MAX PLANCK GESELLSCHAFT

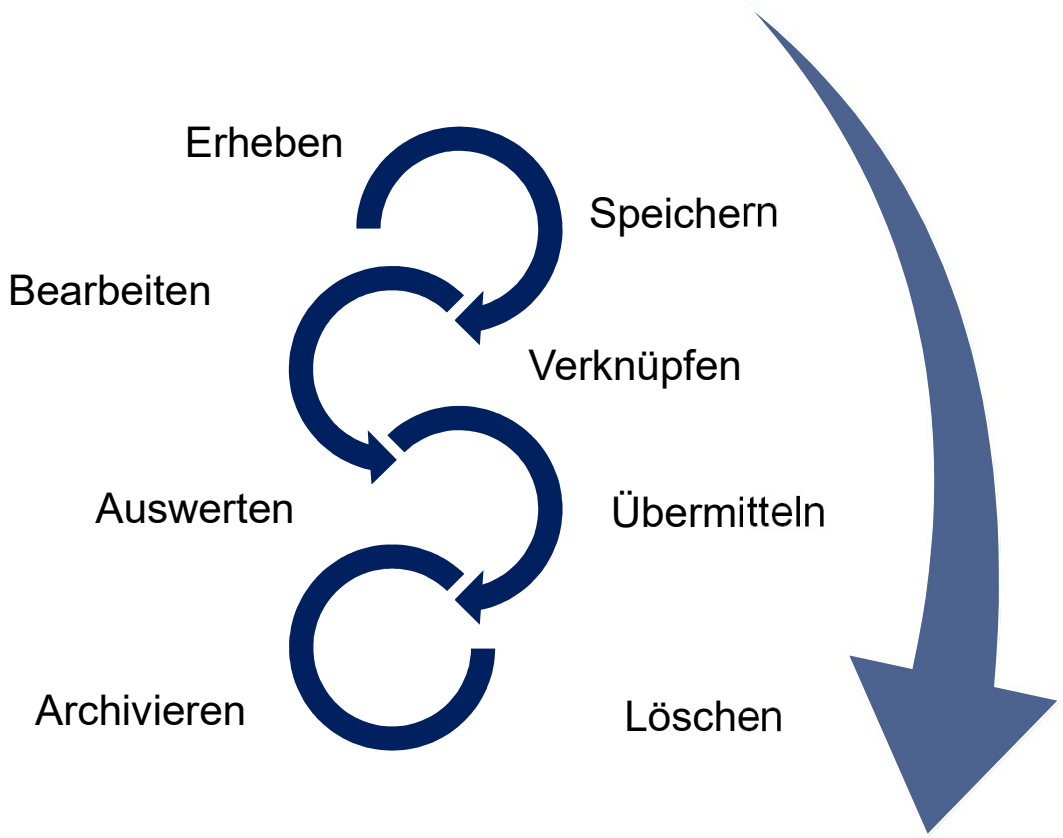
STUDIENTEILNEHMENDEN-MANAGEMENT IN DER PRAKTISCHEN UMSETZUNG

6. FDM-WORKSHOP 2024

Heidi Schuster, Datenschutzbeauftragte der MPG

Thomas Feg, Datenschutzkoordinator MPI für Bildungsforschung

DATA LIFE CYCLE MANAGEMENT IM DATENSCHUTZ



Ziel (Art. 5 Abs. DS-GVO):

Nachweis der Umsetzung der Datenschutzgrundsätze und des Schutzes der Personen während **des gesamten Data Life Cycles**

Notwendig:

Geeignete technische und organisatorische Maßnahmen

WAS MUSS DAS FDM IN DER HUMANFORSCHUNG ABBILDEN?

Unterschiedliche personenbezogene Datentypen

- Kontaktdaten, Selektionskriterien, Forschungsdaten
- Sensible Daten?

Angewandte Rechtsgrundlagen

- Einwilligung: bei aktiver Studienteilnahme
- Interessenabwägung: bei Beobachtungsstudien

Beschreibung der Verarbeitungsschritte

Insb. Pseudonymisierung durch Code-ID / Anonymisierung?

WAS MUSS DAS FDM IN DER HUMANFORSCHUNG ABBILDEN?

Data-Sharing

- Kooperationspartner
- Drittlandtransfer
- Rechtliche Basis für Transfer an sich / für Drittlandübermittlung

Within an existing project collaboration
inside the EU / EEA
outside the EU / EEA

Without an existing project collaboration
Data service center / repository
Internet platform
Restricted /controlled recipients?
Unlimited recipients?

What kind of personal data?

Speicherdauer

- Getrennt nach Kontaktdaten, Selektionskriterien, Forschungsdaten
- Erforderlichkeit basierend auf Studiendesign (Primär-/Sekundärforschung
- 10 Jahre Rohdaten (Sicherung guter wissenschaftlicher Praxis)

Archivierungen

- MPG Archiv
- Transfer in Repositorien / externe Archive

PRIVACY BY DESIGN AND DEFAULT (ART. 25)

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Data protection by design and by default

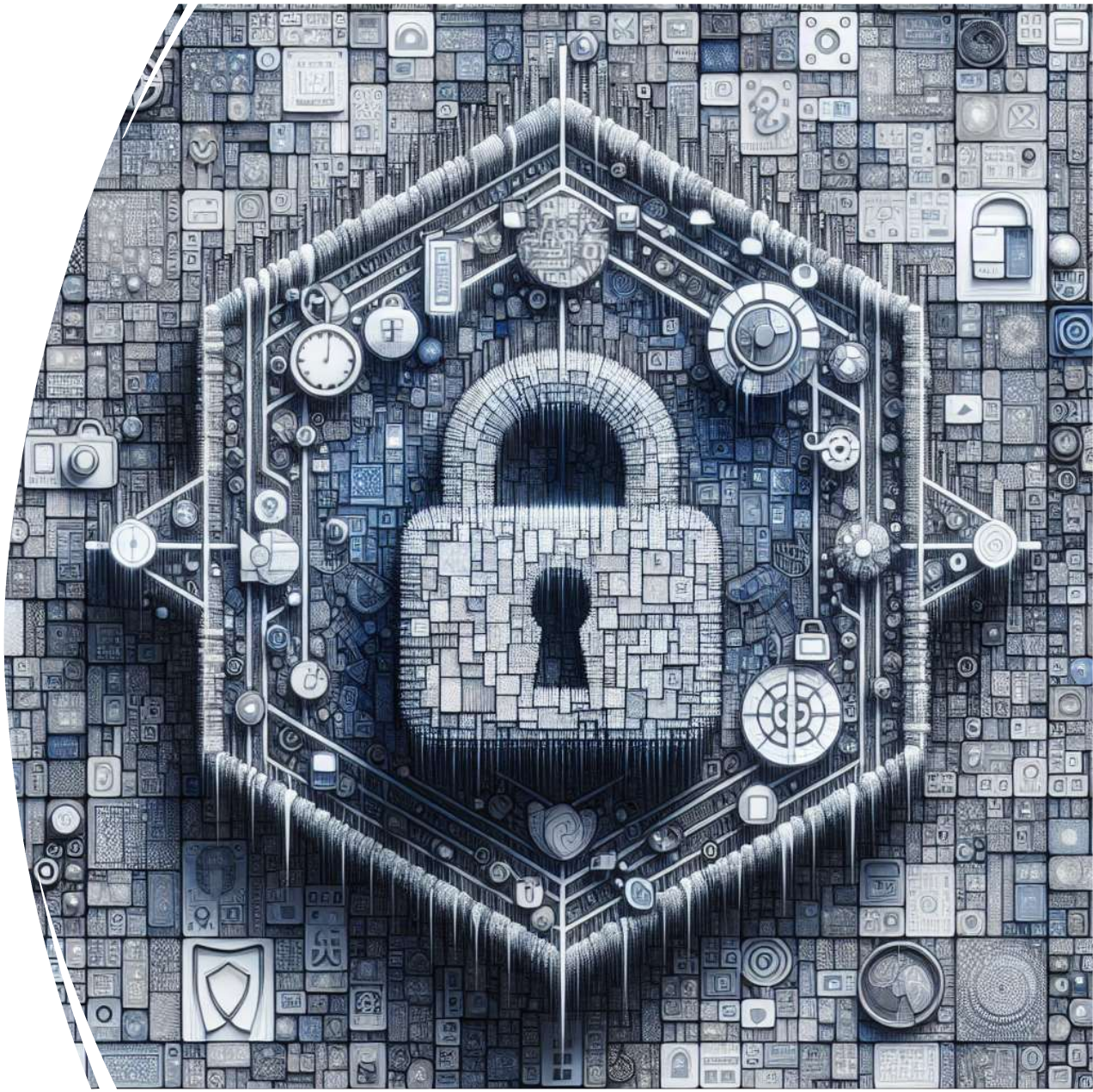
Maßstab:
Stand der Technik
Implementierungskosten
Art, Umfang, Umstände und Zwecke der Verarbeitung
Eintrittswahrscheinlichkeit / Schwere der Risiken
für die Personen

Der Verantwortliche trifft sowohl

- zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch
- zum Zeitpunkt der eigentlichen Verarbeitung

geeignete **technische und organisatorische Maßnahmen** – wie z. B. Pseudonymisierung, die dafür ausgelegt sind, die Datenschutzgrundsätze […] wirksam umzusetzen und die […] Rechte der betroffenen Personen zu schützen.

CLASS *DATA_PROTECTION*
{
};



Gibt es ein Softwareframework für Datenschutz?

- Privacy by Design Frameworks
- Open Web Application Security Project (OWASP)
- Microsoft's Privacy Tools for .NET

Was ist das Privacy by Design Framework?

- "Privacy by Design" ist ein Konzept, das in der frühen Phase der Erstellung von Technologien, Systemen und Geschäftspraktiken integriert wird, um den Datenschutz und die Datensicherheit zu gewährleisten.
- Es wurde ursprünglich in den **1990er** Jahren von Dr. Ann Cavoukian, der damaligen Datenschutzbeauftragten von Ontario, Kanada, entwickelt.

DATENSCHUTZ DURCH TECHNIKGESTALTUNG

1. Planungsphase:
Identifizieren Sie bereits in der Planungsphase die datenschutzrelevanten Aspekte Ihrer Anwendung. Entscheiden Sie, welche Daten Sie benötigen, wie Sie sie sicher speichern und verarbeiten können, und wie Sie den Benutzern Kontrolle über ihre Daten geben können. Erstellen Sie ein Konzept für den Datenschutz, das als Leitfaden für die gesamte Projektentwicklung dient.

2. Designphase:
Integrieren Sie Datenschutz und -sicherheit in das Design Ihrer Anwendung. Dies könnte beispielsweise bedeuten, dass Sie Funktionen für die Benutzerkontrolle der Daten direkt in die Benutzeroberfläche einbauen, oder dass Sie die Datenübertragung und -speicherung so gestalten, dass sie den Datenschutzprinzipien entspricht.

3. Entwicklungsphase:
Nutzen Sie während der Entwicklung datenschutzfreundliche Technologien und Praktiken. Dies könnte beispielsweise die Verwendung von Verschlüsselung, die Begrenzung der Datenerfassung auf das Notwendige oder die Implementierung von Datenschutz durch Voreinstellung beinhalten.

DATENSCHUTZ DURCH TECHNIKGESTALTUNG

4. Testphase:
Führen Sie während der Testphase spezielle Datenschutz- und Datensicherheitstests durch. Überprüfen Sie, ob Ihre Anwendung die in der Planungsphase festgelegten Datenschutzanforderungen erfüllt und ob alle Datenschutzfunktionen wie vorgesehen funktionieren.

5. Einführungsphase und darüber hinaus:
Nach der Einführung Ihrer Anwendung sollten Sie weiterhin Datenschutz und Datensicherheit im Auge behalten. Führen Sie regelmäßige Überprüfungen und Aktualisierungen durch, um sicherzustellen, dass Ihre Anwendung auch weiterhin den Datenschutzprinzipien entspricht.

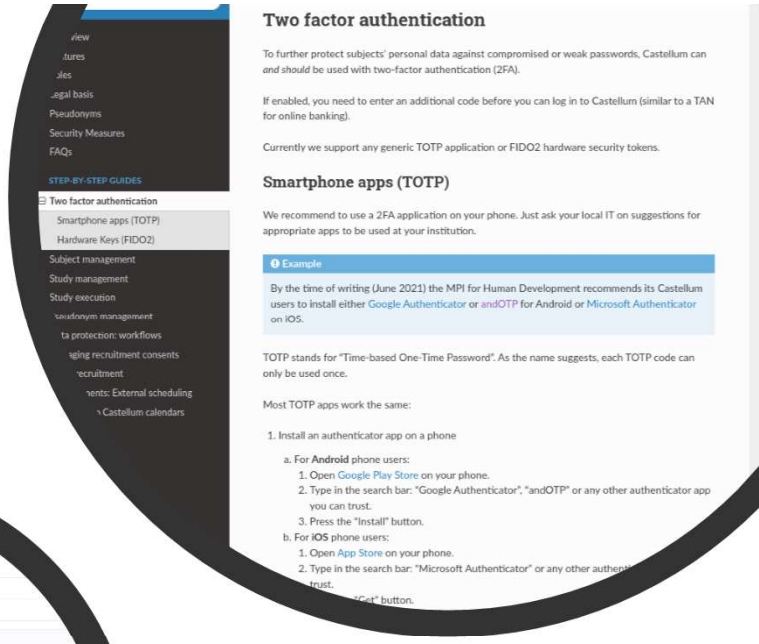
Darüber hinaus ist es wichtig, dass Sie Ihr Entwicklerteam in Datenschutz und Datensicherheit schulen. Sie sollten sicherstellen, dass alle Teammitglieder die Bedeutung des Datenschutzes verstehen und wissen, wie sie Datenschutzprinzipien in ihrer Arbeit umsetzen können.

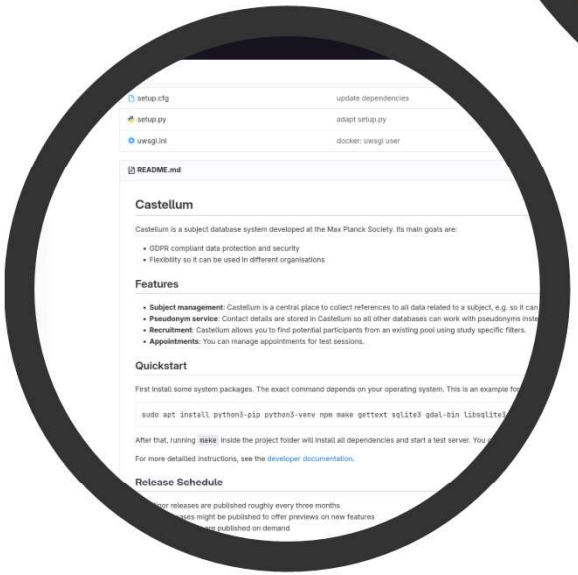
TOOLS & TECHNOLOGIEN CASTELLUM

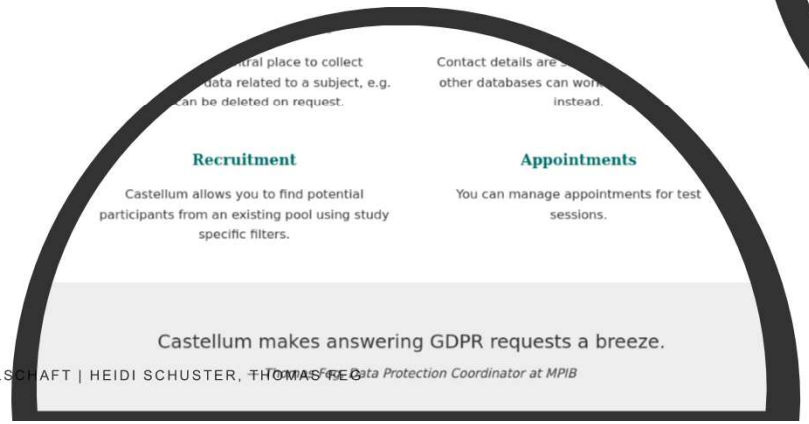
- Scrum
- Taiga
- Django
- Pad
- GIT
- GIT Pages
- ...

ESSENTIALS

- Monatliche Treffen mit
  - DSB,
  - IT-Sec,
  - DSK's der beteiligten Institute
- Bestimmen der User Stories für den Sprint







USER STORIES

Fragestellung:

Wie sollen wir handeln, wenn potentiell beim Export sensible Daten in ein anderes System wandern bei dem wir keine Permission-Kontrolle mehr haben?

Antwort:

- Belehrungen/Schulungen sind (wahrscheinlich) das einzige Mittel
- Bei Exporten in Castellum sollten Warnungen wiederspiegeln, dass dadurch Permissions umgangen werden könnten (am besten positiv formuliert)

Fragestellung:

Übersetzungen von Einwilligungen: Formal das gleiche Dokument?

Anwort:

- “In der Sprache, die die unterzeichnende Person ausreichend versteht”
- Sprachfassungen sind rechtlich gleichwertig, trotzdem sollte man die konkret verwendete Sprache der Einwilligung irgendwie nachvollziehen können; es reicht wohl aus das unterschriebene Dokument zu prüfen (und nicht in Castellum speichern welche Sprachversion)

USER STORIES

Fragestellung:

14-Tage Backupbereinigung bei Löschgesuch

Antwort:

- Das Thema Backup wird in juristischen Texten vergessen/übergangen, alles bezieht sich immer nur auf produktiv
- man muss löschen, wenn Einwilligung zurückgezogen wird UND keine andere Grundlage zu finden ist; Aufbewahrungspflichten könnten hier eine Begründung sein
- Interessenabwägung bei Backups, da völlig neuer Zweck dieser Datenverarbeitung; man muss aber sicherstellen, dass bei Rückspielung produktiv nichts ursprünglich gelöschtes wieder auftaucht;
- man sollte begründen, warum man einen bestimmten Backup-Zyklus benötigt;
  6 Monate, um Gefahrenabwehr bei Bedrohungsszenarien zu gewährleisten (BSI: 6-9 Monate)
- Kommunikation im Rahmen von Betroffenenrechten für bis zu 3 Jahre aufheben

USER STORIES

Fragestellung:

Gesetzliche Grundlage für Gesetzliche Vertreter*in: Art. 6 Abs. 1 lit.a, Art. 9 Abs. 2 lit.a DSGVO und §§ 1626, 1902 BGB

Antwort:

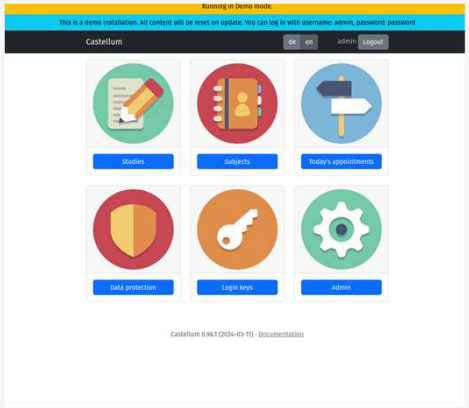
- Alleiniges Sorgerecht oder Verlagerung des Themas auf das anwesenden Elternteil:
  *Als Sorgeberechtigte*r bzw. gesetzliche*r Vertreter*in eines*r minderjährigen Studienteilnehmers*in versichere ich, dass ich auch im Namen des*der zweiten Sorgeberechtigten handle oder alleine sorgeberechtigt bin."*

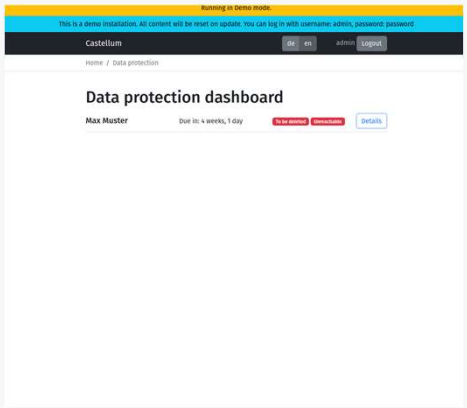
Fragestellung:

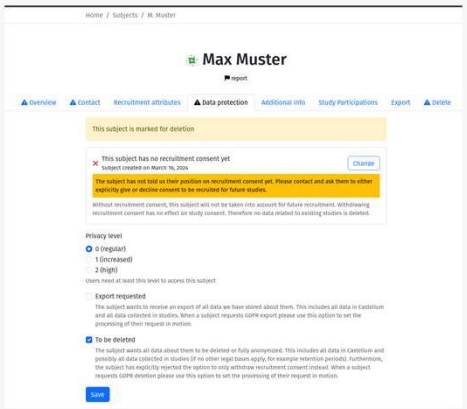
Namensänderung; kein *Also Known As*-Feld. Bedeutet organisatorischer Prozess für alte Einwilligungen?

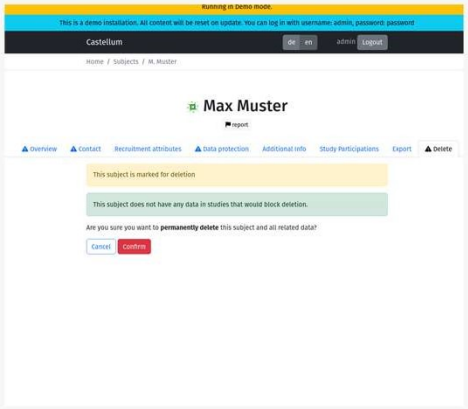
Antwort:

- Man kann davon ausgehen, dass betreffende Person auf anderen Namen hinweist, wenn Einwilligung nicht gefunden werden kann (Mitwirkungs-/Mitteilungspflicht)
- Aus technischer Managementsicht, kann das aber praktikabel sein – "Finden können!"
- Möglichkeit: neuen Datensatz anlegen und vermerkt im "alten" die Änderung vermerken









DATA PROTECTION DASHBOARD

- Benachrichtigung via E-Mail an Funktionalaccount
- Übersichtliches Dashboard
- Bei Studienteilnahme Hinweise auf weitere Daten

HERZLICHEN DANK FÜR IHRE AUFMERKSAMKEIT

Bei Fragen wenden Sie sich gerne an:

Heidi Schuster
Datenschutzbeauftragte

Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V.
Hofgartenstr. 8, 80539 München

Telefon + 49 89 2108-1554
E-Mail heidi.schuster@gv.mpg.de

Thomas Feg
Datenschutzkoordinator

Max-Planck-Institut für Bildungsforschung
Lentzeallee 94, 14195 Berlin

Telefon + 49 30 82406-313
E-Mail thomas.feg@mpib-berlin.mpg.de

https://max.mpg.de/Zentrale-Beauftragte/Datenschutz