MAX-PLANCK-INSTITUT
FÜR BILDUNGSFORSCHUNG

CASTELLUM
Datenschutzkonforme Probandendatenbank

Beschreibung der Versuchspersonendatenbank „Castellum“

MAX PLANCK INSTITUTE FOR HUMAN DEVELOPMENT,
Lentzeallee 94, 14195 Berlin, datenschutz@mpib-berlin.mpg.de

1 Präambel

Die Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (MPG) nimmt den Schutz personenbezogener Daten sehr ernst. Der gesetzeskonforme Umgang mit personenbezogenen Daten ist eine Basis für eine vertrauensvolle Beziehung zu Studienteilnehmenden, Beschäftigten, zu Kooperations- und Geschäftspartnerinnen und -partnern sowie allen an der Forschung der Max-Planck-Gesellschaft interessierten Personen.

Grundlage dieses Konzepts bildet die Datenschutz-Grundverordnung (DS-GVO) sowie das Bundesdatenschutzgesetz (BDSG) in seiner zum Zeitpunkt der Erstellung des Konzeptes gültigen Form.

2 Begriffsbestimmungen

personenbezogene Daten

Personenbezogene Daten sind nach Art. 4 Nr. 1 DS-GVO alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. Zu den besonderen Kategorien personenbezogener Daten zählen nach Art. 9 Abs. 1 DS-GVO Daten, aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Verarbeitung

Verarbeitung umfasst nach Art. 4 Nr. 2 DS-GVO jeden analogen oder digitalen Vorgang im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung personenbezogener Daten.

3 Grundsätze für die Verarbeitung von Daten in der Forschung

Die Max-Planck-Gesellschaft schützt die Rechte von Personen, die im Rahmen von Forschungsprojekten an Studien aktiv teilnehmen, die Teil von Beobachtungsstudien sind oder mit deren Daten oder Bioproben an den Max-Planck-Instituten geforscht wird. Dies gilt insbesondere, wenn es sich um schutzbedürftige Personen wie Minderjährige oder in ihrer Geschäftsfähigkeit eingeschränkte Personen handelt. Forschung mit personenbezogenen Daten findet auf Basis der Einwilligung statt, wenn die Daten direkt bei den Teilnehmenden erhoben werden.

Die Erfüllung der Betroffenenrechte, die Sicherstellung geeigneter technischer und organisatorischer Schutzmaßnahmen werden beim Studiendesign berücksichtigt und in der Projektbeschreibung dargestellt.

4 Verwendete Software

Das Max-Planck-Institut für Bildungsforschung betreibt eine Versuchspersonendatenbank mit dem Namen „Castellum“. Die Datenbank dient dazu interessierten Personen eine Teilnahme an wissenschaftlichen Studien zu ermöglichen und zur zentralen Verwaltung aller Proband*innen Kontaktdaten. Zu diesem Zweck müssen Kontaktdaten und für die Studiendurchführung relevante personenbezogene Daten verwaltet und gespeichert werden. Um eine Verarbeitung der Daten in Einklang mit geltenden Standards der DS-GVO und des BDSG zu gewährleisten, wurde Castellum entwickelt.

Bei Castellum handelt es sich um eine Webanwendung, die in einem zentralen Projekt der Max-Planck-Gesellschaft massgeblich von einem Entwicklungsteam am Max-Planck-Institut für Bildungsforschung entwickelt wurde. Die Anwendung wird lokal am Max-Planck-Institut für Bildungsforschung gehostet und steht nur im Intranet zur Verfügung, d.h, ein direkter Zugang über das Internet ist nicht möglich. Der Zugriff auf die Weboberfläche erfolg verschlüsselt (SSL). Zur Nutzung der Webanwendung müssen Nutzer*innen einen begründeten formlosen Antrag stellen. Die Freischaltung des Accounts erfolgt erst nach einer allgemeinen DS-GVO-Schulung und einer spezifischen Einführung in Castellum. Die Accounts haben jeweils eine einjährige Laufzeit und können nur nach der Teilnahme an Auffrischungsschulungen um ein weiteres Jahr verlängert werden. Die Berechtigungen innerhalb der Datenbank werden

regelmäßig überprüft und nicht mehr benötigte Accounts werden gelöscht.

Der Zugriff auf den Server ist nur einem kleinen Administratoren-Kreis des Max-Planck-Instituts für Bildungsforschung vorbehalten.

5 Umfang der Datenverarbeitung

Die in der Datenbank enthaltenen Daten werden vertraulich nach Vorgabe der europäischen Datenschutzgrundverordnung (DS-GVO) erhoben, verarbeitet und genutzt. Näheres dazu findet sich im Kapitel Rechtsgrundlage der Datenverarbeitung.
Es werden drei Arten von Daten gespeichert:
Die personenidentifizierenden Daten (1) ermöglichen es, Kontakt mit Teilnehmer*innen aufzunehmen.
Wissenschaftlich relevante Merkmale (2) ermöglichen es, dass Studieneinladungen gezielt nur an geeignete Teilnehmer*innen ergehen.
Die Logistikdaten (3) fallen im Verlauf der Vorbereitung und Durchführung einer Studie an.

So werden in Castellum unter anderem folgende Informationen zu Personen gespeichert:

Zu (1) Personenidentifizierende Daten

- Vorname, Nachname
- Geburtsdatum
- Geschlecht
- akademischer Titel
- Straße
- Hausnummer
- Postleitzahl
- Ort
- E-Mail
- Telefon
- Telefon alternativ

Zu (2) Wissenschaftlich relevante Merkmale

- Händigkeit
- Muttersprache
- Alter

- Teilnahme an Studien
- Höchster Schulabschluss
- Tauglichkeit für bestimmte Experimente und Studien (z.B. MRT, ggf. auf der Grundlage von Gesundheitsinformationen)

Zu (3) Logistikdaten

- Aufnahme in die Datenbank
- Rechtsgrundlage für die Datenverarbeitung
- Zuletzt kontaktiert
- Erreichbarkeit (zeitlich befristete Abwesenheit)
- Datenquelle
- Einsichtsbestätigung zu Eignungsdokumenten je Studientyp
- Bevorzugte Kontaktierungsmöglichkeit (Telefon, Mail)
- Bisherige, vorherige oder aktuelle Studienteilnahmen mit Namen der Studie
- Pro Studie:
  - Kontakt- bzw. Teilnahmestatus (z.B. „auf Antwort wartend“, „nicht erreicht“, „nimmt teil“, „ausgeschlossen“)
  - Zugewiesene Rekrutierer*innen
  - Termine zu Sitzungen inkl. zugewiesenen Durchführer*innen

6 Rechtsgrundlage der Datenverarbeitung Castellum

Am Max-Planck-Institut für Bildungsforschung existieren vier rechtliche Grundlagen für die Speicherung von Kontaktdaten („Personenidentifizierende Daten“) in Castellum. Diese stellen sicher, dass sämtliche Kontaktdaten von (potentiellen) Proband*innen an einem Ort gepflegt werden können und sich der Zugriff auf diese Daten einheitlich und regelkonform am Institut steuern lässt.

Hierbei ist wichtig zu erwähnen, dass es keine allgemeine Einwilligung zur Aufnahme in die Versuchspersonendatenbank gibt. Die Speicherung der Proband*innen-Daten ist also immer an Zwecke gebunden, die mit den vier Rechtsgrundlagen beschrieben werden.

1 Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DSGVO
„Einwilligung zur Rekrutierung“
Die Einwilligung zur Rekrutierung erlaubt aus Castellum heraus Personen für zukünftige Studien einzuladen, die laut Auswahlkriterien zu den Personen passen. Daher werden für diese Rechtsgrundlage zusätzlich auch Rekrutierungsmerkmale zu den Proband*innen gespeichert. Diese werden in einer getrennten Datenbank abgelegt.
Castellum speichert direkt zu den Proband*innen-Datensätzen, ob diese Einwilligung vorliegt. Somit ist sichergestellt, dass die Einladung zu Studien über Castellum nur erfolgen kann, wenn diese vorliegt.

2 Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DSGVO und Art. 27 BDSG
„Studieneinwilligung“
Das Management der Einwilligungen zu Studien wird als dezentral angesehen. Studienleiter*innen am Max-Planck-Institut für Bildungsforschung sind selbst dafür verantwortlich diese einzuholen und korrekt und wiederauffindbar außerhalb von Castellum zu archivieren. Das jeweilige Vorgehen wird in der entsprechenden Studieneinwilligung beschrieben. In den Studieneinwilligungen wird auch erklärt, dass die Kontaktdaten in Castellum gespeichert werden und der Zugriff nur über Studienpseudonyme und entsprechende Nutzer*innen-Rechte möglich ist.
Castellum managt diese Studieneinwilligungen also nicht selbst, so dass bei einer gesetzten Studienteilnahme davon auszugehen ist, dass die individuelle Einwilligung erteilt wurde und die Rechtsgrundlage gegeben ist.
Man kann Studienteilnahmen von Proband*innen unabhängig von (1) in Castellum manuell anlegen. Organisatorisch sind die Studienleiter*innen am MPIB dazu angehalten, diesen manuellen Workflow möglichst selten zu nutzen und stattdessen über den Filtermechanismus auf Personen mit (1) gegangen wird.

3 Art. 6 Abs. 1 lit. a, Art. 9 Abs. 2 lit. a DSGVO und Art. 1626, 1902 BGB
*„Gesetzliche Vertreter*in“*
In Castellum werden die Kontaktdaten von gesetzlichen Vertreter*innen gespeichert. Da diese für Personen unter gesetzlicher Vertretung Unterschriften tätigen ist es ausreichend, wenn auf die entsprechend verknüpften Personen (1) oder (2) zutrifft.

4 Art. 6 Abs. 1 lit. f DSGVO
*„Proband*in ist gesperrt“*
Personen, die sehr unangenehm in Studien aufgefallen sind sollen unter Einhaltung eines Vier-Augen-Prinzips gesperrt werden bzw. nie wieder eingeladen werden. Statt diese Personen-Daten einfach zu löschen behalten wir die Kontaktdaten, um zu verhindern, dass die Person erneut in die DB gelangen kann.

7 Datenlöschung und Speicherdauer

Die personenbezogenen Daten der betroffenen Person werden gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt. Eine Speicherung kann darüber hinaus erfolgen, wenn dies durch den europäischen oder nationalen Gesetzgeber in unionsrechtlichen Verordnungen, Gesetzen oder sonstigen Vorschriften, denen die Max-Planck-Gesellschaft unterliegt, vorgesehen wurde. Eine Sperrung oder Löschung der Daten erfolgt auch dann, wenn eine durch die genannten Normen vorgeschriebene Speicherfrist abläuft, es sei denn, dass eine Erforderlichkeit zur weiteren Speicherung der Daten für einen Vertragsabschluss oder eine Vertragserfüllung besteht.

Zugriff auf Kontaktdaten über Pseudonyme

Castellum vergibt für Teilnehmende einer Studie jeweils individuelle studienspezifische Pseudonyme, um sicherzustellen, dass die eigentlichen wissenschaftlichen Daten über die Verwendung der Pseudonyme getrennt von den Kontaktdaten in einem anderen System gespeichert werden können. Darüber hinaus erlaubt es Castellum, dass in Studien auch mehrere Pseudonymräume („Domänen“) erstellt werden können, so dass je teilnehmender Person auch mehrere Pseudonyme in einer Studie verwendet werden können. Die spezifische und erweiterbare Vergabe von Pseudonymen soll verhindern, dass über Studien (oder z.B. auch Personengruppen) hinweg wissenschaftliche Daten ohne entsprechende Grundlage zusammengeführt werden können.

Während der Durchführung einer Studie ist technisch sichergestellt, dass ausschließlich Nutzer*innen mit der entsprechenden studienspezifischen Zugriffsrolle über eine Pseudonym-Suche auf die Kontaktdaten in Castellum zugreifen können. Sobald die Studie in Castellum als beendet markiert wird, erlischt diese Möglichkeit. Somit ist es dann nur noch der/dem Datenschutzkoordinator*in des Max-Planck-Instituts für Bildungsforschung möglich auf Studienteilnahmen und daraus

resultierende Kontaktdaten zuzugreifen. Darüber hinaus kann auch der

Pseudonymraum einer Studie vor Beendigung einer Studie gelöscht werden, dann ist es auch dem Datenschutzkoordinator*in unmöglich von pseudonymisierten wissenschaftlichen Daten auf die Kontaktdaten in Castellum zu schließen (die Forschungsdaten sind dann anonymisiert). Lediglich die Teilnahme an einer Studie ist dann noch in Castellum verzeichnet. Dieser Vorgang ermöglicht bzw. ersetzt das übliche Vorgehen, dass zu einem bestimmten Zeitpunkt nach einer Datenerhebung die Kodierliste zerstört wird.

8 Datenschutzmaßnahmen

Technische und organisatorische Maßnahmen (Art. 24, Art. 32 DS-GVO)

Die Max-Planck-Gesellschaft setzt ausgehend vom Schutzbedarf der personenbezogenen Daten und unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten und um sicherzustellen, dass die Verarbeitung gemäß den gesetzlichen Vorgaben erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert. Personenbezogene Daten werden insbesondere vor versehentlicher oder unrechtmäßiger Vernichtung, Verlust, Veränderung oder vor unbefugter Offenlegung beziehungsweise vorn beziehungsweise unbefugtem Zugang zu personenbezogenen Daten geschützt.

Privacy by Design / Privacy by Default

IT-Systeme und Applikationen werden im Rahmen von Risikobetrachtungen grundsätzlich so ausgestaltet, dass sie die Vorgaben Datenschutz durch Technikgestaltung (privacy by design) und Datenschutz durch datenschutzfreundliche Voreinstellungen (privacy by default) des Art. 25 DS-GVO erfüllen.

Verpflichtung zur Vertraulichkeit

Alle Beschäftigten sowie externe Personen, die im Rahmen ihrer Tätigkeit Umgang mit personenbezogen Daten der Max-Planck-Gesellschaft haben, werden auf die Wahrung der Vertraulichkeit sowie die Einhaltung der externen und internen Regelungen verpflichtet.

Schulungen

Die Max-Planck-Gesellschaft verfügt über ein Schulungskonzept, das verpflichtende Basis-Schulungen für alle Beschäftigten sowie fachspezifische Schulungen enthält. Darüber hinaus werden potentielle Nutzer*innen erst nach einem erfolgreichen Abschluss in einem internen Online-DS-GVO-Kurs und einer individuellen Castellum-

Schulung der entsprechenden LDAP-Gruppe hinzugefügt.

Technische Umsetzung

Das Max-Planck-Institut für Bildungsforschung setzt für Castellum mehrere Sicherheitsmaßnahmen und organisatorische Prozesse bei der Zugriffskontrolle ein. So ist Castellum eine interne Anwendung, die nur aus dem internen Institutsnetz erreichbar ist. Die Daten in Castellum werden physisch auf Servern des Max-Planck-Institut für Bildungsforschung gespeichert. Der Zutritt zu dem Serverraum ist nur dem IT Personal des Max-Planck-Institut für Bildungsforschung möglich. Der Serverraum ist mit einer Alarmanlage gesichert, Zutritt zu den Räumlichkeiten ist nur mittels Transponder und Codeeingabe möglich. Die Schliessanlage protokolliert die Zugriffszeiten. Aufgrund der Zeitstempel der Datendateien als auch auf Grundlage der Logfiles der Server ist sichergestellt, das Zugriffszeiten und User eindeutig identifiziert werden können.

Rollen- und Rechtemanagement

Nutzer*innen in der entsprechenden LDAP-Gruppe werden in Castellum verschiedenen Rollen zugewiesen. Es gibt fünf globale Rollen: Data protection coordinator, Principal subject manager, Receptionist, Study approver, Study coordinator.

Zwei dieser Rollen (Data protection coordinator, Principal subject manager) erlauben einen umfassenden Zugriff auf Proband*innen-Daten. Diese Rollen werden nur einem sehr kleinen Personenkreis zugewiesen.

Recruiter erhalten innerhalb einer Studienrekrutierung Zugriff auf die Kontaktdaten von Personen, die den gesetzten Filterkriterien der Studie entsprechen. Conductor erhalten Zugriff auf die Kontaktdaten und die Pseudonyme von Personen, die in der Studie als teilnehmend markiert sind. Während Nutzer*innen mit der Rolle Principal subject manager bei der Proband*innen-Suche sämtliche passenden Datensätze in der Ergebnisliste angezeigt werden, bekommen die studienspezifischen Subject Manager nur Suchergebnisse geliefert.

Zusätzlich zum Nutzer*innen-Management über Rollen steuert Castellum den Zugriff auf die Datensätze über Vertraulichkeitsstufen. Nutzer*innen, Proband*innen und den Merkmalen zur Person werden verschiedene Vertraulichkeitsstufen zugeteilt. Das stellt sicher, dass Nutzer*innen unabhängig von der zugewiesenen Rollen nur Datensätze einsehen können, die ihrer Vertraulichkeitsstufe entsprechen. Hierarchisch steht die Vertraulichkeitsstufe einer Proband*in über den jeweiligen Vertraulichkeitsstufen der Merkmale zur Person.

In Castellum werden diese Daten über zwei Datenbanken verteilt (Kontaktdaten getrennt von allen anderen Daten). Die eigentlichen Forschungsdaten werden nicht in Castellum gespeichert. Die Verknüpfung wird über Pseudonyme geregelt, die nur über entsprechende Rechte in Castellum miteinander verbunden werden können.

Zwei-Faktor-Authentisierung

Um die persönlichen Daten von Personen vor kompromittierten oder schwachen

Passwörtern zu schützen, wird Castellum mit einer Zwei-Faktor-Authentifizierung (2FA) verwendet. Benutzer müssen einen zusätzlichen Code eingeben, bevor Sie sich bei Castellum anmelden können. Derzeit werden jede generische TOTP-Anwendung oder FIDO2-Hardware-Sicherheitstoken unterstützt.

9 Grundsätze für jede Verarbeitung personenbezogener Daten (Art. 5 DS-GVO)

Rechtmäßigkeit

Personenbezogene Daten werden auf rechtmäßige Weise nach Treu und Glauben verarbeitet. Die Datenverarbeitung erfolgt nur, wenn gesetzliche Vorschriften der DS-GVO, des BDSG oder vorrangige Rechtsvorschriften dies anordnen, ausdrücklich zulassen oder eine Einwilligung der betroffenen Personen vorliegt.

Zweckbindung

Personenbezogene Daten werden nur für legitime Zwecke verarbeitet, die vor der Datenhebung definiert wurden. Nachträgliche Änderungen der Verarbeitungszwecke bedürfen einer erneuten Prüfung einer vorhandenen Rechtsgrundlage.

Transparenz

Die betroffenen Personen werden gemäß den gesetzlichen Vorgaben über die jeweilige Datenverarbeitung informiert. Die Information erfolgt in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache.

Datenminimierung

Jede Verarbeitung personenbezogener Daten ist so gestaltet, dass sie sowohl quantitativ als auch qualitativ auf das für die Erreichung der Zwecke erforderliche Maß beschränkt ist. Sofern der Zweck es zulässt und der Aufwand in einem angemessenen Verhältnis zum angestrebten Ziel steht, werden anonymisierte Daten verwendet.

Richtigkeit

Personenbezogene Daten werden sachlich richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand verarbeitet. Mittels angemessener Maßnahmen wird sichergestellt, dass unrichtige, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

Speicherbegrenzung

Personenbezogene Daten werden grundsätzlich nur so lange verarbeitet, wie dies für die Erfüllung der jeweiligen Zwecke erforderlich ist und keine anderweitigen

gesetzlichen, vertraglichen oder satzungsgemäßen Aufbewahrungspflichten bestehen.

Sicherheit der Datenverarbeitung

Personenbezogene Daten werden durch angemessene technische und organisatorische Maßnahmen vor unberechtigtem Zugriff oder Offenlegung, unrechtmäßiger Verarbeitung sowie versehentlichem Verlust, Veränderung oder Zerstörung geschützt. Diese Maßnahmen berücksichtigen den Stand der Technik, die Risiken der Verarbeitung und den Schutzbedarf. Die Anforderungen an die Maßnahmen sind Teil des Informationssicherheitsmanagements der Max-Planck-Gesellschaft.

10 Rechte der betroffenen Personen

Als betroffene Person, deren personenbezogene Daten im Rahmen der Versuchspersonendatenbank erhoben werden, bestehen grundsätzlich folgende Rechte, soweit in Einzelfällen keine gesetzlichen Ausnahmen zur Anwendung kommen:

- Auskunft (Art. 15 DS-GVO)
- Berichtigung (Art. 16 DS-GVO)
- Löschung (Art. 17 Abs. 1 DS-GVO)
- Einschränkung der Verarbeitung (Art. 18 DS-GVO)
- Datenübertragbarkeit (Art. 20 DS-GVO)
- Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO)
- Widerruf der Einwilligung (Art. 7 Abs. 3 DS-GVO)
- Beschwerderecht bei der Aufsichtsbehörde (Art. 77 DS-GVO).
  Dies ist für die MPG das Bayerische Landesamt für Datenschutzaufsicht, Postfach 1349, 91504 Ansbach

11 Kontaktdaten der Verantwortlichen

Verantwortlich im Sinne der Datenschutz-Grundverordnung und anderer nationaler Datenschutzgesetze sowie sonstiger datenschutzrechtlicher Bestimmungen ist die Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V. (MPG)

Hofgartenstraße 8
D-80539 München
Telefon: +49 (89) 2108-0

Kontaktformular: https://www.mpg.de/kontakt/anfragen
Internet: https://www.mpg.de

12 Kontaktdaten der Datenschutzbeauftragten der MPG

Kontaktperson der MPG:

Datenschutzbeauftragte
Heidi Schuster
Hofgartenstraße 8
D-80539 München
Telefon: +49 (89) 2108-1554
E-Mail: datenschutz@mpg.de

Kontaktperson am Institut:

Datenschutzkoordinator
Thomas Feg
Lentzeallee 94
14195 Berlin
E-Mail: datenschutz@mpib-berlin.mpg.de

Thomas Feg

Datenschutzkoordinator am MPIB