeit zum Lesen und Unterschreiben geben. Selbstverständlich kannst du niemanden zur Unterschrift zwingen. Daher solltest du in der Rekrutierung meist schon kommunizieren, was erhoben wird, um unnötige Überraschungen zu vermeiden. Die Zustimmung muss explizit erfolgen und dokumentiert werden. Z.B. als Unterschrift auf der Erklärung selbst, digitale Signatur oder Aufzeichnung. Diese solltest du auch im Nachgang gut verwahren und mindestens so lange abrufbar haben, wie du die Daten gespeichert hast.

Best Practice - Einwilligung
Während die Einwilligung bei persönlichen durchgeführtem Research noch recht einfach per direkter Unterschrift des entsprechenden Dokumentes erledigt werden kann, ist die Sache bei remote Research bereits ein wenig kniffliger, da sichergestellt werden muss, dass die Einwilligung wirklich von Proband:innen stammt. Dies kann sowohl über digital signierte Dokumente gelöst werden, wie auch direkt durch Bestätigung in einer Videoaufzeichnung oder entsprechende Eingaben in einem Onlineformular. In allen Fällen sollte die Erklärung beinhalten, in welcher Form die entsprechenden Datenschutzerklärungen zur Verfügung gestellt werden.

Stolperfalle: Die Möglichkeit zum Widerruf!
Eine Zustimmung ist oft zeitlich beschränkt – aber zusätzlich kann diese jederzeit widerrufen werden. Dieses Recht muss stets gegeben sein. Achte auf den Hinweis bei der Erstellung der Dokumente.

DSGVO im Research Projekt

Stolperfalle: Geschäftskontakte
Auch wenn Kontakte im Rahmen von z. B. Kundengesprächen befragt werden, können im Gespräch personenbezogene Daten genannt oder aufgezeichnet werden. Nur weil Probanden nicht als Privatperson am Gespräch teilnehmen, heißt dies nicht, dass der Datenschutz über die Firmenbeziehung geregelt ist.

Best Practice - Ansprache bei digitalen Einwilligungsanfragen
Immer häufiger werden Nutzungsdaten heutzutage direkt während der Nutzung einer Software eingeholt. Dies kann entweder in Form kontinuierliche Aufzeichnung von Telemetrie Daten oder an bestimmten Punkten im Arbeitsablauf erfolgen.

Wichtig sind vor allem in zweiten Fall eine kurze Zusammenfassung des Zwecks und der erhobenen Daten sowie ein Kontakt für Nachfragen. Die Ansprache sollte direkt, transparent und zweckgebunden erfolgen, um sich von den allgegenwärtigen Cookie Bannern abzuheben.

Selbst wenn nur anonymisierte Daten erhoben werden sollten die Nutzer über Zweck und Umfang informiert werden und die Möglichkeit haben, die Erhebung von Nutzungsdaten zu überspringen.

Datenerhebung

Der eigentlich “kritische” Teil ist die Erhebung selbst - denn hier werden die relevanten und sensiblen Daten in der Regel ja erst aufgezeichnet und damit in deine/eure Verantwortung übergeben.

Beachtung der in der Einwilligung erteilten Erlaubnisse
Wichtig ist es, bei der Durchführung selbst auch darauf zu achten, dass man selbst sich nur innerhalb der erlaubten Grenzen der Einwilligung bewegt. Verstöße treten hier häufig auf, wenn sich nach der Erstellung der Einwilligung nochmal wesentliche Bestandteile der Datenerhebung ändern - z.b. die Tools, Beteiligten oder der Zweck des Ganzen. Ein Verstoß - ob beabsichtigt oder nicht - ist hier besonders unnötig, da man sich ja die formale Arbeit zur passenden Einwilligung schon gemacht hat.

Stolperfalle: “Versteckte” personenbezogene Daten
Manchmal gibt es je nach Toolwahl oder Methodik auch eine unbeabsichtigte Aufzeichnung von Daten. Da diese sich meist nicht in den Einwilligungen befinden, sind diese ein oft Verstoß gegen die DSGVO. Am häufigsten sind hierbei z.b. volle IP-Adressen, die von Fragebogentools gespeichert werden. Aber auch bei Befragungen mit Freitextfeldern kann es sein, dass Proband:innen selbst nicht erwünschte Daten eintragen. Der Eintrag ist dabei keine Einwilligung und sollte deshalb verhindert werden - z.b. durch einen expliziten Hinweis.

DSGVO im Research Projekt

Stolperfalle: Unbeabsichtigte Aufnahmen
Gerade bei Aufnahmen können von Proband:innen unbeabsichtigt Dinge gezeigt werden, welche personenbezogene Daten von ihnen - oder sogar Dritten - beinhalten.
Bei Screensharings zeigen Funktionen wie “Autovervollständigen” bereits eingegebene Daten, können Notizen und Dateinamen auf dem Desktop relevant sein oder ungewollte Informationen in Push Notifications auftauchen.
Bei Aufnahmen können unbeteiligte Dritte ins Bild laufen oder hineinsprechen und so ohne vorliegende Einwilligung aufgezeichnet werden.
Grundsätzlich habt ihr vermutlich nach bestem Wissen und Gewissen gehandelt - am besten weist ihr aber präventiv zu Beginn noch mal explizit auf diese Gefahren hin. Sollte es dennoch vorkommen, informiert die Proband:innen auf diese Umstände, am besten notiert ihr euch noch den Zeitpunkt und entfernt diese Abschnitte aus dem Video-/Audiomaterial direkt nach Ende der Aufnahme.

Stolperfalle: Bestehende Daten
In manchen Kontexten kann es vorkommen, dass schon vor der Konzeption und Durchführung einer Studie Daten erhoben wurden, die zur Studie passen. Das könnten ältere Interviews sein, oder in anderen Kontexten (z.B. Sales oder Support) erhobene personenbezogene Daten sein. Ob und wie diese verwendet werden dürfen, hängt also von den damals mit den Feedbackgebern eingewilligten Verwendungszwecken und - dauern ab.

Nachbereitung

Im Rahmen von User Research Aktivitäten wird auf Basis der erhobenen Daten im Regelfall eine Analyse durchgeführt, um Situationen, Kontexte und Potenziale herauszuarbeiten. Das Ergebnis einer Studie ist daher meist eine Zusammenfassung und Interpretation der Beobachtungen. Hierbei finden in vielen Fällen einzelne Zitate und Anekdoten Einzug in die Berichterstattung, um als Evidenz und O-Ton Erkenntnisse zu stützen. Hierbei kann es sich je nach Detailgrad um personenbezogene Daten handeln.

Erstellung von nicht-personenbezogenem Reporting
Bei der Berichterstellung gilt es, für das Aufzeigen einer Referenz aus der Studie nur die wirklich relevanten Daten zu übernehmen. Meist reicht dies, um den Personenbezug zu umgehen, da viele Details nicht nötig sind, um die Kernaussage zu erhalten. In vielen Fällen kann ein Bezug zu einer verallgemeinerten Zielgruppe dennoch die Relevanzaussage erhalten.

Stolperfalle: Highlight Reels, Best-of Videos
Werden für Präsentationen o.Ä. Zusammenschnitte von z.B. Aufzeichnungen eines Usability Tests angefertigt, werden diese häufig im Unternehmen zugänglich gemacht und z.B. in eine Präsentation eingebettet. Im Rahmen der einzuhaltenden Löschungen der Videos kommt es in der Praxis häufig vor, dass diese später bei Eintreten der Löschfrist vergessen werden und daher eine Verletzung der Vereinbarung mit dem Probanden eintritt.

DSGVO im Research Projekt

Stolperfalle: Sehr kleine Sample Sizes im Reporting
Schneller als gedacht kann es Dritten trotz vieler Anonymisierungsmaßnahmen möglich sein, einzelne Personen in einem Report oder einer Datensammlung zu identifizieren. Dies ist vor allem dann der Fall, wenn ein enger Bezug zu den Probanden besteht, man den Kontext sehr detailliert kennt und Ergebnisse in sehr kleinen Stichproben ausgewertet und gespeichert werden. Besonders häufig tritt dies bei der Auswertung von Kundengesprächen auf, weil z.B. andere Mitarbeiter:innen über mehrere Details Rückschlüsse ziehen können - oder bei internen Befragungen, bei denen der Proband:innenpool bekannt ist und andere Mitarbeiter:innen schnell rückschließen können.

Stolperfalle: Public URLs
Wird im Rahmen der Auswertung mit Cloud-Tools gearbeitet, gibt es mittlerweile häufig die Option via Link mit einer anderen Person Inhalte zu teilen. Viele dieser “Sharing”-Optionen benötigen zum Öffnen keinen Login. In den falschen Händen haben also unbeteiligte Dritte Zugriff auf die Auswertung und damit auch auf personenbezogene Daten.

Projektabschluss

Sind die Analysen abgeschlossen gilt es “Aufzuräumen” und dafür zu sorgen, dass die Daten, die in deiner Obhut waren und im Rahmen der Einwilligung zu einem bestimmten Zweck übergeben wurden, nun so behandelt werden, dass keine Gefahren für die personenbezogenen Daten des/der Proband:in bestehen bleiben.

Anonymisieren von Daten
Wenn Daten nach Ende des Projekts (oder nach Ende des in der Einwilligung der Proband:in genannten Datums) gespeichert bleiben sollen, ist dies nur möglich, wenn die Daten korrekt anonymisiert werden. Das heißt, es darf keine Möglichkeit geben, diese nachträglich auf eine einzelne Person zurückzuführen. Somit können sie auch keine Rechte eines Einzelnen bzw. die DSGVO verletzen. Mit diesen Daten darf somit “alles” getan werden. Natürlich kann diese Anonymisierung auch schon früher im Prozess durchgeführt werden.

Dies ist besonders wichtig, wenn ein Unternehmen eine langfristige Datensammlung als Wissensspeicher anlegen möchte - oder wenn diese an Dritte weitergegeben werden, wo der weitere Umgang mit den Daten nicht sicher nachvollziehbar ist. Dies ist v.a. bei Reports nötig, die dann weitergeleitet werden.

DSGVO im Research Projekt

Stolperfalle: Wann sind Daten ausreichend anonymisiert?
Kurz gesagt: Wenn es Dritten nicht möglich ist mit bestehenden Daten von euch und anderen Datenquellen die Personen exakt zu identifizieren oder auf eine sehr kleine Gruppe einzuschränken.
Dazu etwas detaillierter:
Dritte sind Personen mit ausreichender fachlicher Kompetenz. Diese könnten Firmenintern oder extern sein. Im Prinzip alle außer denjenigen, die initial an der Studie beteiligt waren. Auch Kolleg:innen darf es nicht möglich sein aus dem Kontext eine Identifikation durchzuführen. Bestehende Daten sind in erster Linie natürlich Aufzeichnungen, können aber auch E-Mails, Teilnehmer:innenlisten oder externe Register sein. Die Erinnerung von beteilitgten Researcher:innen zählt hier nicht. Es handelt sich dabei nicht um eine Datenquelle die “Dritten” zur Verfügung steht.

Stolperfalle: Datenbanken und / oder Querverweise
Zur Zuordnung von Teilnehmern kann es teilweise vorkommen, dass bei (sonst anonymisierten) Rohdaten zusätzliche Informationen notiert werden, um eine Zuordnung zu ermöglichen. Auch wenn diese Zuordnung nur von Personen durchgeführt werden können, die zu beiden Daten Zugriff haben, ist dies eine Verletzung des Datenschutzes, wenn keine explizite Einwilligung vorliegt.
Das Gleiche gilt auch für (scheinbar anonyme) Datensätze, die unter Zuhilfenahme von Daten von Dritten eine Deanonymisierung erlauben.

Löschen verbleibender personenbezogener Daten
Manche Daten lassen sich nicht anonymisieren oder sind nur ein Zwischenprodukt und sollen nicht langfristig dokumentiert werden. Diese können nun gelöscht werden. Beachte dabei bitte auch Sicherungskopien zu löschen und informiere dich bei deinen IT-Verantwortlichen oder Toolbetreibern, ob die Daten auch unwiderruflich gelöscht sind - in vielen Systemen lassen sich Daten erstaunlich lange wieder wiederherstellen.

Stolperfalle: Projektverzug oder Folgeprojekte
Generell gilt, das ihr den angegebenen Zweck und Zeitraum immer beachten müsst. Daher kann es zum Beispiel Sinn machen, einen kleineren Projektverzug von vornherein zu berücksichtigen um nicht 2 Wochen vor Projektende plötzlich Daten löschen zu müssen, die vielleicht nochmal gebraucht werden würden.
Anonymisierte Daten und aus den Daten abgeleitete Erkenntnisse sind hiervon nicht betroffen. Jedoch dürfen personenbezogene Daten nach Projektende nicht weiter aufbewahrt und verwendet werden, auch nicht für eventuelle Folgeprojekte.

DSGVO im Research Projekt

Stolperfalle: Nebendokumentation
Im Rahmen von Research Projekten fallen mitunter auch weitere Notizen und Aufzeichnungen an, welche im Rahmen eines Löschantrags oder Erreichen einer Löschfrist vernichtet werden müssen. Gerade analoge Medien (z.B. Notizen), Fotodokumentationen, Mails oder ähnliche Zwischenprodukte, die personenbezogene Daten beinhalten, werden hier oft bei der Löschung vergessen.

Stolperfalle: Rekontaktierung
Daten werden im Regelfall zu einem bestimmten Zweck überlassen. Wenn man z.B. Kontaktdaten von Proband:innen zur Kommunikation bekommt, sind diese nach der Studie zu löschen und dürfen im Regelfall z.B. nicht für eine spätere Kontaktaufnahme im Rahmen einer Folgestudie verwendet werden (sofern nicht anders vereinbart).

Beispielszenarios

Zur anschaulichen Erklärung der DSGVO-relevanten Aspekte von User Research haben wir verschiedene typische Setups entworfen und beschrieben. Anhand dieser kannst du dich selbst hineinversetzen und erarbeiten, auf was du aus Datenschutzsicht achten musst, um für deine eigenen Anwendungsfälle passend vorbereitet zu sein.

Onlinebefragung

Daten:	Quantitativ
Durchführung:	Online
Methode:	Fragebogen
Rekrutierung:	Selbst

Beispielszenario
Für einen Marketingclaim wurden zwei Vorschläge entwickelt. Es werden zufällig zwei Gruppen gebildet unter den Teilnehmern – eine pro Claim – und das Ziel ist es, mindestens 100 Kunden pro Gruppe zu befragen. Als Entscheidungsgrundlage für die Auswahl sollen Daten erhoben werden. Den Teilnehmern soll jeweils einer der Claims gezeigt werden. Anschließend sollen die Wahrnehmung des Unternehmens als Marke abgefragt werden und auch, ob der Claim zum Unternehmen passt.

Teilnehmer
Da geprüft werden soll, ob der Claim zum Unternehmen passt, werden Kunden befragt.

Rekrutierung
Ein Teil der Kunden hat sich sowohl für den Newsletter angemeldet als auch zugestimmt, ab und an Befragungen zugeschickt zu bekommen. An diese Gruppe soll der Fragebogen gehen.

Verwendete Tools
Es soll ein Online-Befragungstool wie z. B. SurveyMonkey verwendet werden.

Durchführung
Die Kunden bekommen den Link zugesendet und wer sich dazu entscheidet, füllt den Fragebogen alleine zu Hause aus.

Erhobene Testdaten
Es werden Alter und Geschlecht abgefragt und auch, wie lange die Person schon Kunde des Unternehmens ist. Ansonsten werden keine persönlichen oder sensiblen Daten im Fragebogen abgefragt.

Beispielszenarios

Usability Test (remote inkl. Aufnahme)

Daten:	Quantitativ
Durchführung:	Online
Methode:	Moderierter Usability Test
Rekrutierung:	Externe Agentur

Beispielszenario
Ein Produkt befindet sich gerade in der Entwicklung und die erste Konzipierung ist abgeschlossen. Bevor es an die Umsetzung geht, soll die Usability mit Hilfe eines Prototyps getestet werden. Mit einer Gruppe von 6 Personen sollen die 2 häufigsten Use Cases für das neue Produkt getestet werden.

Teilnehmer
Da die App sich v. a. an Studenten richtet, soll mit dieser Zielgruppe getestet werden.

Rekrutierung
Eine Rekrutierungsagentur wird beauftragt, um Personen aus der Zielgruppe zu rekrutieren. Die Agentur handhabt die Daten der Proband:innen sowie deren Einverständniserklärungen.

Verwendete Tools
Ein Online-Konferenz-Tool, wie z. B. Zoom, wird verwendet.

Durchführung
Die Agentur vereinbart Termine mit den Proband:innen für zwei Erhebungstage und schickt ihnen ebenfalls eine Einverständniserklärung zu. Im Vorfeld schickt die Agentur dem Teilnehmer einen Link, zu dem er sich zum Termin einwählen soll. Sollte der Proband nicht erscheinen, kann der Researcher die Agentur anrufen, damit diese die Testperson anruft. Dies ist notwendig, da der Researcher die Telefonnummer aus Datenschutzgründen selbst nicht erhalten hat. Außer dem Researcher wählen sich noch weitere Kollegen aus dem Entwicklungsteam ein, um die Tests still zu beobachten. Des Weiteren wird eine Aufnahme von der Sitzung gemacht, die für die Analyse und zum Herstellen von Videoclips verwendet werden soll.

Erhobene Testdaten
Die Proband:innen teilen ihren Bildschirm, während sie mit dem Prototyp interagieren. Zudem werden Gesicht und Stimme aufgezeichnet, die ebenfalls auf der Aufnahme zu sehen bzw. zu hören sein werden.

Beispielszenarios

Interview in Person (Vor-Ort-Befragung ohne Aufnahme)

Daten:	Qualitativ
Durchführung:	Vor-Ort
Methode:	Interview
Rekrutierung:	Andere Abteilung

Beispielszenario
Ein B2B-Unternehmen hat schon des Öfteren von den Kunden den Bedarf für eine App zu ihrem Online-Tool kommuniziert bekommen. Als Start des Projekts sollen Interviews mit ungefähr 10 Kunden geführt werden, um genau herauszufinden, für welche Use Cases und in welchen Situationen die Kunden die App vor allem benutzen wollen. Kunden des Unternehmens sollen eingeladen werden zu einem kurzen Interview, das vom Researcher bei den Kunden vor Ort geführt werden soll, auch um sich einen Eindruck von den Arbeitsbedingungen der Kunden zu machen.

Teilnehmer
Kunden des Unternehmens.

Rekrutierung
Die Sales-Kollegen prüfen die Bereitschaft der Kunden, an den Interviews teilzunehmen, und organisieren die Termine vor Ort.

Verwendete Tools
Persönliches Gespräch und ein Notizblock. Außerdem sollen Fotos vom Arbeitsplatz gemacht werden.

Durchführung
Zum vereinbarten Termin führt der Researcher das Interview mit den Kunden an einem ruhigen Ort durch (und besichtigt deren Arbeitsplätze).

Erhobene Testdaten
Es gibt keine Aufzeichnungen außer den Notizen des Researchers. Diese enthalten jedoch meist den Namen und die Adresse der Teilnehmer:in sowie einige sensible Daten, um die es im Interview ging, wie etwa vertrauliche firmeninterne Informationen. Zusätzlich gibt es Fotos vom Arbeitsplatz (aber ohne den Teilnehmer).

Anwendungsbeispiele

Onlinebefragung

Vorbereitung

Überprüfen, ob Einwilligungserklärung notwendig ist	• Eine Einwilligungserklärung ist notwendig, da personenbezogene Daten erhoben werden (Alter, Geschlecht, Dauer der Kundenbeziehung). Der Nutzung der E-Mail Adresse wurde bereits in anderem Kontext zugestimmt. (Achtung: Dieser Zweck der Nutzung muss mit abgedeckt sein.) • Zudem muss geprüft werden, welche personenbezogenen Daten vom Befragungstool genutzt werden.
Erstellen einer passenden Einwilligungserklärung	Folgende Bestandteile sollte die Einwilligungserklärung enthalten: • Erhebung von Daten zur Verbesserung des Marketings • Speichern der Daten nur für die Dauer der Auswertung und anschließender Löschung • Kontaktdaten des Verantwortlichen/Ansprechpartners • Information über Widerruf • Angaben zu Datenschutzbestimmungen des verwendeten Umfragetools

Durchführung

Einholen der expliziten Zustimmung für die Datenerhebung durch Probanden	• Anzeige der Einwilligungserklärung vor dem eigentlichen Fragebogen • Explizite Bestätigung (z.B. Checkbox) • Absenden des Formulars nur mit Einwilligung
Beachten der in der Einwilligung erteilten Erlaubnisse	• Prüfen, dass nur Fragen enthalten sind, die dem angekündigten Zweck der Erhebung dienen • Prüfen, dass das verwendete Umfragetool keine zusätzlichen Daten erhebt • Keine Verwendung zusätzlicher Freitextfelder (z.B. “Gibt es sonst noch etwas, was Sie uns mitteilen wollen?”)

Anwendungsbeispiele

Onlinebefragung

Nachbereitung

Erstellen von nicht-personenbezogenem Reporting	• Kein Reporting nach Alter/Geschlecht/Dauer der Kundenbeziehung, wenn die Gruppen dadurch sehr klein werden.
Personenbezogene Daten schützen	• Prüfen, wer Zugriff auf die Umfrageergebnisse hat (z.B Firmenaccount) • Eventuelle Downloads der Rohdaten nur auf sichere Datenträger • Zugriff auf Mailinglisten zum Versand der Einladungen prüfen

Projektabschluss

Anonymisieren von zu speichernden Daten	• Da die Reports bereit anonymisiert sind, müssen nun keine weiteren Schritte unternommen werden.
Löschen verbleibender personenbezogener Daten	• Löschen der Umfrageergebnisse im Umfragetool • Löschen aller lokalen Kopien/Downloads der Daten aus der Umfrage • Sicherstellen, dass im Umfragetool und lokal keine Sicherungskopien vorhanden sind

Anwendungsbeispiele

Usability Test (remote inkl. Aufnahme)

Vorbereitung

Überprüfen, ob Einwilligungserklärung notwendig ist	• Eine Einwilligungserklärung ist notwendig für die Kontaktdaten, die von der Recruitingagentur verwendet werden, sowie für die Videoaufzeichnung und Verarbeitung. Dies können auch zwei verschiedene Dokumente sein.
Erstellen einer passenden Einwilligungserklärung	Folgende Bestandteile sollte die Einwilligungserklärung enthalten: • Erhebung der Daten für die Durchführung der Tests und der eigentlichen Testdaten für die Auswertung • Speichern der Daten nur für die Dauer der Auswertung und anschließender Löschung • Kontaktdaten des Verantwortlichen/Ansprechpartners beim Auftraggeber. • Information über Widerruf

Durchführung

Einholen der expliziten Zustimmung für die Datenerhebung durch Probanden	• Am besten die Einwilligungserklärung im Vorfeld zur Studie unterschrieben zurücksenden lassen. Andernfalls als Erstes nach Beginn der Video-Session die Einwilligung des Probanden, wie auf der Erklärung beschrieben, abfragen und auf Video dokumentieren. (Der Start der Aufnahme benötigt ebenfalls eine Einverständnis.)
Beachten der in der Einwilligung erteilten Erlaubnisse	• Kontaktdaten verbleiben bei der Agentur • Video Aufzeichnungen sind nur vom Researcher einsehbar • Prüfen, ob das Tool zur Videokonferenz/Aufzeichnung Daten speichert

Anwendungsbeispiele

Usability Test (remote inkl. Aufnahme)

Nachbereitung

Erstellen von nicht-personenbezogenem Reporting	• Keine Referenzen zu den einzelnen Usability-Tests im Reporting • Prüfen der Bildschirmaufnahme auf sensible Daten (Namen, Kontakte, offene Webseiten, Logins…) und ggf. verpixeln / rausschneiden.
Personenbezogene Daten schützen	• Zugriff auf Kontaktdaten bei der Agentur prüfen • Ausschnitte aus Videos nicht als Datei teilen • Zugriff auf Video Aufzeichnungen überprüfen (z.B. Firmenaccount)

Projektabschluss

Anonymisieren von zu speichernden Daten	• Da die Reports bereit anonymisiert sind, müssen nun keine weiteren Schritte unternommen werden.
Löschen verbleibender personenbezogener Daten	• Löschen der Kontaktdaten bei der Recruitingagentur (wenn nicht Probanden aus deren Pool/Panel) • Löschen der Videoaufzeichnungen vom verwendeten Tool und lokalen Kopien

Anwendungsbeispiele

Interview in Person (Vor-Ort-Befragung ohne Aufnahme

Vorbereitung

Überprüfen, ob Einwilligungserklärung notwendig ist	• Da personenbezogene Daten vom Researcher notiert werden ist eine Einwilligungserklärung notwendig.
Erstellen einer passenden Einwilligungserklärung	Folgende Bestandteile sollte die Einwilligungserklärung enthalten: • Erhebung der Daten zur Gestaltung einer App • Speichern der Daten nur für die Dauer der Auswertung und anschließender Löschung • Kontaktdaten des Verantwortlichen/Ansprechpartners • Information über Widerruf

Durchführung

Einholen der expliziten Zustimmung für die Datenerhebung durch Probanden	• Unterschreiben der Einwilligungserklärung vor dem Start des Interviews
Beachten der in der Einwilligung erteilten Erlaubnisse	• Auf den Fotos dürfen keine anderen Personen ohne Einverständnis zu sehen sein.

Nachbereitung

Erstellen von nicht-personenbezogenem Reporting	• Fotos von Arbeitsplätzen nur zeigen, wenn nicht auf den Befragten rückgeschlossen werden kann (Namensschilder, Firmenlogos, Unterlagen, …)
Personenbezogene Daten schützen	• Notizen sicher verwahren, egal ob physisch oder digitalisiert

Anwendungsbeispiele

Interview in Person (Vor-Ort-Befragung ohne Aufnahme

Projektabschluss

Anonymisieren von zu speichernden Daten	• Aussagen aus den Interviews ohne persönliche Daten speichern • Auf Fotos alle Bereiche ausblenden/verpixeln die Rückschlüsse auf den Befragten zu lassen (oder Fotos löschen)
Löschen verbleibender personenbezogener Daten	• Notizen (physisch und digital) vernichten/löschen • Bilder von Kamera, Computer und eventuellen Backups entfernen (z. B. bei Verwendung von Smartphone als Kamera)

Zum Schluss

Dein nächstes Projekt kann kommen! Wir hoffen, dieses Dokument hilft dir, sicher mit dem Thema DSGVO umzugehen und dich ohne Angst vor dem Datenschutz in User Research zu stürzen. Es gibt schließlich nichts Besseres als das Gefühl, neue, spannende und überraschende Einsichten gewonnen zu haben. Nur wenn die Nutzer uns vertrauen, sagen sie uns, was sie wirklich bewegt. Und nur wenn wir das Wissen sammeln, können wir es nutzen, um bessere Produkte und Services zu gestalten. Dafür setzen wir uns in den Arbeitskreisen der German UPA ein. Wenn du neugierig geworden bist, schau doch auch gerne mal bei uns vorbei.

Die Arbeitskreise
Der Arbeitskreis Usable Security & Privacy beschäftigt sich mit Ansätzen und Konzepten, die sicherheits- und privatheitsfördernde Verfahren für Software und interaktive Produkte stärker an den Zielen und Aufgaben der Nutzer ausrichten und die dafür sorgen, dass Funktionsweisen von Sicherheitselementen auch für Nichtexperten verständlich sind.

Ziel des Arbeitskreises User Research ist es, die Sichtbarkeit des Themenfeldes User Research innerhalb des Fachbereichs User Experience zu erhöhen. User Experience ist mehr als Interaktions- und visuelles Design; ein gutes Design beruht auf einer auf Nutzerdaten fundierten Anforderungsanalyse und einem guten Konzept, sowie der Evaluation des entwickelten Designs mit repräsentativen Nutzern.

Die German UPA
Als Berufsverband der Deutschen Usability und User Experience Professionals bilden wir ein hochwertiges Netzwerk für und von Usability Experten. Unsere ehrenamtlichen Mitglieder fühlen sich der Wissensvermittlung und Meinungsbildung rund um das Thema Usability und UX verpflichtet.

Im Anhang findest du noch

Checkliste kompakt
Zum Ausdrucken und mitnehmen, dein schneller Überblick für dein nächstes Research Projekt

FAQ
Antwort auf häufige Fragen zum Thema DSGVO im User Research

Glossar
Die wichtigsten Begriffe zum Thema DSGVO kurz erklärt

Checkliste kompakt

Vorbereitung

- Überprüfen, ob Einwilligungserklärung notwendig ist
- Werden personenbezogene Daten für die Rekrutierung erhoben? (z.B. Kontaktdaten)
- Werden personenbezogene Daten während der Studie erhoben? (z.B. Aufnahmen)
- Sammelt das System personenbezogene Daten im Hintergrund? (z.B. IP-Adressen)
- Erstellung einer passenden Einwilligungserklärung
- Klar definierter Zweck, welche Daten, Speicherdauer und Beteiligte
- Rechtliche Angaben vorhanden: Widerrufserklärung, Verantwortliche
- Geklärt, ob kritische Zielgruppen (Kinder, Betriebsinterne)
- Geklärt, das alle Dritten (Dienstleister, Tools) den Datenschutz einhalten

Durchführung

- Einholung der expliziten Zustimmung für die Datenerhebung durch Probanden
- Rechtssichere Dokumentation der Zustimmung vor Aufnahme von Daten
- Beachtung der in der Einwilligung erteilten Erlaubnisse
- Sichergestellt, dass nur die in der Erklärung angegebenen Daten von euch erhoben werden
- Sichergestellt, dass verwendete Tools auch nur die angegeben Daten erheben

Nachbereitung

- Erstellung von nicht-personenbezogenem Reporting
- Geprüft, dass aus dem Reporting nicht auf Einzelpersonen oder kleine Gruppen Rückschlüsse geschlossen werden können
- Personenbezogene Daten schützen
- Keine personenbezogenen Daten (Z.B. Highlight-Reels) im Rahmen von Präsentationen oder Videos Dritten übermitteln (als Datei) um eine Verbreitung und Kopie zu verhindern.
- Sichergestellt, dass auf Daten nur von Beteiligten zugegriffen werden kann
- Speicherfrist während der Bearbeitung im Blick haben

Projektabschluss

- Anonymisieren von zu speichernden Daten
- Löschen/Ersetzen/Verallgemeinern von Identifikationsmerkmalen (Namen, Demographiemerkmale, Zugehörigkeiten, Referenzen)
- Verdecken/starkes Verpixeln von Gesichtern, On-Screen Informationen
- Löschen verbleibender personenbezogener Daten
- Reports/Zusammenfassungen/Highlight-Reels mit personenbezogenen Informationen löschen
- geklärt, dass Daten auch in Backups gelöscht werden
- geklärt, dass Daten, die weitergegeben wurden (Intern, Dienstleister) auch gelöscht wurden
- organisatorische Dokumentation zur Begleitung löschen (Proband:innen-Kommunikation, Listen, etc.)
- Arbeitsverzeichnisse durchgehen um Zwischendokumentationen mit personenbezogenen Daten zu löschen

FAQ

Wie muss eine Studie gestaltet sein, um ohne Datenschutzregularien auszukommen?
In der Regel ist das dann der Fall, wenn es keine Freitextfelder gibt, keine Demografien abgefragt werden und die Eingabe somit hauptsächlich über Skalen oder andere vorgefertigte Antwortoptionen erfolgt. Wichtig ist aber auch, dass auch automatisch keine identifizierenden Daten (wie z.B. eine IP-Adresse) dokumentiert werden.

Wer kann sich beschweren / klagen?
Hauptsächlich der betroffene und etwaig geschädigte Teilnehmer, dessen Datenschutzrechte verletzt wurde, ist berechtigt zu klagen. Aber auch der Gesetzgeber kann Bußgelder verhängen, insb. wenn Systeme so gestaltet sind, das Verstöße laufend stattfinden.

Was darf ich mit anonymisierten Daten tun?
Korrekt anonymisierte Daten sind per Definition ohne die Möglichkeit, sie auf eine einzelne Person zurückzuführen und somit können sie auch keine Rechte eines Einzelnen verletzen. Mit diesen Daten darf somit “alles” getan werden.

Was muss ich bei einem Widerruf machen?
Wenn ein Teilnehmer eine Einverständniserklärung widerruft, sind die erhobenen, personenbezogenen Daten sehr zeitnah zu löschen und die Löschung ist zu bestätigen. Bereits anonymisierte Daten dürfen weiterhin erhalten und verwendet werden.

Wie lange muss/darf ich personalisierte Daten aufbewahren?
Es gibt keine Vorgaben, wie lange personalisierte Daten aufbewahrt werden müssen.
In der Einwilligungserklärung muss der Zeitraum für das Aufbewahren der Daten genannt werden, länger dürfen die Daten nicht aufbewahrt werden. Dies kann entweder ein bestimmter Zweck (z.B. ein Projekt) sein oder ein konkret benannter Zeitpunkt.

Wer ist verantwortlich/haftbar bei Verstößen?
Verantwortlich ist prinzipiell, wer die personenbezogenen Daten erhebt. Dies ist in der Regel ein Unternehmen, wer jedoch als Freelancer selbst Daten erhebt ist auch selbst dafür verantwortlich. Erfolgt die Datenverarbeitung durch einen Dienstleister ist grundsätzlich trotzdem der Auftraggeber haftbar.

Müssen die Daten digital und analog besonders geschützt werden? Wo/Wie lagern?
Bei der Speicherung der Daten gilt, dass auf dem Stand der Technik geeignete Maßnahmen getroffen werden müssen, um die Daten gegen unberechtigten Zugriff zu schützen.
Dies gilt sowohl bei der Speicherung wie auch in jedem Verarbeitungsschritt.

Was ist, wenn nur der Vorname der Proband:innen beibehalten werden?
Da Vornamen zusammen mit anderen demografischen Daten eine Identifizierung der Person ermöglichen kann, sollte hier immer mindestens eine Pseudonymisierung der Daten erfolgen.

Glossar

Personenbezogene Daten
Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, z.B. Name, Anschrift oder Geburtsdatum. Weiterhin betrifft dies Daten, die in Verbindung mit Zusatzwissen identifizierbar sind, wie Telefon-, Matrikel- und Sozialversicherungsnummern oder Online-Kennungen wie IP-Adressen und Cookie-Kennungen. Ausreichend ist dabei, wenn die Information die Identifizierung der betroffenen Person theoretisch ermöglicht, es kommt also nicht darauf an, ob die Person tatsächlich identifiziert wird. Die Informationen müssen sich auf einen lebenden Menschen beziehen. Einzelangaben über juristische Personen, wie Kapitalgesellschaften oder eingetragene Vereine, sind keine personenbezogenen Daten (außer z.B. bei Einzelunternehmen). Besondere Kategorien personenbezogener Daten werden nach Artikel 9 DS-GVO besonders geschützt. Das sind zum Beispiel Gesundheitsdaten, Daten über die ethnische Herkunft sowie religiöse oder weltanschauliche Überzeugungen.

Anonymisieren der Daten
Daten zu anonymisieren, bedeutet, das alle Daten gelöscht werden, die eine Zuordnung zu einer natürlichen Person ermöglichen.

Pseudonymisieren
Daten zu pseudonymisieren hingegen bedeutet, die Identifikationsmerkmale (wie Namen) mit anderen, erfundenen Daten auszutauschen, sodass auch hier keine Zuordnung zu der natürlichen Person mehr möglich ist.

Consent
Consent ist der englische Begriff für das Einverständnis und die “consent form” entspricht zu deutsch der Einverständniserklärung.

Widerruf
Die Teilnehmenden haben das Recht, ihr Einverständnis zur Teilnahme an der Studie, auch im Nachhinein, zu widerrufen.

Wiederherstellung
Wird ein Widerspruch eingereicht und die Daten eines Probanden gelöscht, kurz bevor eine Wiederherstellung des Gesamtsystems stattfindet, muss nach der Wiederherstellung sichergestellt werden, dass die wiederhergestellten Daten auch nochmals gelöscht werden.

Sicherungskopien
Werden Sicherungskopien langfristig aufbewahrt, können auch bereits in Live-Systemen gelöschte Daten noch vorhanden sein und somit der Löschfrist nicht folge geleistet sein. In der Praxis werden in vielen Systemen Sicherungskopien nach z.b. 30 Tagen überschrieben, sodass langfristig keine Kopien erhalten bleiben.

Glossar

Technische Maßnahmen
Die nach dem derzeitigen Stand der Technik angemessenen Maßnahmen um persönliche Daten vor dem Zugriff Dritter zu schützen. Die Angemessenheit richtet sich nach Art der Daten und Zweck der Verwendung.

"Verarbeitung"
Jegliche Art von manuellem oder automatisiertem Vorgang zur Erhebung, Speicherung, Organisation, Anpassung, Analyse oder Bereitstellung personenbezogener Daten. Die Sicherheit der Daten muss bei jeder Verarbeitung gegeben sein, dies schließt auch das Löschen der Daten mit ein.

Dienstleister
Natürliche oder juristische Personen, die Teile der Verarbeitung und/oder Nutzung der Daten übernehmen im Rahmen eines weisungsgebundenen Auftrags. Wenn es sich dabei um personenbezogene Daten handelt ist immer ein Vertrag zur Auftragsverarbeitung erforderlich.

Auftragsverarbeitung
Die Verarbeitung personenbezogener Daten durch eine natürliche oder juristische Person im Rahmen eines definierten Auftrages mit einem definierten Zweck. Dauer und Art der Verarbeitung müssen dabei vorab festgelegt werden.

Betroffene Person
Natürliche Person, deren persönliche Daten verarbeitet werden.

Geschädigte Person
Natürliche Person, der durch Verstoß gegen Bestimmungen der DSGVO ein Schaden entstanden ist.

Löschfrist
Grundsätzlich müssen personenbezogene Daten gelöscht werden, wenn der Zweck der Einwilligung oder die angegeben Aufbewahrungszeit erreicht ist. In Einzelfällen kann dem eine gesetzliche Aufbewahrungsfrist entgegen stehen, dann müssen die Daten auch nicht auf Anfrage der betroffenen Person gelöscht werden.

Einwilligung
Die freiwillige, informierte und unmissverständliche Zustimmung der betroffenen Person zur Verarbeitung personenbezogener Daten für einen definierten Zweck.

Profiling
Automatisierte Verarbeitung personenbezogener Daten, welche die Beurteilung persönlicher Aspekte der betroffenen Person erlaubt und es beispielsweise ermöglicht, Vorlieben, Interessen oder Aufenthaltsorte zu analysieren oder vorherzusagen.