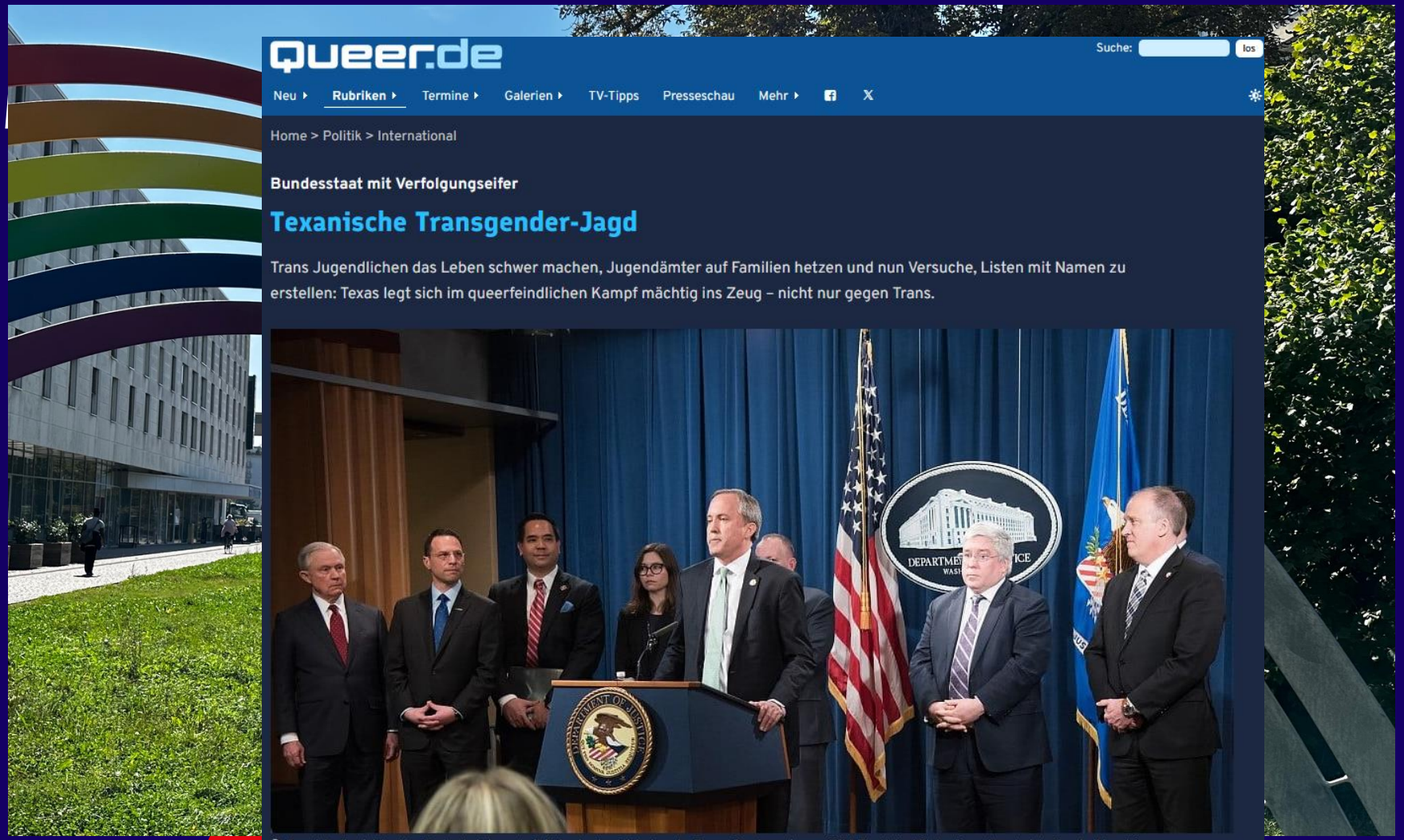
Informatik Festival 2024

Multi-Party Computation als Instrument zur Umsetzung datenschutzkonformer behördlicher Datenabgleiche

Eine interdisziplinäre Analyse am Beispiel der Diskussionen um das Gesetz zur Selbstbestimmung über den Geschlechtseintrag

Linda Seyda, Andreas Brüggemann, Gerrit Hornung und Thomas Schneider

IM GEDENKEN AN DIE
OPFER DES §175 StGB



Queer.de

Suche: los

Neu | Rubriken | Termine | Galerien | TV-Tipps | Presseschau | Mehr

Home > Politik > International

Bundesstaat mit Verfolgungseifer

Texanische Transgender-Jagd

Trans Jugendlichen das Leben schwer machen, Jugendämter auf Familien hetzen und nun Versuche, Listen mit Namen zu erstellen: Texas legt sich im queerfeindlichen Kampf mächtig ins Zeug – nicht nur gegen Trans.

Texas' Justizminister Ken Paxton bei einem Auftritt im Justizministerium der Trump-Bundesregierung (Bild: The United States Department of Justice / wikipedia)

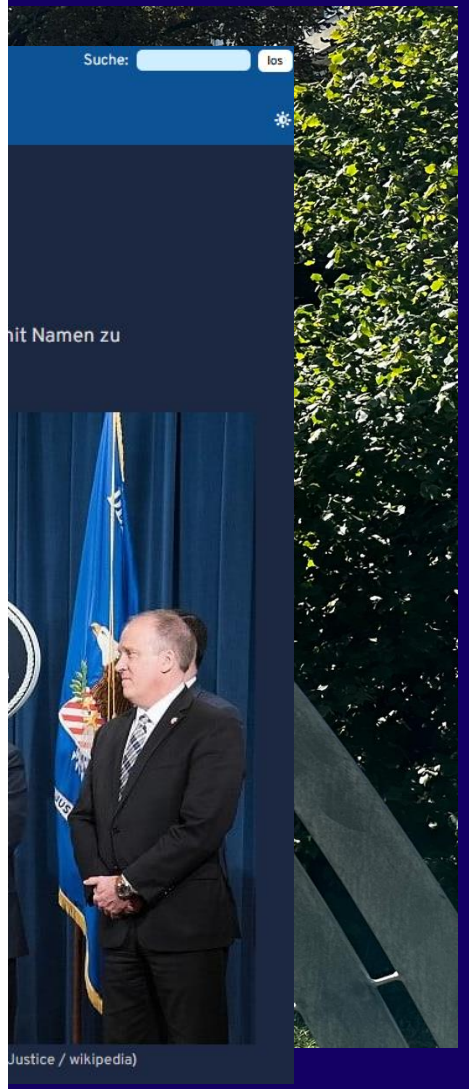
Sexuelle Identität

Zahl der queerfeindlichen Straftaten in Bayern verdoppelt

10. April 2024, 14:14 Uhr | Lesezeit: 1 Min.

Die Zahl der queerfeindlichen Straftaten ist in Bayern von 96 im Jahr 2022 auf 190 im vergangenen Jahr gestiegen. (Foto: Sven Hoppe/dpa)

Süddeutsche Zeitung



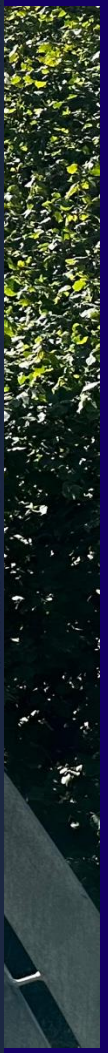
Sachsen

CSD in Bautzen nur mit Polizeischutz möglich

Stand: 11.08.2024 11:19 Uhr

Wegen rechter Gegendemonstrationen hatten die Veranstalter des CSD ihre Aftershow-Party abgesagt. Gefeiert wurde aber trotzdem. Am Sonnabend bahnte sich ein bunter CSD-Demozug ohne Zwischenfälle seinen Weg durch Bautzens Innenstadt. Einsatzkräfte der Polizei hielten dabei rechte Gegendemonstranten auf Abstand.

mdr



Daniel Bache und Frank Laubenburg. "Alljährlich verhindern Polizeibeamte rechtswidrig, dass Puppies an CSD-Demonstrationen teilnehmen können, immer wieder unterschlägt die Polizei homo- und transfeindliche Angriffe am Rande von CSDs in ihrer Öffentlichkeitsarbeit – oder negiert die gruppenbezogene Menschenfeindlichkeit der Angreifer*innen als Motiv."

Sachsen

CSD in Bautzen nur ...

Stand: 11.08.2024 11:19 Uhr

Wegen rechter Gegendemonstrationen hatten die Veranstalter des ... Aftershow-Party abgesagt. Gefeiert wurde aber trotzdem. Am Sonnabend bahnte sich ein bunter CSD-Demozug ohne Zwischenfälle seinen Weg durch Bautzens Innenstadt. Einsatzkräfte der Polizei hielten dabei rechte Gegendemonstranten auf Abstand.

mdr

Queer.de

Daniel Bache und Frank Lauben

rechtswidrig, dass Puppie

wieder unterschlägt

CSDs in ihrer

Mensch

Geraten geheime Informationen in falsche Kanäle?

Amtsträger haben Zugang zu Informationen, die der Öffentlichkeit vorenthalten bleiben. Nach einem Schreiben der GdP, das dem ZDF vorliegt, herrsche in den Innenministerien eine "Nervösität".

Die GdP berichtet von der "Sorge der Sicherheitsbehörden", dass bei "bestimmten Wahlausgängen geheime Informationen in die falschen Hände geraten".

ZDFheute

...nen, immer

...griffe am Rande von

...ppenbezogene

...tiv."

...nen hatten die Veranstalter des ...

...agt. Gefeiert wurde aber trotzdem. Am Sonnabend

...ein bunter CSD-Demozug ohne Zwischenfälle seinen Weg durch

...autzens Innenstadt. Einsatzkräfte der Polizei hielten dabei rechte

Gegendemonstranten auf Abstand.

mdr

Queer.de

Geschlechtliche Vielfalt

Bundestag beschließt Selbstbestimmungs-gesetz

Das Selbstbestimmungsgesetz soll es trans-, intergeschlechtlichen und nichtbinären Menschen erleichtern, ihren Geschlechtseintrag und Vornamen zu ändern. Nach abschließender Beratung wurde das Gesetz nun vom Bundestag verabschiedet.

BMFSFJ

Informatik Festival 2024

Linda Seyda

sie/ihr

UNIKASSEL VERSITÄT

Privacy and Trust for Mobile Users

Gerrit Hornung

Andreas Brüggemann

dey/denen

TECHNISCHE UNIVERSITÄT DARMSTADT

ENCRYPTO
CRYPTOGRAPHY AND PRIVACY ENGINEERING

Thomas Schneider

Begriffe

- **Queer** (LGBTQIA+) = Sammelbezeichnung für sexuelle Orientierungen, die nicht heterosexuell sind, für Geschlechtsidentitäten, die nichtbinär oder nicht-cisgender sind, sowie Lebens- und Liebesformen, die nicht heteronormativ sind

- **Trans*** = Personen, deren Geschlechtsidentität nicht mit dem nach der Geburt zugewiesenen Geschlecht übereinstimmt

- **Nicht-binär** = Menschen, die sich nicht (ausschließlich) als männlich oder weiblich identifizieren und sich als außerhalb der zweigeteilten, binären Geschlechterordnung verstehen

- **Intergeschlechtlich** = Menschen, deren körperliche Geschlechtsmerkmale nicht eindeutig als männlich oder weiblich einzuordnen sind

Das Selbstbestimmungsgesetz (SBGG)

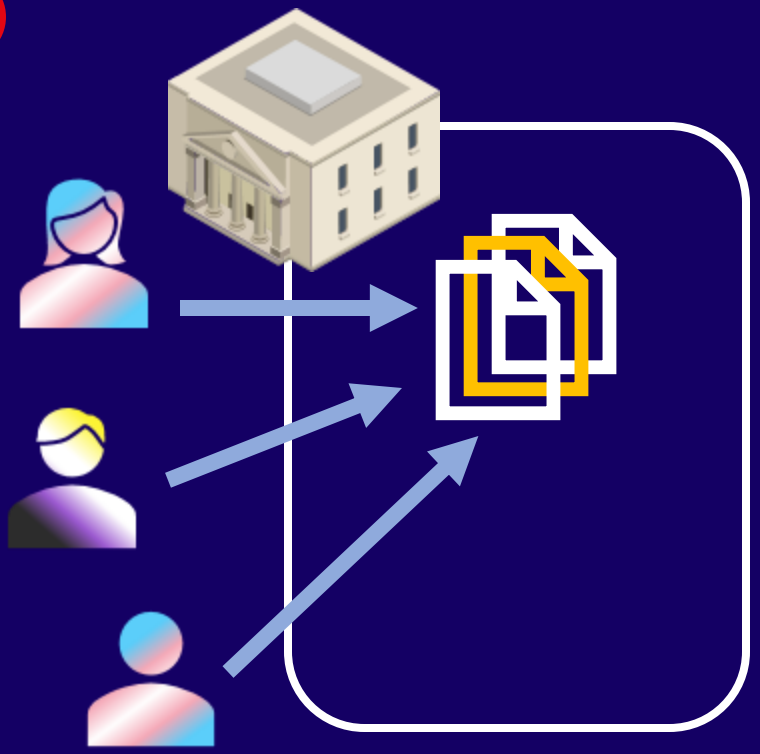
- Zur Ablösung des in Teilen verfassungswidrigen „Transsexuellengesetz“
- Trans*, Intergeschlechtliche und nicht-binäre Personen können durch Eigenerklärung beim Standesamt ihren Vornamen und Geschlechtseintrag ändern
- ab dem vollendeten 14. Lebensjahr keinerlei weitere Nachweise erforderlich
- Anmeldung der Erklärung drei Monate vorher (seit August 2024)
- Offenbarungsverbot, dh. kein Ausforschen der früheren Identität

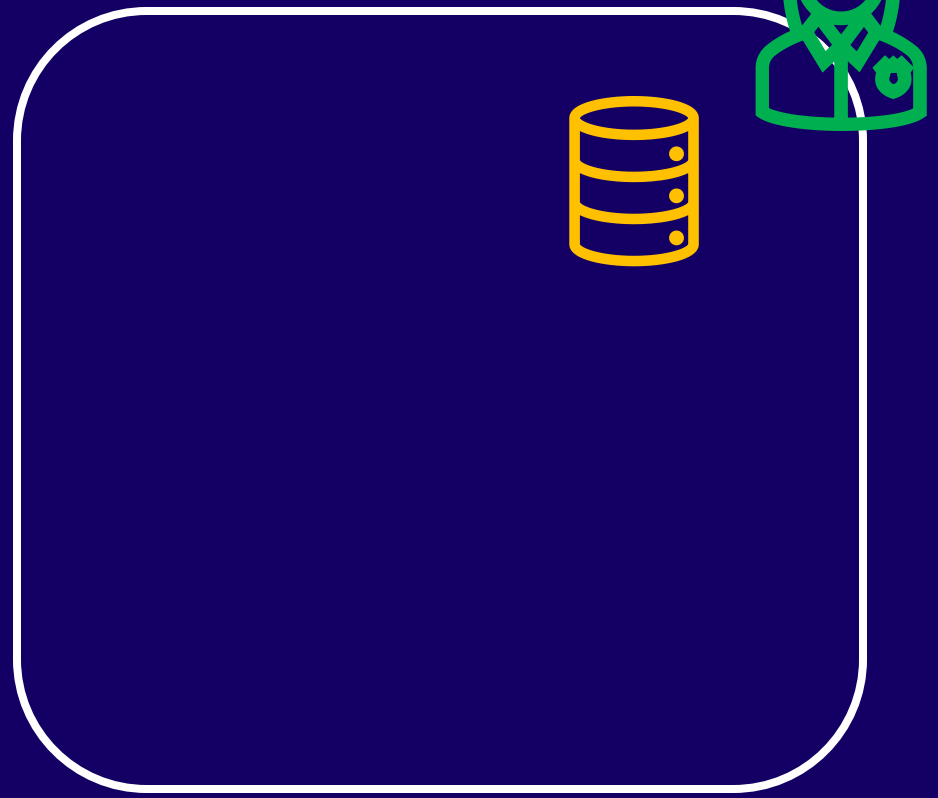
§ 13 Abs. 5 SBGG-RegE

- Zeitweise § 13 Abs. 5 SBGG-RegE: Weitergabe der geänderten Daten an etliche Sicherheitsbehörden zur Nachverfolgbarkeit des Individuums
- Angelehnt an § 20a BZRG:
  - Bei Namensänderungen Meldung an die Behörde und Löschgebot bei Irrelevanz
- Ersatzlose Streichung dieser Regelung aus Gründen der Einheitlichkeit mit dem Namensrecht, *ABER* …

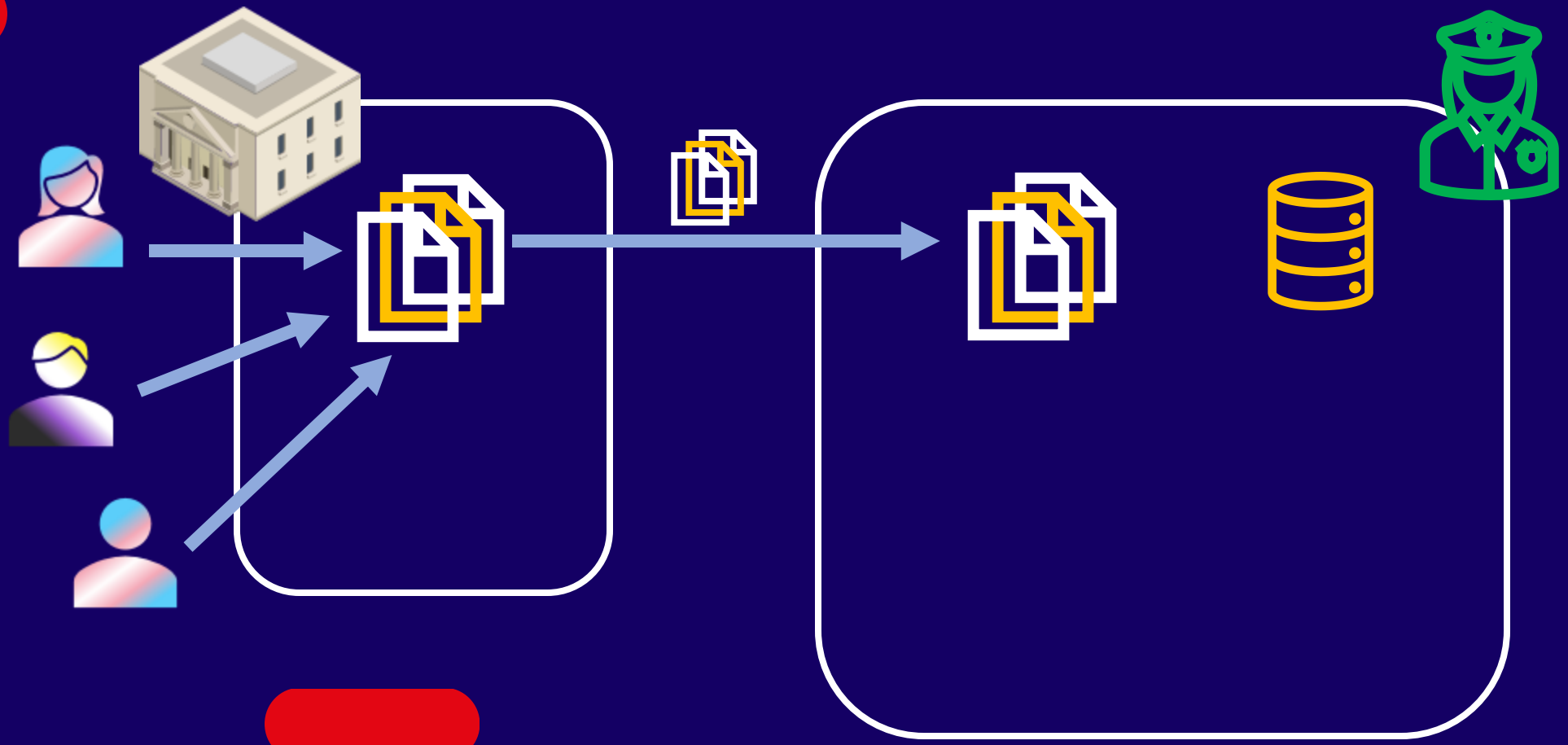
Ursprünglich geplante Datenweitergabe

Ursprünglich geplante Datenweitergabe

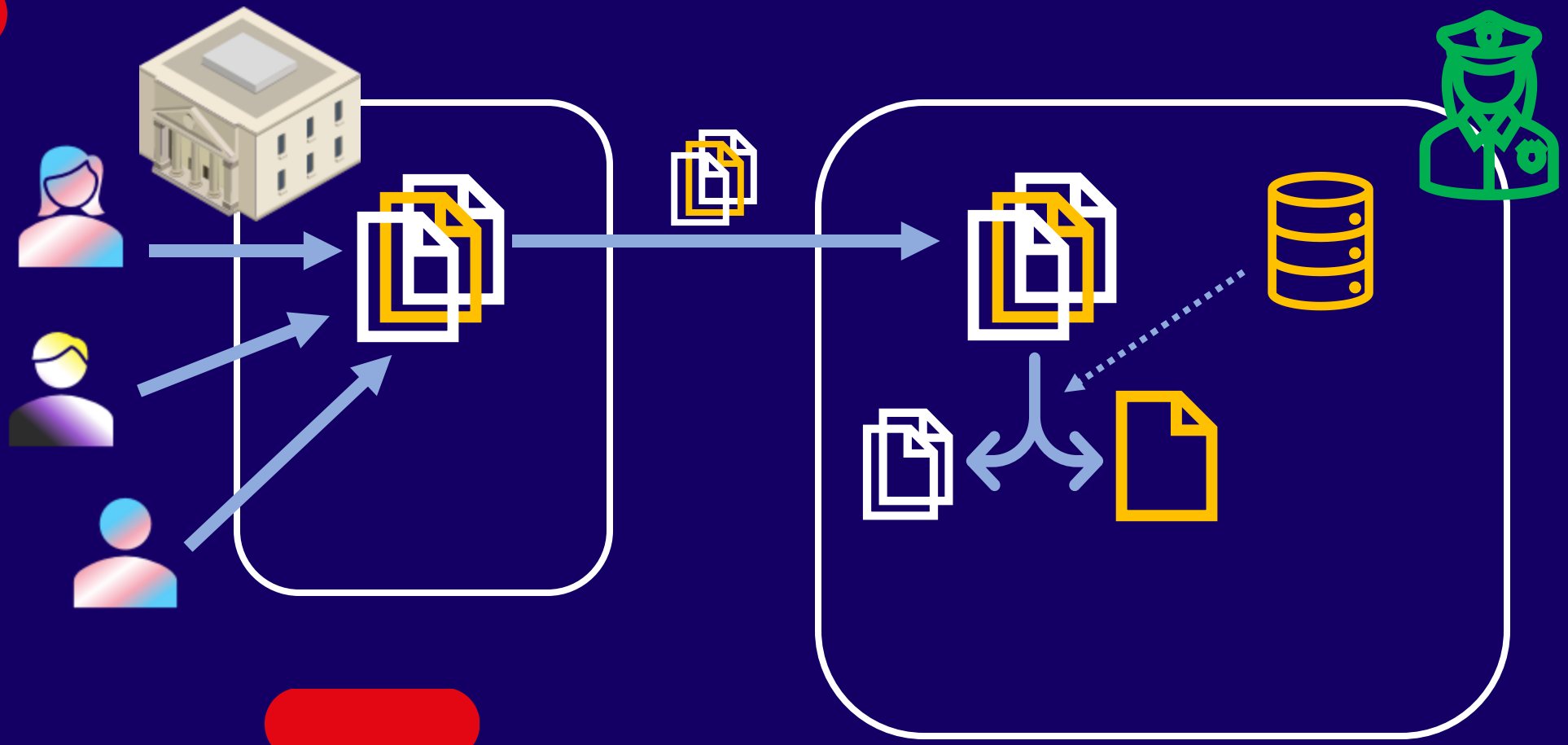




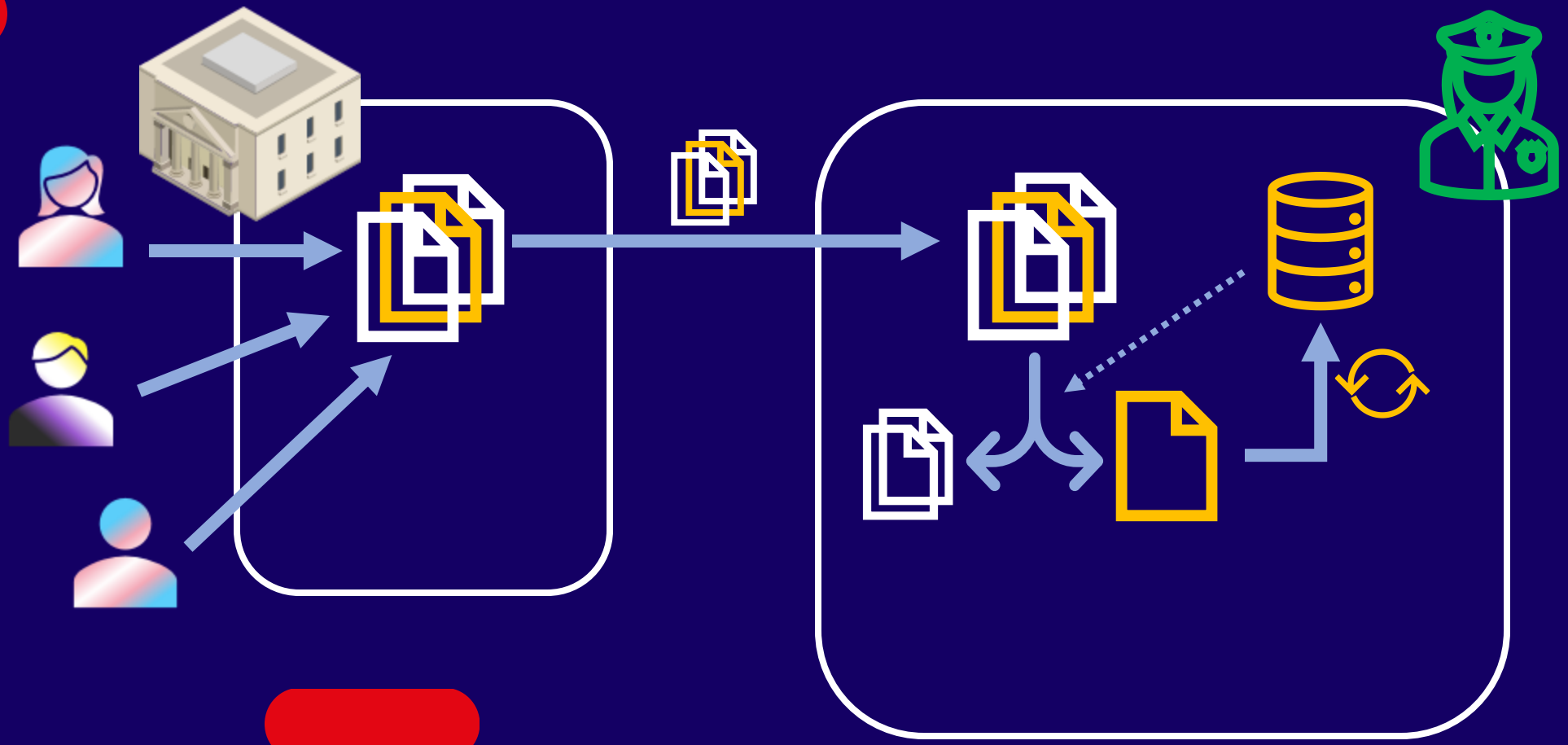
Ursprünglich geplante Datenweitergabe



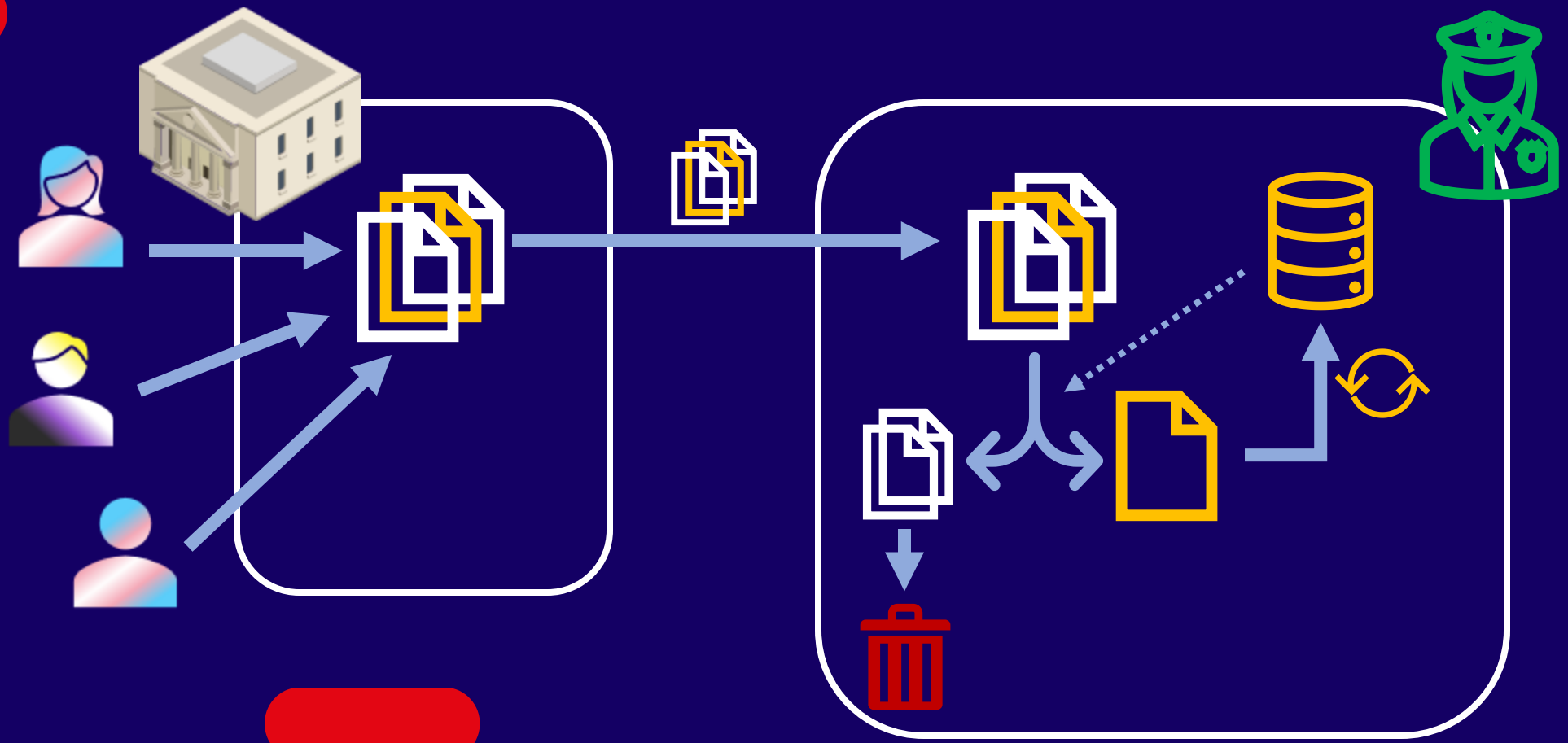
Ursprünglich geplante Datenweitergabe



Ursprünglich geplante Datenweitergabe



Ursprünglich geplante Datenweitergabe



Fortdauernde Relevanz der Problematik

- Entschließungsantrag an die BReg:
  - Reformation des öffentlich-rechtlichen Namensrechts
  - mit weiterem Diskriminierungspotential: Möglichkeit der Änderung „fremdländisch“ klingender Namen
  - Betonung von Datenschutzkonformität und Effektivität (jedoch ohne konkrete Vorschläge)

Die ursprünglich angedachte automatisierte Datenweitergabe könnte also **doch** kommen – in einem anderen Gesetz!

Datenweitergabe an Sicherheitsbehörden

Einerseits…

- Grundsatz der Datenrichtigkeit
  - Personenbezogene Daten müssen richtig und auf aktuellem Stand sein
  - Dies entfällt nach erfolgten Änderungen an Namen und Geschlechtseintrag
- legitime staatliche Interessen
  - An korrekten Daten der Bürger*innen (die schon in behördlichen Datenbeständen geführt wurden)
- Interesse der Betroffenen, mit dem richtigen Namen und der richtigen Anrede adressiert zu werden

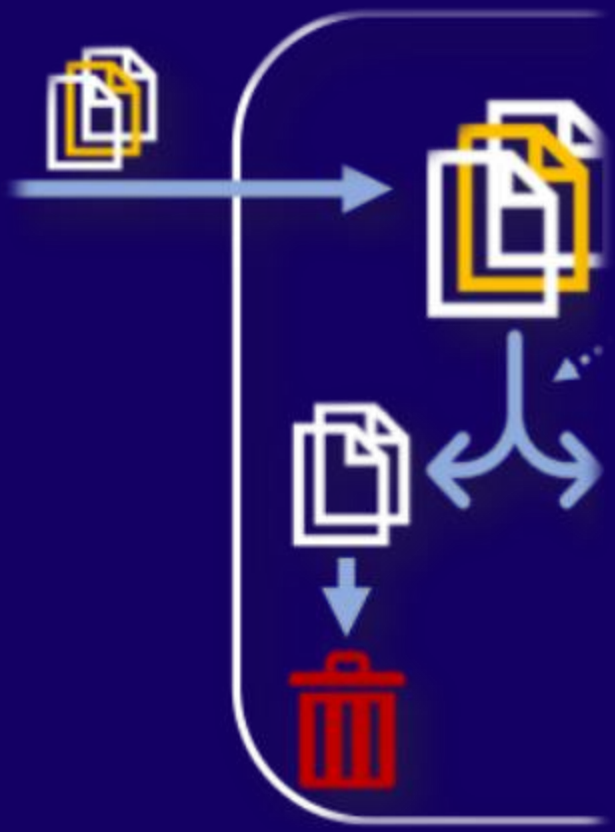
- Pro automatisierte Übermittlung

Datenweitergabe an Sicherheitsbehörden

Andererseits…

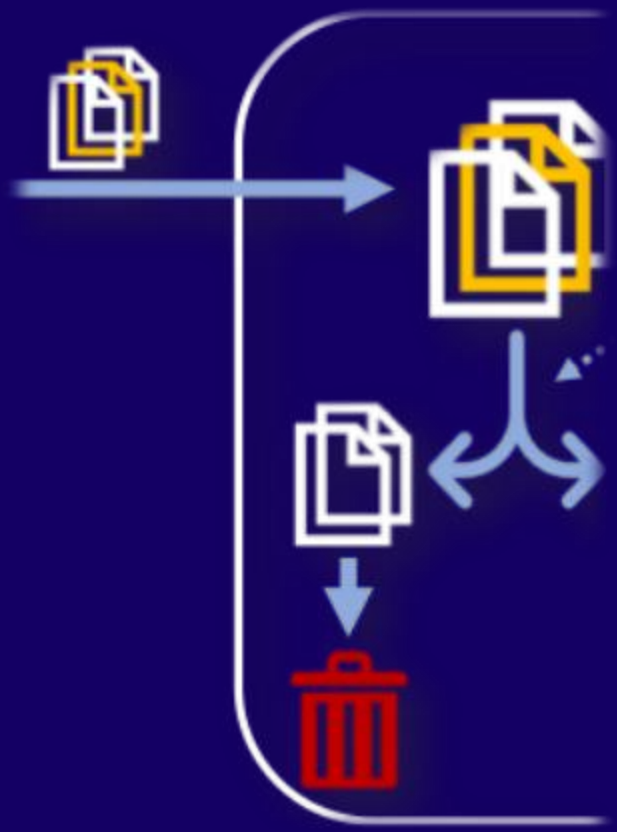
- Grundsatz der Datenminimierung
  - Personenbezogene Daten müssen dem Zweck angemessen sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
  - Benennung des Zwecks: staatliche Sicherheitsinteressen
  - ABER: nur bzgl. der Personen, die bereits in den behördlichen Datenbeständen geführt werden
    - Andernfalls entfällt schon objektiv der Zweck der Verarbeitung
  - (P) Meldende Behörde kann und darf nicht wissen, ob die übermittelnden Daten für die Sicherheitsbehörden relevant sind
    - Contra automatisierte Übermittlung

Technische Bedenken



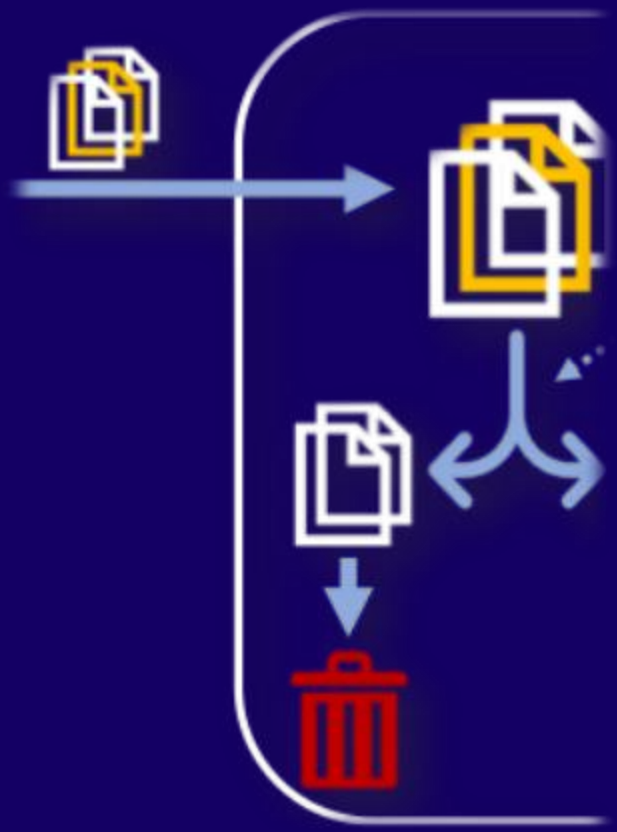
Technische Bedenken

- Zuverlässige Löschung nicht trivial



Technische Bedenken

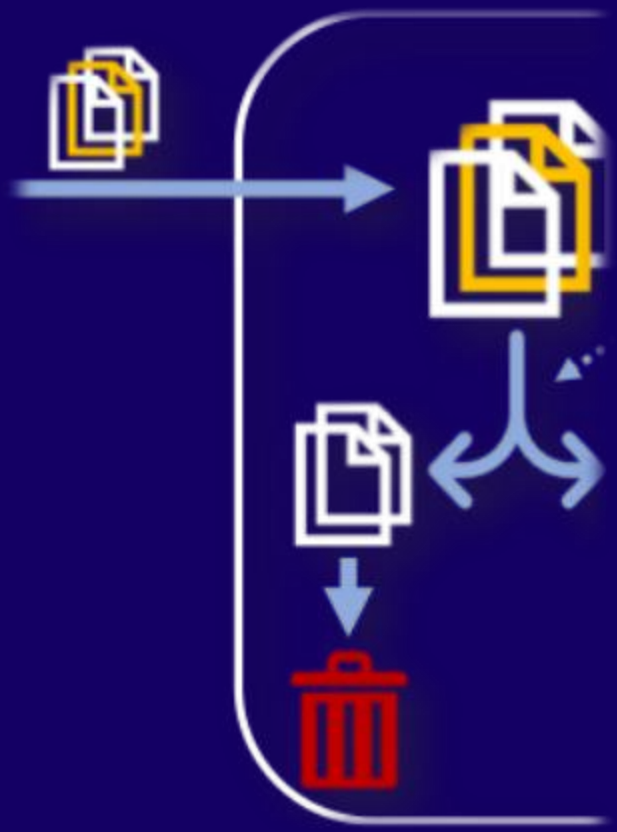
- Zuverlässige Löschung nicht trivial
- Löschung nicht verifizierbar



Technische Bedenken

- Zuverlässige Löschung nicht trivial
- Löschung nicht verifizierbar

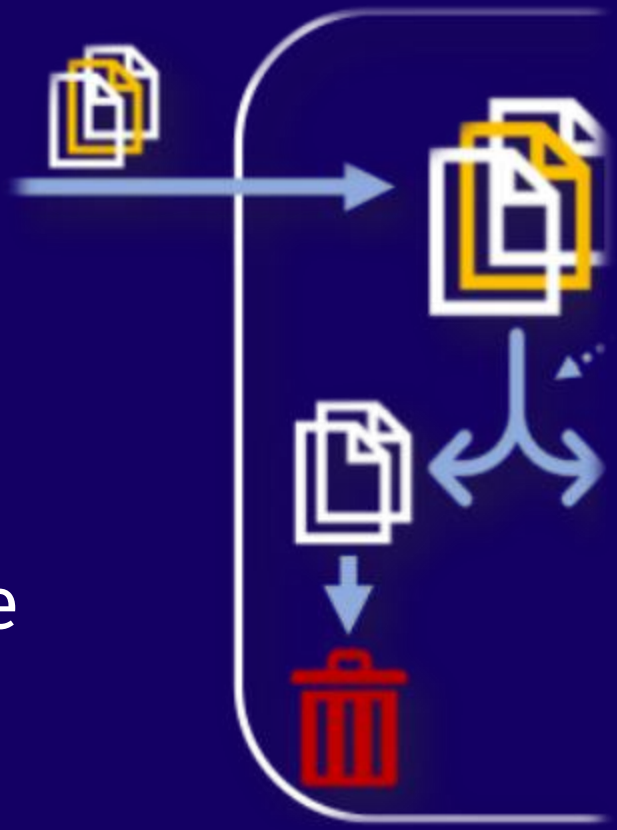
- Aktives Abgreifen von Daten



Technische Bedenken

- Zuverlässige Löschung nicht trivial
- Löschung nicht verifizierbar

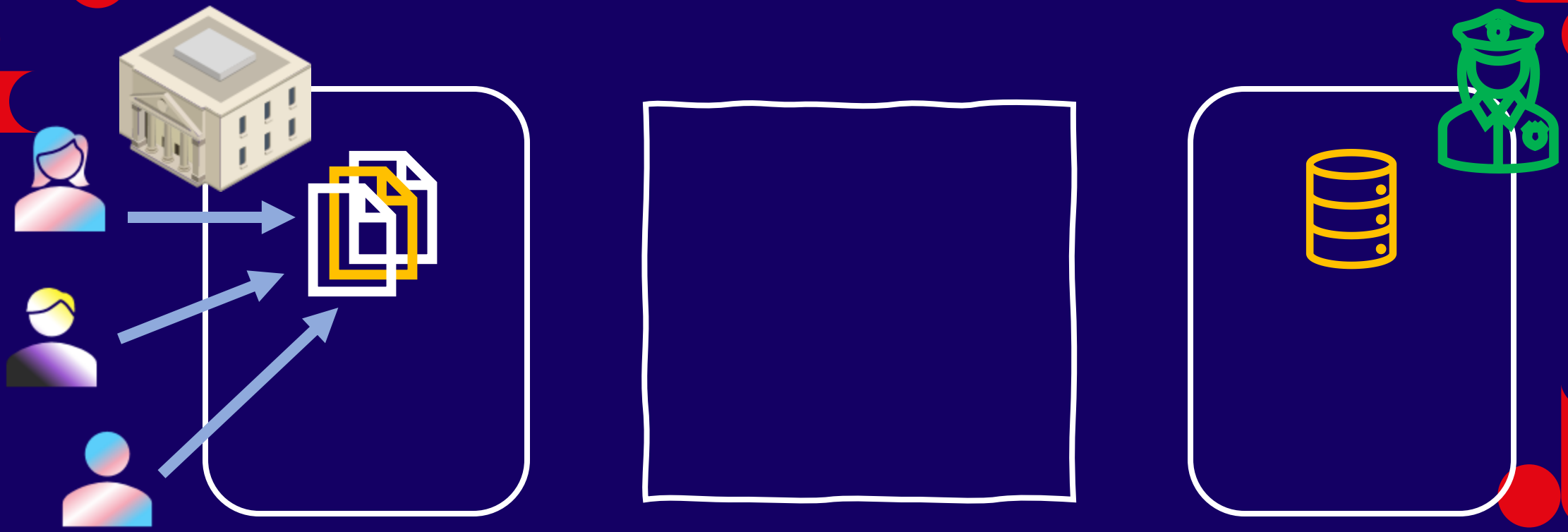
- Aktives Abgreifen von Daten
- Passives Abgreifen durch automatisierte Logs, Backups, …



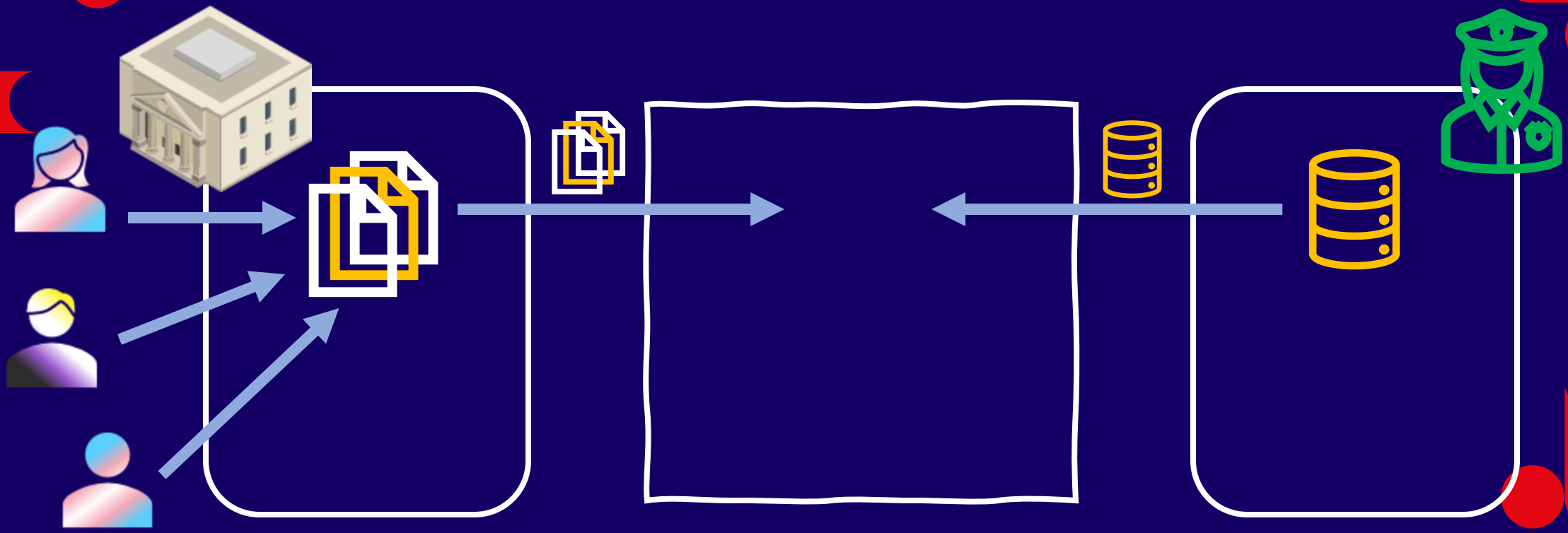
Datenschutzrechtliches Dilemma

- Theoretisch müsste zwischen Datenminimierung oder Datenrichtigkeit entschieden werden
- Geänderte Namens- und Geschlechtseinträge müssen korrigiert werden, aber nur, wenn die Daten für die jeweilige Sicherheitsbehörde relevant sind
- Relevanz kann nicht antizipiert werden
- Problem ist dem Gesetzgeber bekannt (vgl. Gesetzesbegründung zu § 20a BZRG)
- Lösung durch Technik?

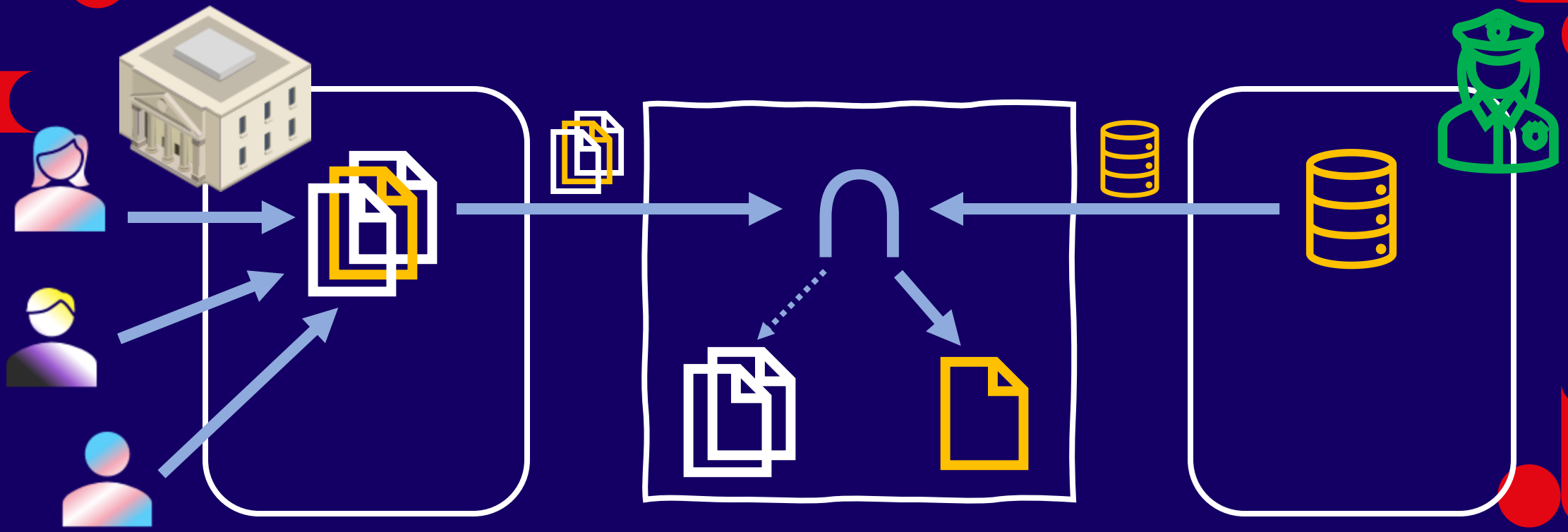
Angestrebte Funktionalität



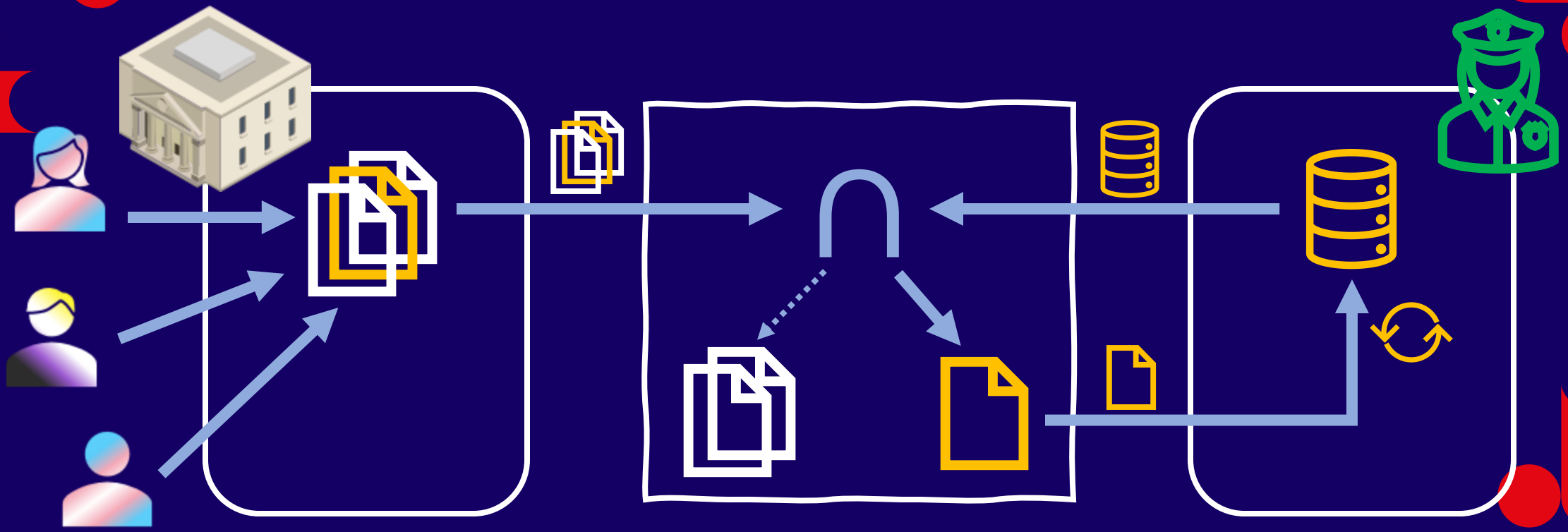
Angestrebte Funktionalität



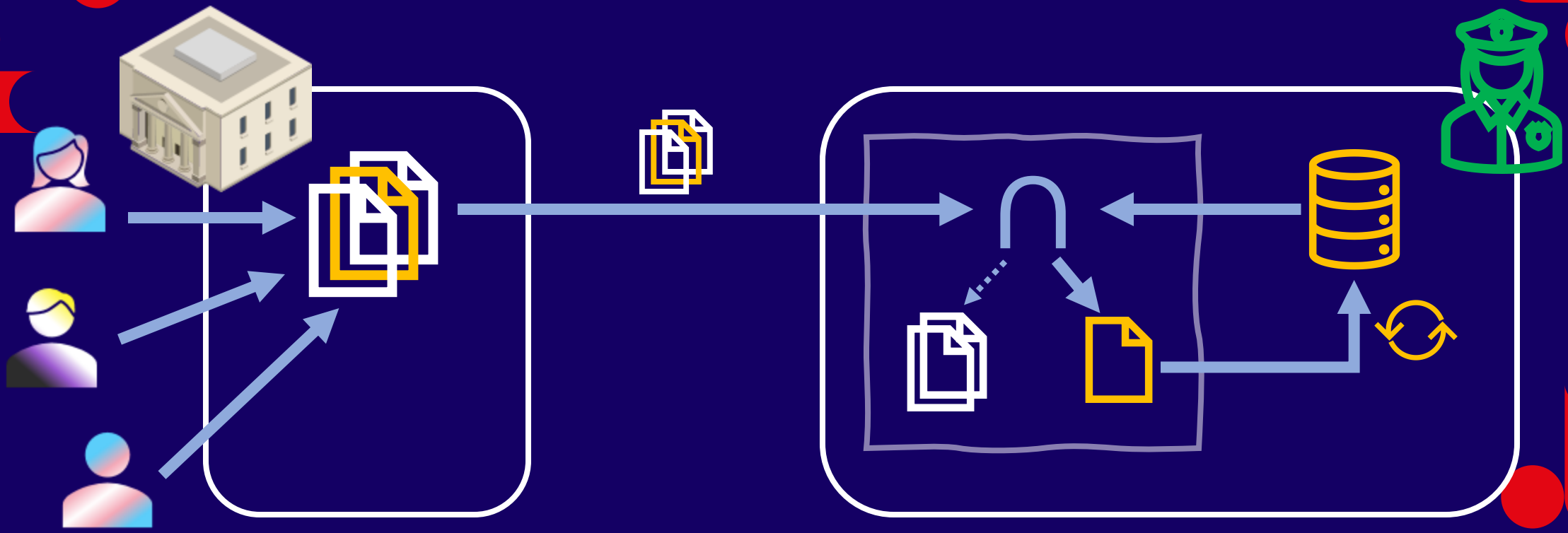
Angestrebte Funktionalität



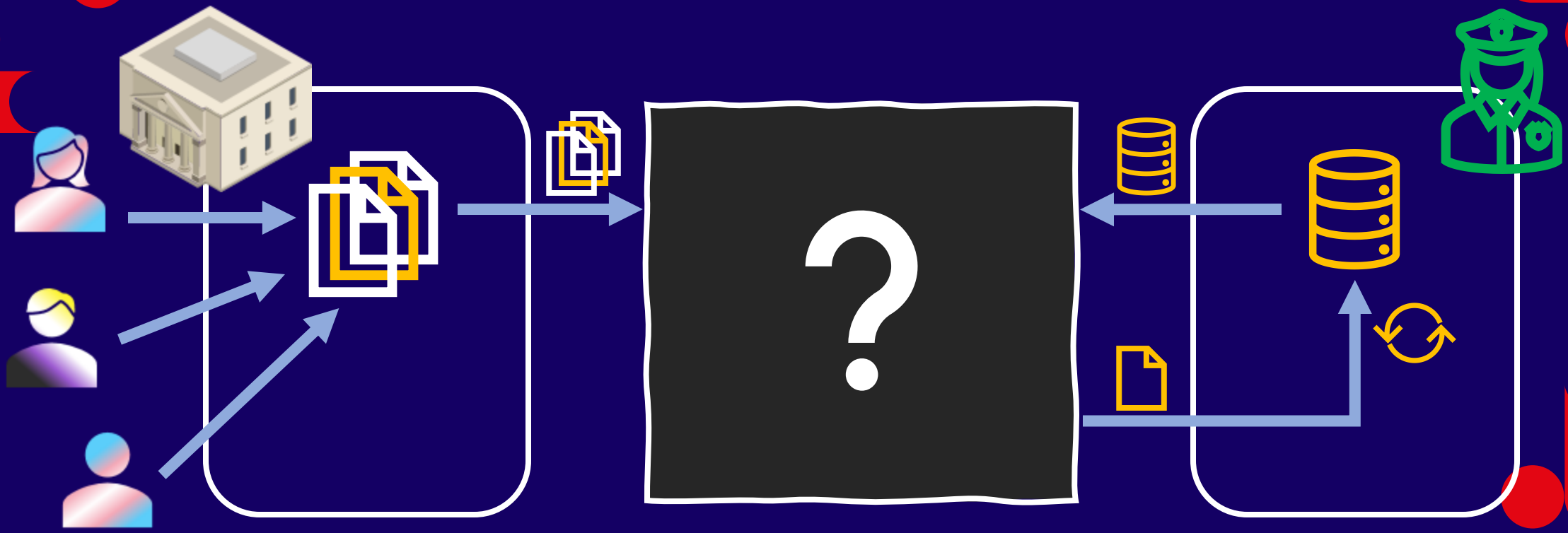
Angestrebte Funktionalität



Riskante Umsetzung (ursprünglich für SBGG geplant)



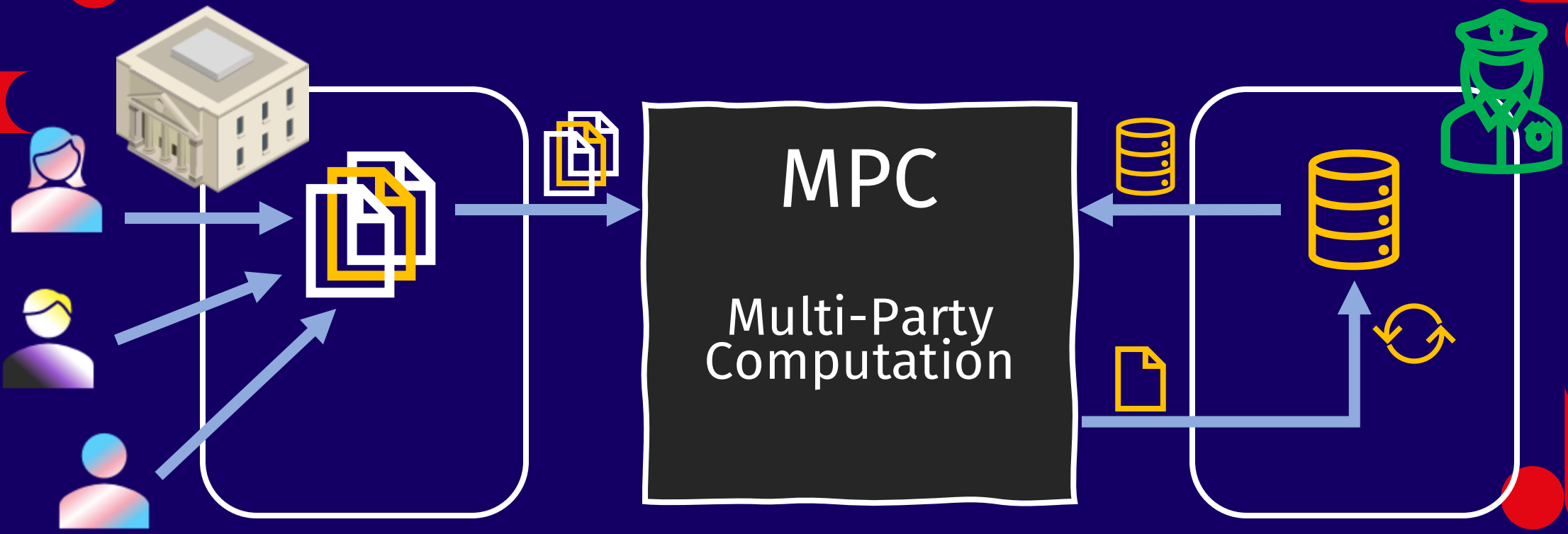
Ideale Umsetzung als Black-Box?



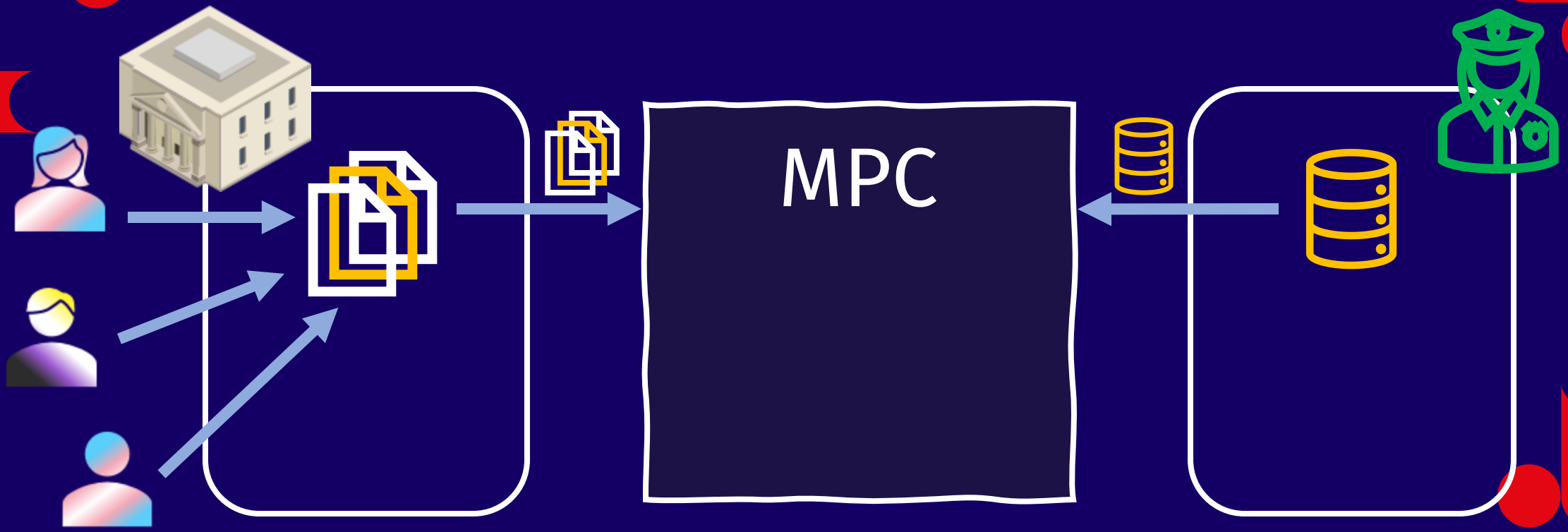
Ideale Umsetzung **unmöglich?**

„Die Mitteilungen über Namensänderungen können nicht auf die Personen beschränkt werden, über die das Register eine Eintragung enthält, da dies den Gerichten und Behörden, deren Entscheidungen Namensänderungen bewirken, regelmäßig nicht bekannt sind.“
(Gesetzesbegründung zu § 20a BZRG,
BT-Drs. 13/4709, 1996)

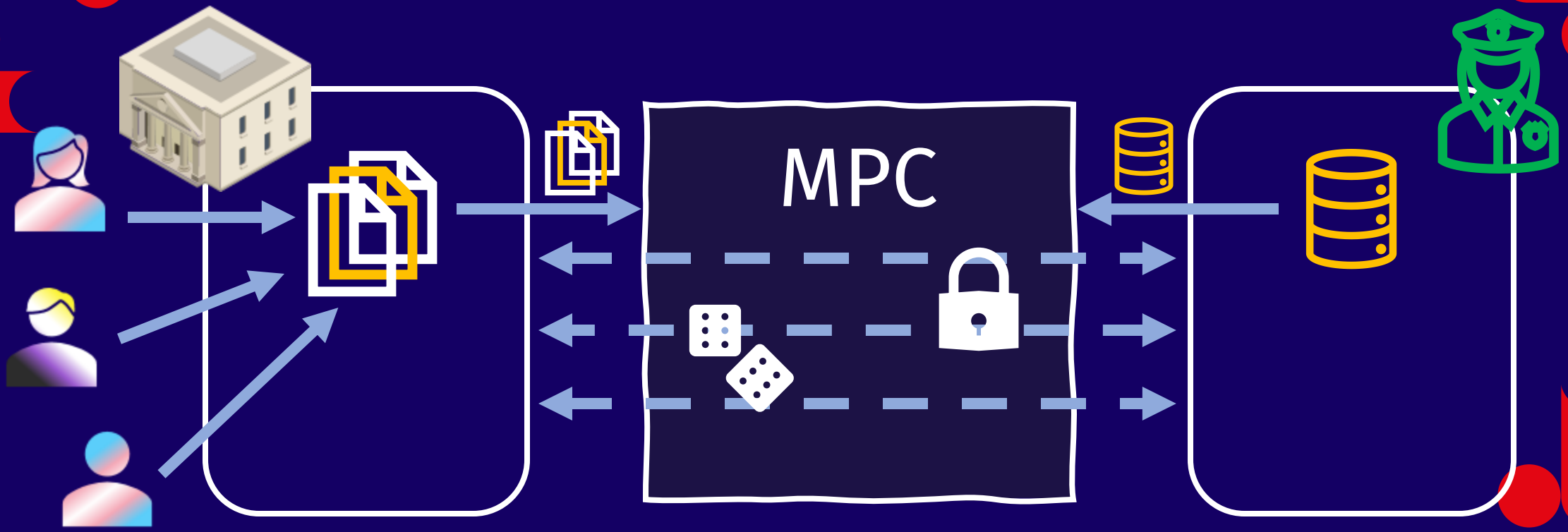
Ideale Umsetzung **ist möglich!**



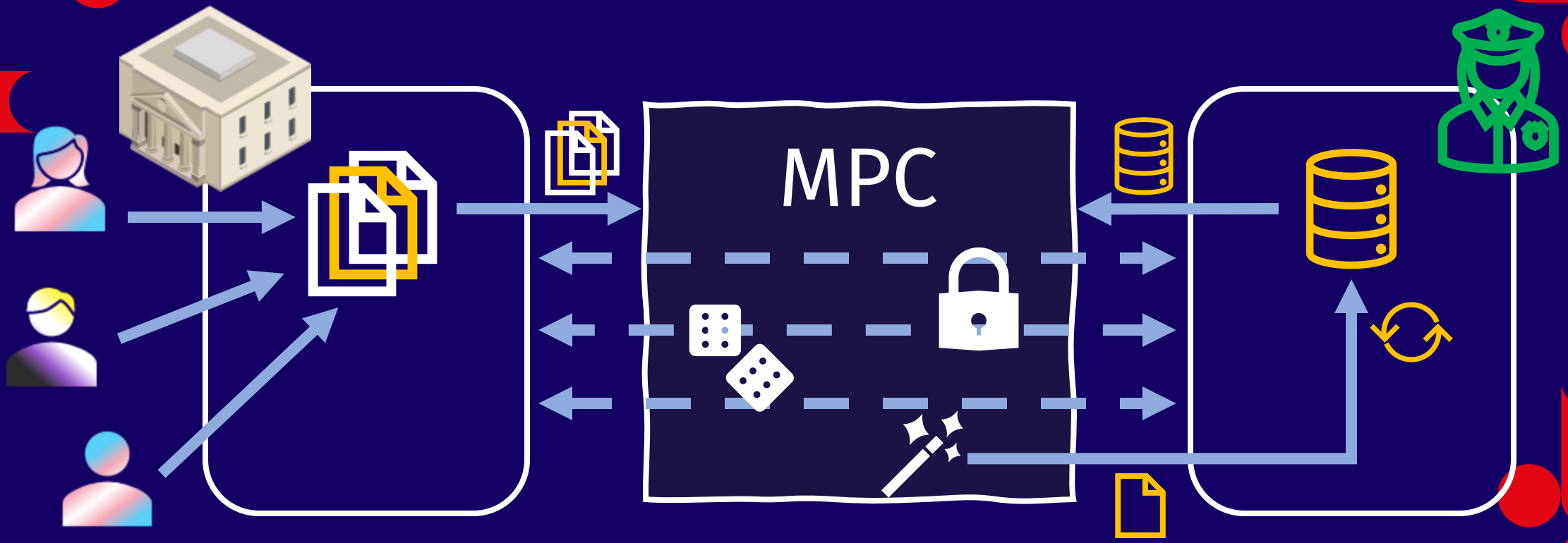
Umsetzung mittels MPC



Umsetzung mittels MPC



Umsetzung mittels MPC



Sicherheit von MPC

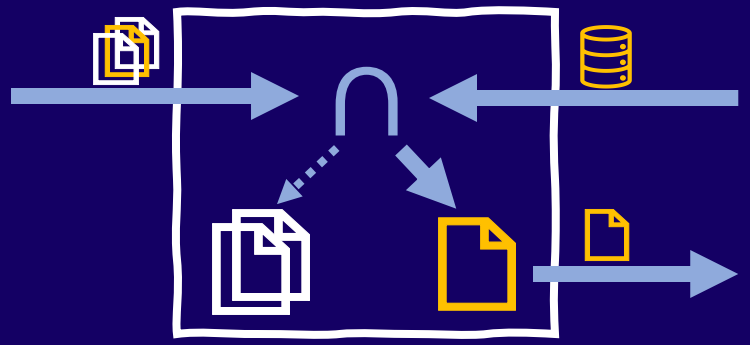
- Parteien kommunizieren untereinander
- Aus empfangenen Nachrichten ableitbare Informationen können bereits aus eigener Ein- und Ausgabe abgeleitet werden

Sicherheit von MPC

- Parteien kommunizieren untereinander
- Aus empfangenen Nachrichten ableitbare Informationen können bereits aus eigener Ein- und Ausgabe abgeleitet werden
- Formal **beweisbare Sicherheit** auf Basis etablierter kryptographischer Annahmen

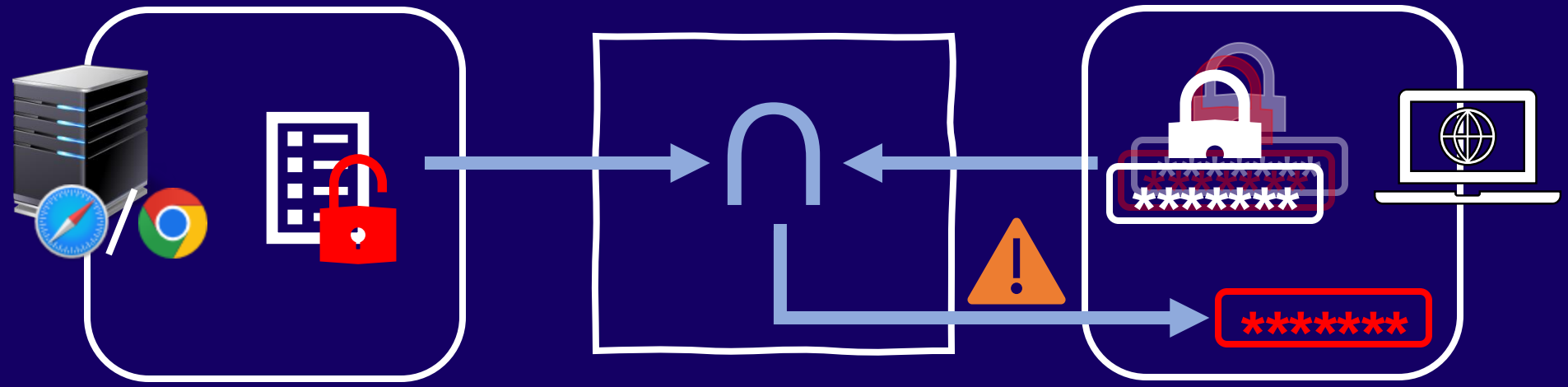
PSI: Private Set Intersection

- Spezialfall von MPC: Berechnung einer Schnittmenge
- Bereits auf Geräten von Endnutzer*innen im Einsatz:



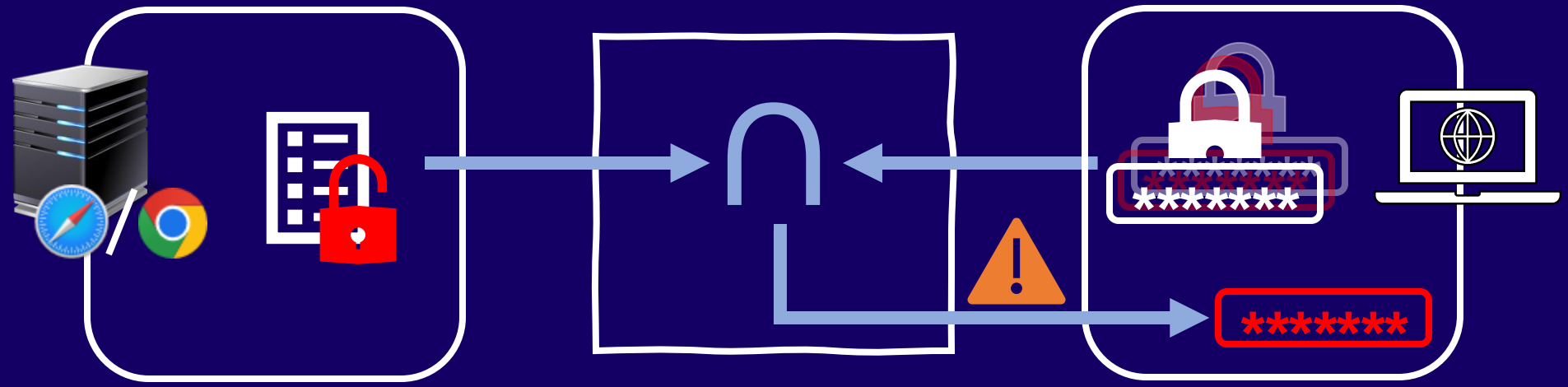
PSI: Private Set Intersection

- Spezialfall von MPC: Berechnung einer Schnittmenge
- Bereits auf Geräten von Endnutzer*innen im Einsatz:



PSI: Private Set Intersection

- Spezialfall von MPC: Berechnung einer Schnittmenge
- Bereits auf Geräten von Endnutzer*innen im Einsatz:



- Einfacher Austausch von Hash-Werten wäre unsicher!

PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

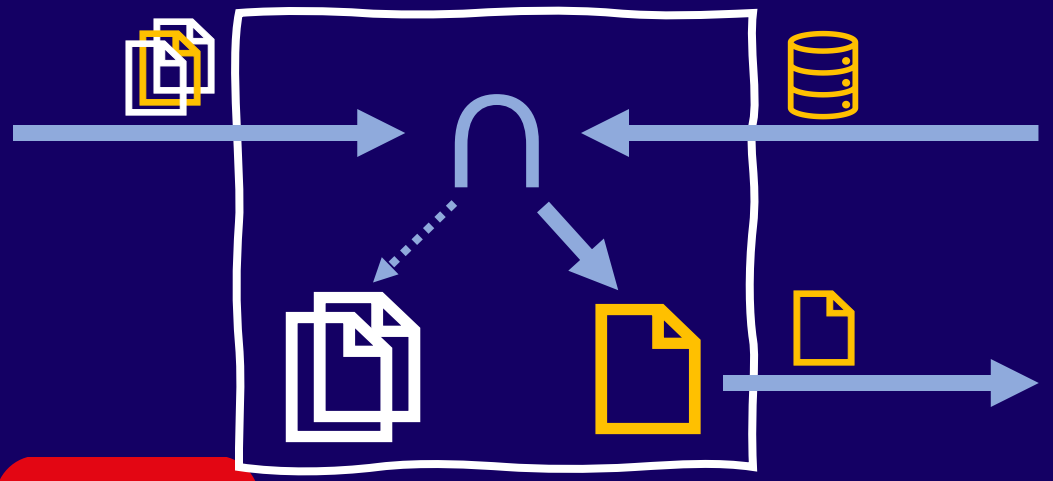
- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird

PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?

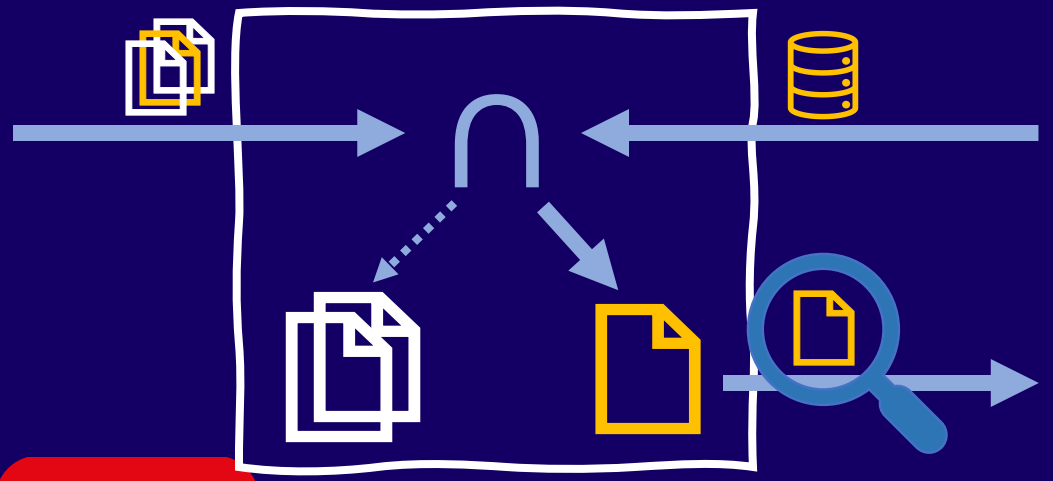
PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?



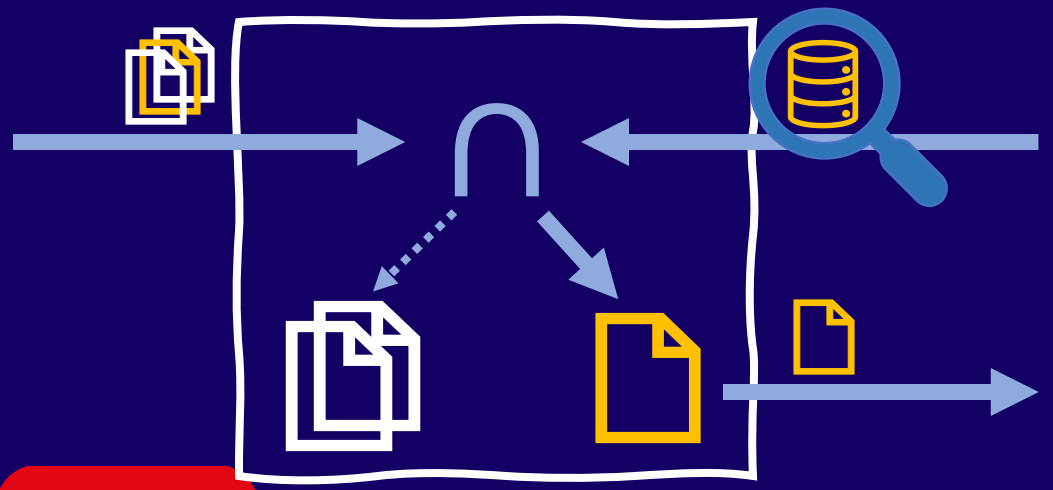
PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?



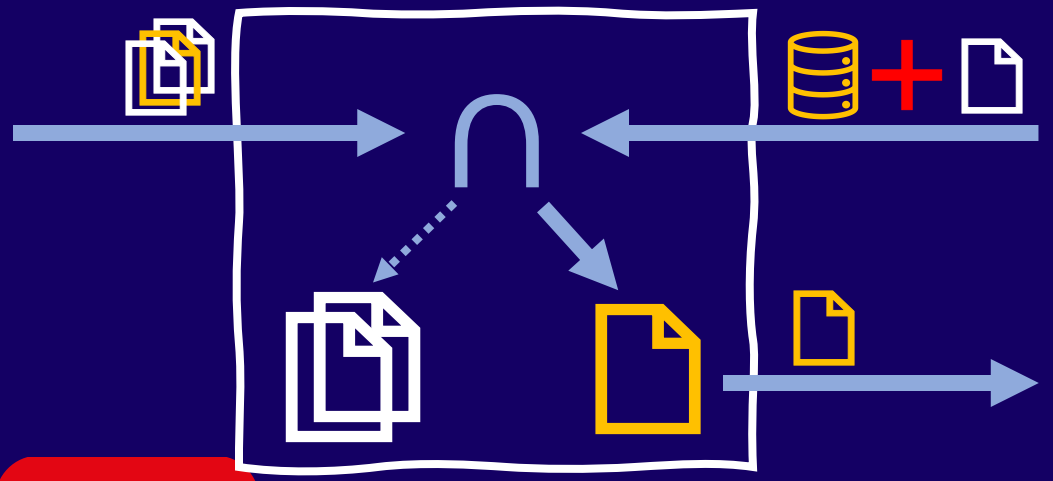
PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?



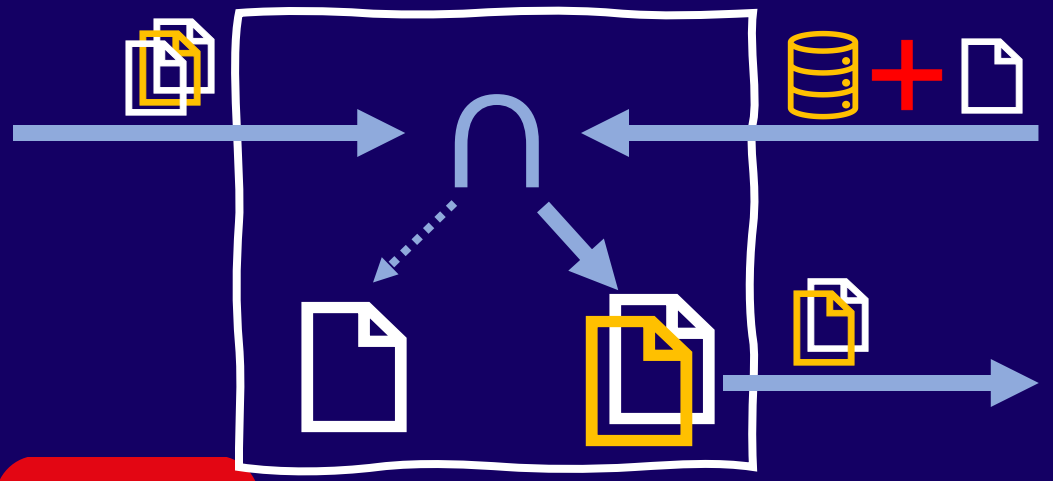
PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?



PSI zum behördlichen Datenabgleich
Grenzen der Sicherheitsgarantien

- MPC stellt sicher, dass die Funktionalität in einer Black-Box berechnet wird
- Aber was passiert außerhalb der Black-Box?
- Welche Risiken birgt die Funktionalität?



Fazit

- Trotz Streichung von § 13 Abs. 5 SBGG-RegE ist eine automatisierte Datenweitergabe an Sicherheitsbehörden nicht vom Tisch
- Rein (datenschutz)rechtlich besteht bei der gebotenen behördlichen Datenübermittlung zu Nachverfolgbarkeitszwecken ein Dilemma
- Diesem kann durch technologische Ansätze wie Multi-Party Computation entgegengesteuert werden
- Es verbleibt ein Restrisiko in Gestalt unredlichen Handelns von Einzelpersonen
- Es sind langfristig auch gesamtgesellschaftliche Maßnahmen (Aufklärung und Diskurs) auszuschöpfen, um Diskriminierung jeglicher Art nachhaltig entgegenzuwirken

Keine (sichtbaren) Daten ➔ Kein Datenmissbrauch

Linda Seyda

Andreas Brüggemann

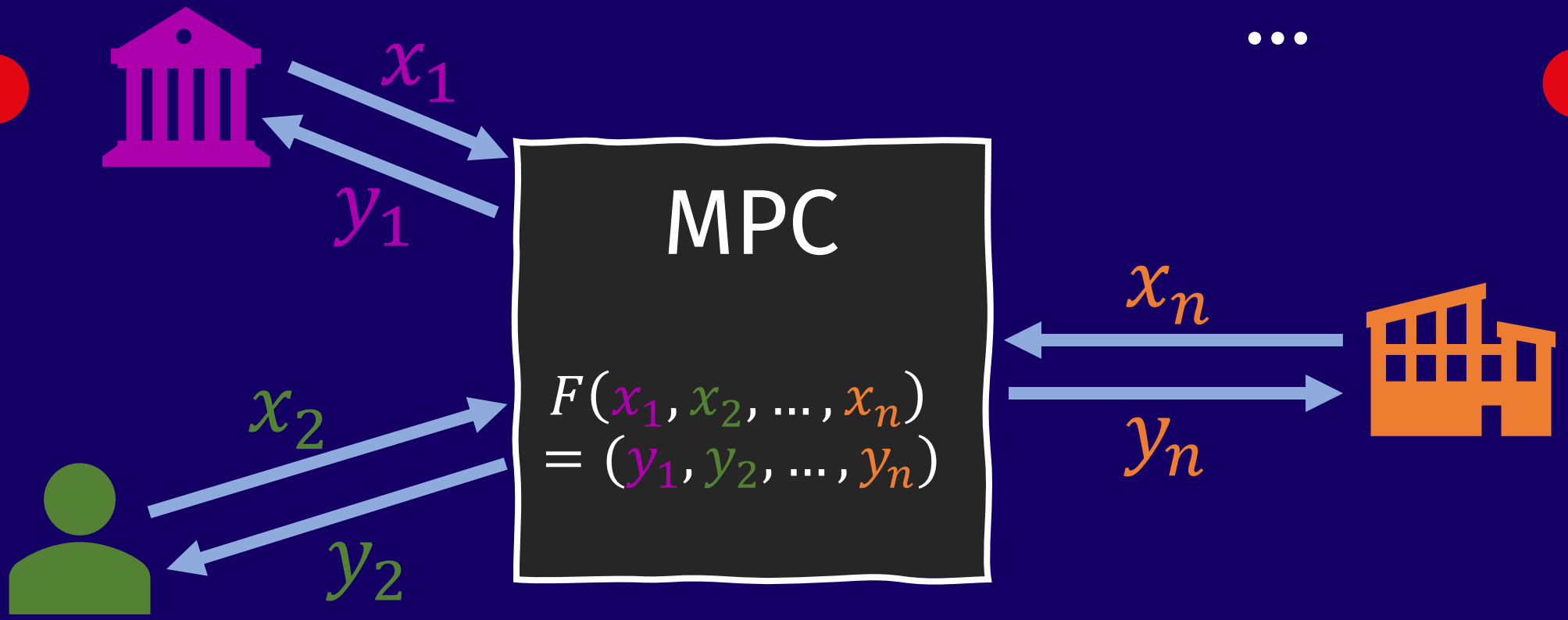
Privacy and Trust for Mobile Users

European Research Council
Established by the European Commission

DFG Deutsche Forschungsgemeinschaft
German Research Foundation

CROSSING

MPC im Allgemeinen



Informatik Festival 2024

PSI zum behördlichen Datenabgleich
Überlegungen und Limitierungen

- PSI/MPC ist teuer (Rechenkapazitäten, Kommunikation, Implementierung, …)
  - ➢ Jedoch bereits Abgleich von Millionen Einträgen innerhalb weniger Minuten möglich
- Ungenauigkeiten/Fehler in Daten
  - ➢ *Fuzzy* PSI

Robin A. Müller
=
Robin Mueller

- Fehler in Systemdesign / Sicherheitsbeweis / Implementierung können nie gänzlich ausgeschlossen werden