



BfDI

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Digitale Identitäten und Deutsche Brieftasche

Datenschutz durch Technikgestaltung

Manuel Peter

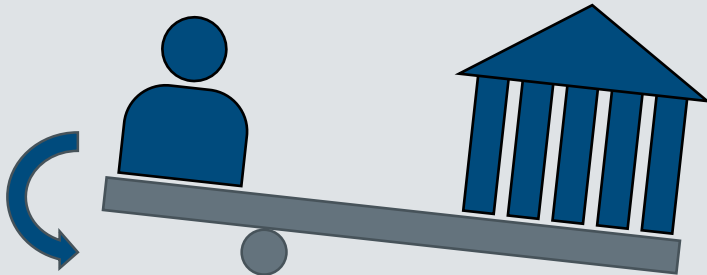
Referat 21 – Projekte der angewandten Informatik, Telematik



Es gibt eine Informationsasymmetrie zwischen Personen und Institutionen. Datenschutz schützt Menschen vor Machtungleichgewicht.

Datenschutz...

...ist notwendig, weil ein **Machtungleichgewicht** zwischen Individuum und Staat oder Individuum und Unternehmen existiert.



Regeln, Technik und Maßnahmen schützen von Anfang an (**Privacy by Design**) und auch ohne das Einzelne sich kümmern müssen (**Privacy by Default**).

Häufige Missverständnisse



Digitale Selbstverteidigung ist kein effektiver Datenschutz. Ein Selbstschutz kann aufgrund der Informationsasymmetrie nur ein Zusatz zu systemischen Maßnahmen sein.

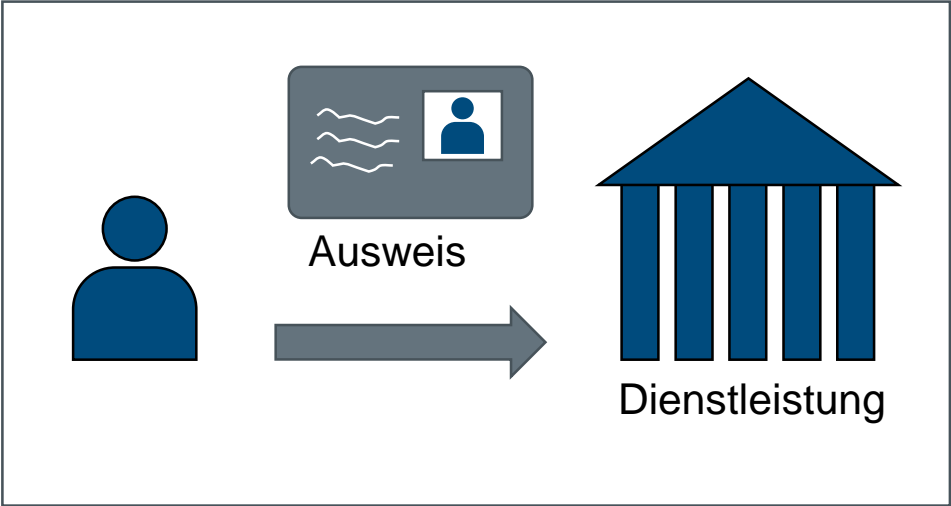


Datensicherheit alleine ist kein Datenschutz. Auch „sichere“ Datenverarbeitung kann die Rechte Einzelner gefährden, wenn nur die Interessen der mächtigeren Partei beachtet werden.

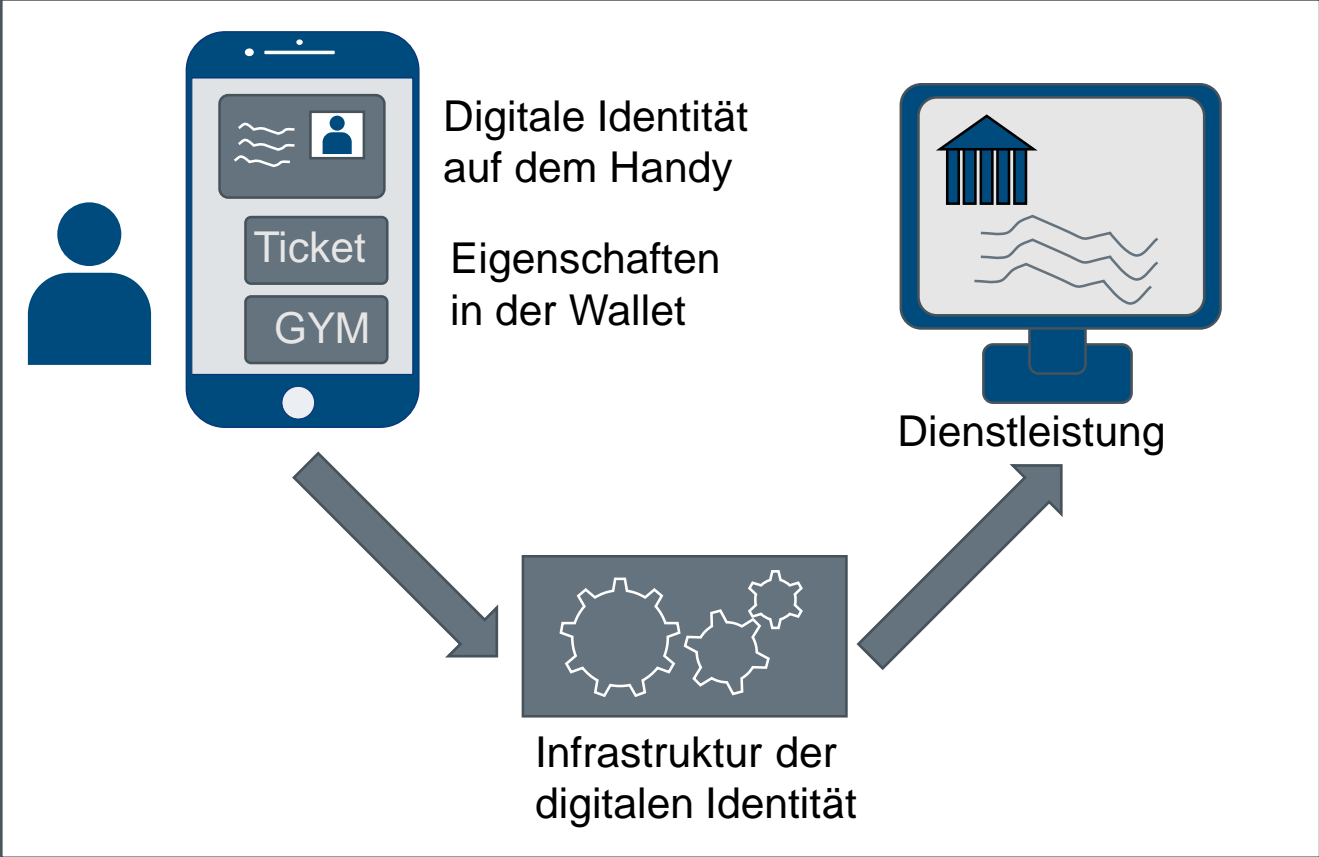
Durch eIDs wird „Ausweisen“ digitalisiert und häufiger. Deshalb müssen die Systeme die Rechte der Bürgerinnen entsprechend schützen.

Identifizierung...

im Analogen



digitalisiert



Die eIDAS-Verordnung legt wichtige Rechte für Bürgerinnen und Bürger sowie Funktionsmerkmale der EUDI-Wallet fest.



Freiwilligkeit der Nutzung
(Art. 5a Abs. 15 S. 1)

Nichtdiskriminierungsklausel
(Art. 5a Abs. 15 S. 2 und 3)



Selektive Offenlegung
(Art. 5a Abs. 4 lit. a)

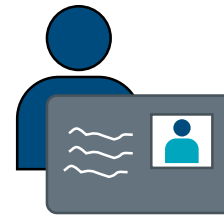
Beschränkung der Relying Partys auf
vorher registrierte Datenkategorien
(Art. 5b Abs. 3)



Übersicht über Transaktionen und Zugriffe in
einem Dashboard
(Art. 5a Abs. 4 lit. d)



Datenverarbeitungen in der Wallet unter
alleiniger Kontrolle der Nutzenden
(Art. 5a Abs. 4 lit. a)



Recht auf pseudonyme Nutzung
(Art. 5a Abs. 4 lit. b)

Pseudonym ist Default-Case
(Art. 5b Abs. 3)



Herunterladen von Daten
(Art. 5a Abs. 4 lit. d)

Datenübertragbarkeit
(Art. 5a Abs. 4 lit. e und f)

Die eIDAS-Verordnung legt wichtige Rechte für Bürgerinnen und Bürger sowie Funktionsmerkmale der EUDI-Wallet fest.



Freiwilligkeit der Nutzung
(Art. 5a Abs. 15 S. 1)

Nichtdiskriminierungsklausel
(Art. 5a Abs. 15 S. 2 und 3)

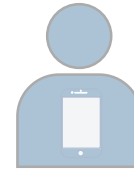


Selektive Offenlegung
(Art. 5a Abs. 4 lit. a)

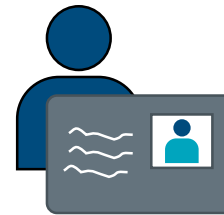
Beschränkung der Relying Partys auf
vorher registrierte Datenkategorien
(Art. 5b Abs. 3)



Übersicht über Transaktionen und Zugriffe in
einem Dashboard
(Art. 5a Abs. 4 lit. d)



Datenverarbeitungen in der Wallet unter
alleiniger Kontrolle der Nutzenden
(Art. 5a Abs. 4 lit. a)



Recht auf pseudonyme Nutzung
(Art. 5a Abs. 4 lit. b)

Pseudonym ist Default-Case
(Art. 5b Abs. 3)



Herunterladen von Daten
(Art. 5a Abs. 4 lit. d)

Datenübertragbarkeit
(Art. 5a Abs. 4 lit. e und f)

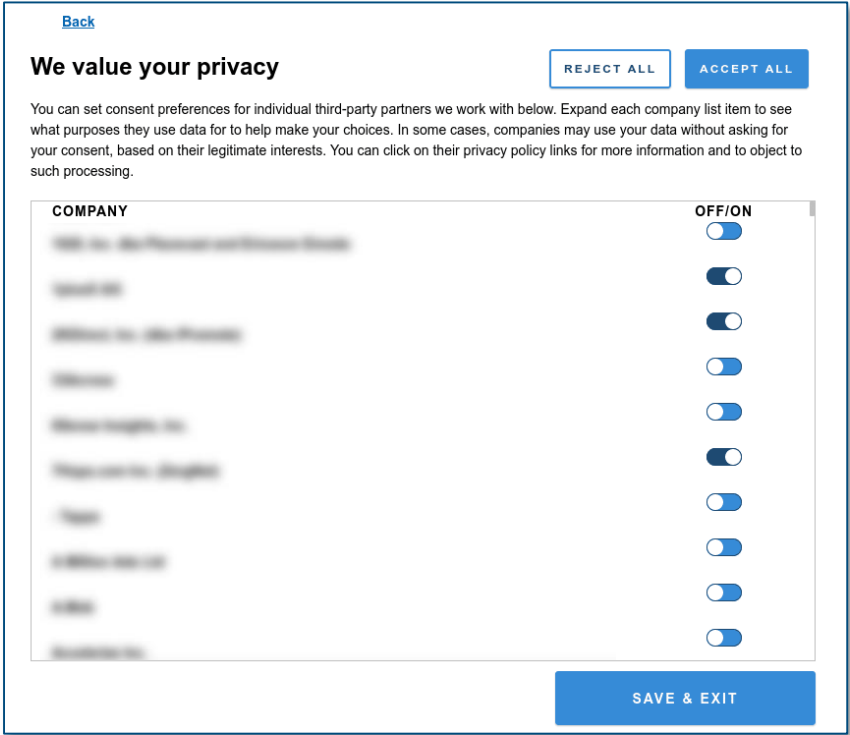
Selektive Offenlegung legt Möglichkeiten und Verantwortung in Nutzendenhand. Sie muss systemisch von der Wallet unterstützt werden.



Selektive Offenlegung

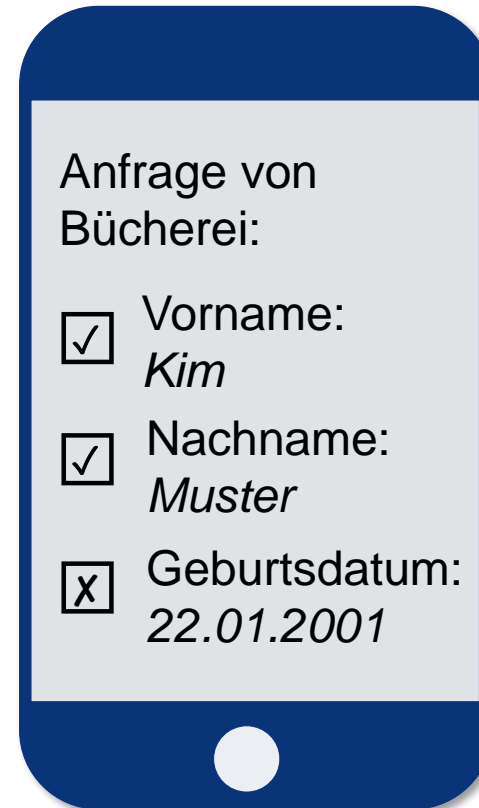
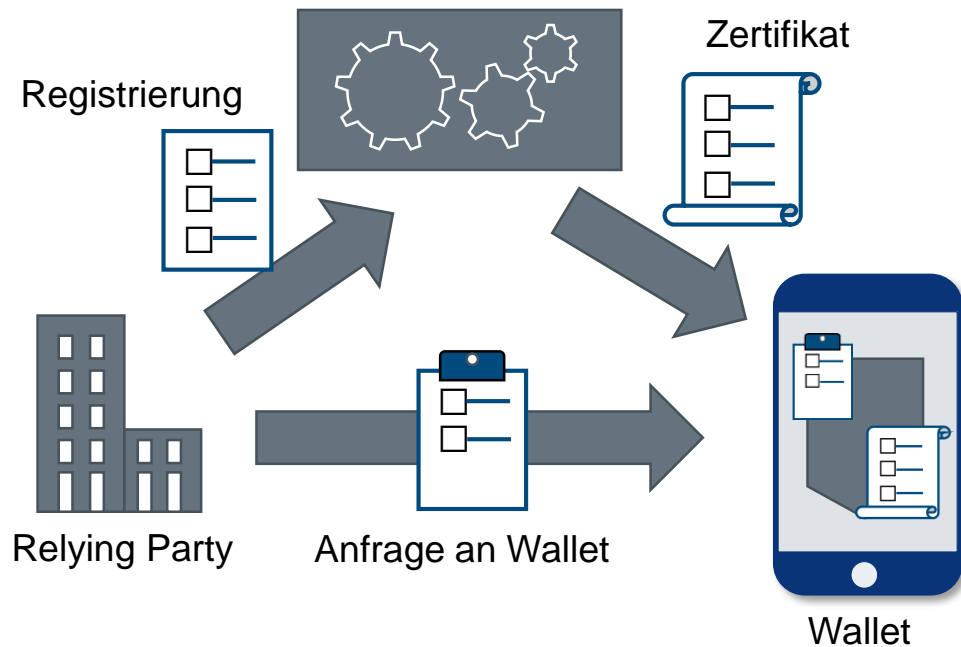


Datenminimierung
(Art. 5 Abs. 1 lit. c DSGVO)
in Hand der Nutzenden



Cookie-Banner-Szenario
muss vermieden werden

Um eine Situation wie bei den Cookie-Bannern zu vermeiden, braucht es eine klare Nutzerführung und technische Unterstützung durch die Wallet

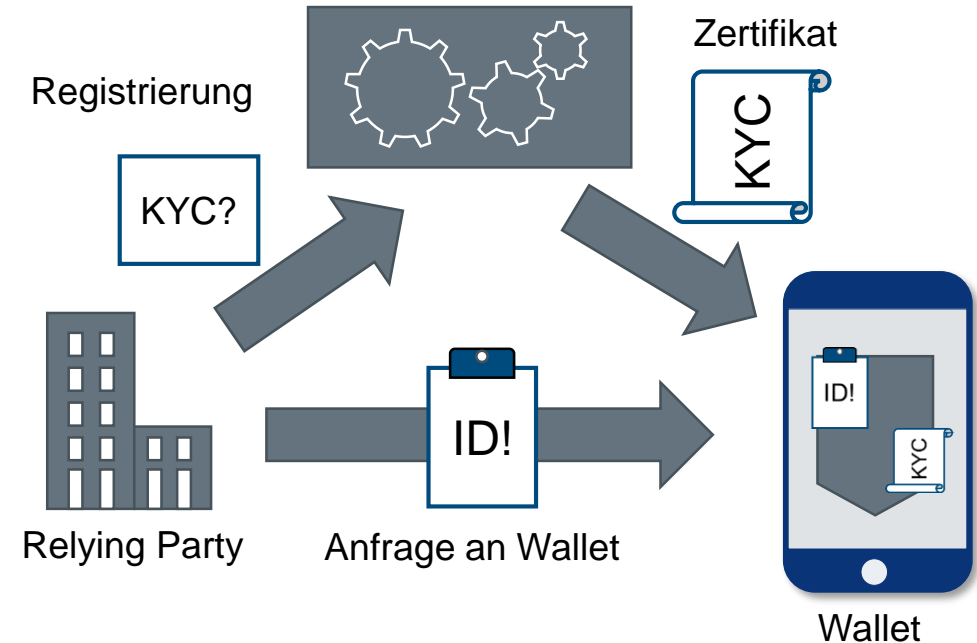


- Wallet vergleicht angefragte Datenfelder mit den registrierten Daten
- UI zeigt klar an, dass Wahlmöglichkeit besteht

Pseudonyme sind eine Maßnahme gegen Überidentifizierung. Für eine wirksame Umsetzung des Rechts müssen sie einfach nutzbar sein.

Pseudonyme

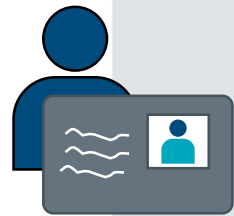
- Pseudonyme sind Maßnahme gegen Überidentifizierung
- Pseudonyme müssen lokal verwaltet werden können (Art. 5a Abs. 4 lit. c)
- **Pseudonyme Nutzung ist der Default Case (Art. 5b Abs. 3)**



Unterscheidbarkeit des KYC-Falls

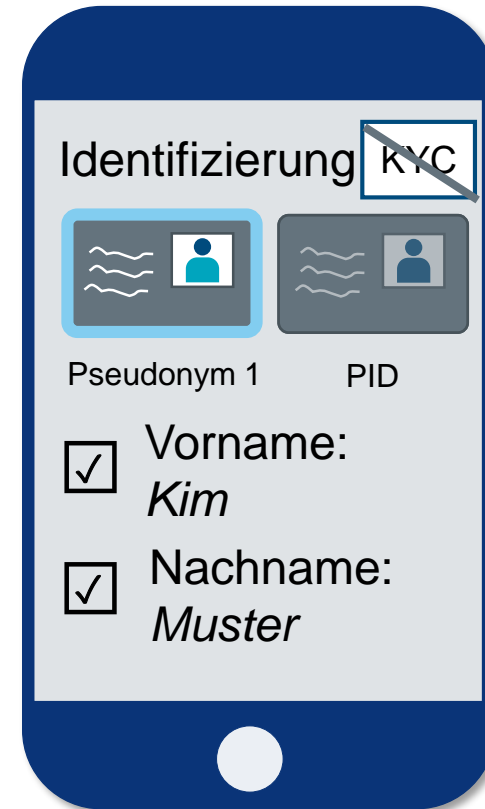
- Identifikation darf nur gefordert werden, wenn ein rechtliche Verpflichtung vorliegt.
- Unterscheidung ob Identifizierung notwendig nicht durch Nutzer

Damit Pseudonyme nutzbar sind, muss die UI sie als Default Case anbieten. Ihre Nutzung muss so einfach wie die PID-Nutzung sein.



Pseudonyme

- Pseudonyme sind Maßnahme gegen Überidentifizierung
- Pseudonyme müssen lokal verwaltet werden können (Art. 5a Abs. 4 lit. c)
- Pseudonyme Nutzung ist der Default Case (Art. 5b Abs. 3)



Nutzbarkeit

- Nutzende müssen erkennen, dass Sie das Recht haben ein Pseudonym zu nutzen
- Anwendung muss genauso einfach sein wie PID-Nutzung
- Im Nicht-KYC-Fall sollten auch die PID-Daten als Pseudonym gesendet werden.

**Die Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit**

Manuel Peter

Referat 21

Graurheindorfer Str. 153

53117 Bonn

FON +49 (0)228-997799-2108

manuel.peter@bfdi.bund.de

www.bfdi.bund.de



Identifizierung soll nur dort stattfinden, wo sie notwendig ist. Risiken von ID-Systemen kann mit rechtlich-technischem Rahmen begegnet werden.



Digitale Identitäten bergen Risiken:

- 1) Überidentifizierung
- 2) Tracking und Profilbildung
- 3) Identitätsdiebstahl



Grundsätzliche Feststellungen

- Identifizierung nur, wo zwingende Notwendigkeit besteht
- **Risiken digitaler Identitäten** müssen durch eine entsprechend datenschutzfreundliche Ausgestaltung des **rechtlichen und technischen Rahmens** begegnet werden