Polizeiliche Informationssysteme und der Datenschutz

Marit Hansen

Landesbeauftragte für Datenschutz
Schleswig-Holstein

BfDI-Symposium

Bonn, 6. Oktober 2021

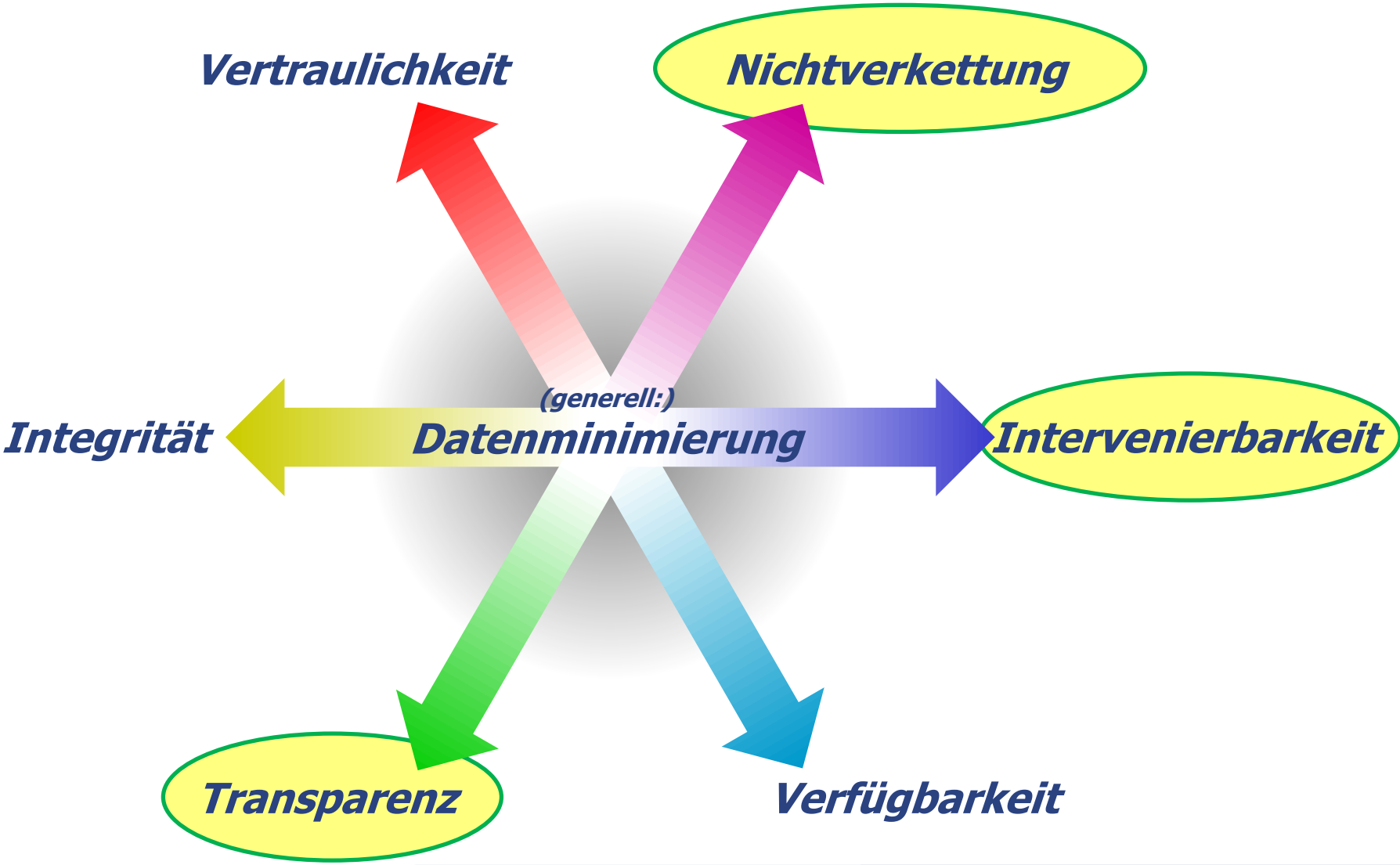
forum <privatheit>
selbstbestimmtes_leben_in_der_digitalen_welt

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Überblick

1. Datenschutz – wie geht‘s?
2. Polizei 2020
3. Trends 2021+
4. Herausforderung Kontrolle
5. Fazit

Gewährleistungsziele: Ja, auch für die JI-RL



JI-RL: EU-Richtlinie für den Bereich Justiz und Inneres

4.5.2016 DE Amtsblatt der Europäischen Union L 119/89

RICHTLINIEN

RICHTLINIE (EU) 2016/680 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 27. April 2016

zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

„Zwilling" der DSGVO

„Treu und Glauben“: Fairness

Art. 4 JI-RL: Grundsätze
[vgl. § 47 BDSG, s.a. Art. 5 DSGVO]

Artikel 4

Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

(1) Die Mitgliedstaaten sehen vor dass personenbezogene Daten

a) auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden,

Rechtmäßigkeit, Treu und Glauben (+Transparenz)

b) für festgelegte, eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden,

Zweckbindung

c) dem Verarbeitungszweck entsprechen, maßgeblich und in Bezug auf die Zwecke, für die sie verarbeitet werden, nicht übermäßig sind,

Datenminimierung

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sind; dabei sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden,

Richtigkeit

e) nicht länger, als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht,

Speicherbegrenzung

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen.

Informationssicherheit

Art. 20 JI-RL: Datenschutz by Design

[vgl. § 71 BDSG, s.a. Art. 25 DSGVO]

Eingebauter Datenschutz beginnend mit Konzeption der Verarbeitung

Artikel 20

Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

(1) Die Mitgliedstaaten sehen vor, dass der Verantwortliche unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung — trifft, die dafür ausgelegt sind, Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen dieser Richtlinie zu genügen und die Rechte der betroffenen Personen zu schützen.

(2) Die Mitgliedstaaten sehen vor, dass der Verantwortliche geeignete technische und organisatorische Maßnahmen trifft, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Überblick

1. Datenschutz – wie geht‘s?
2. Polizei 2020
3. Trends 2021+
4. Herausforderung Kontrolle
5. Fazit

Polizei 2020

Am 30. November 2016 verständigten sich die Innenminister des Bundes und der Länder im Rahmen ihrer Herbstkonferenz auf die Saarbrücker Agenda zur Informationsarchitektur der Polizeien des Bundes und der Länder als Teil der Inneren Sicherheit. Damit wurden die Weichen dafür gestellt, das Informationsmanagement grundlegend zu modernisieren und zu vereinheitlichen. Kernziele der Modernisierung sind:

- Verbesserung der **Verfügbarkeit** polizeilicher Informationen,
- Erhöhung der **Wirtschaftlichkeit**
- Stärkung des **Datenschutzes** durch Technik.

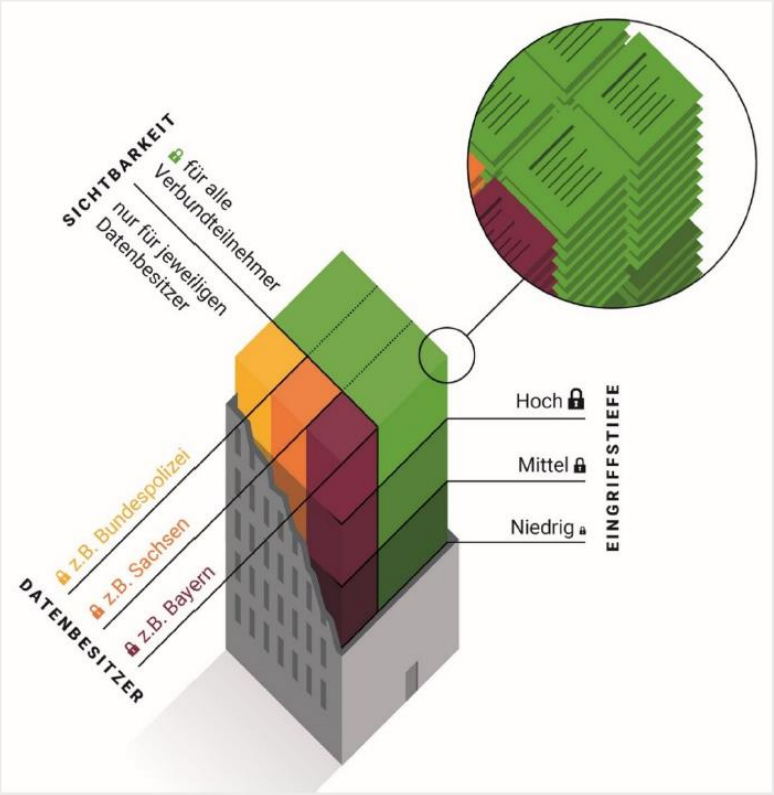
https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.html

Zentrale Speicherung, logische Mandantentrennung

- Data Warehouse-Konzepte sind nicht für perfekten Datenschutz bekannt
- „Agile Umsetzung" mglw. problematisch
- Risiken:
  - Aufweichung der Zweckbindung
  - Zentraler „Angriffspunkt"
  - Komplexität + Dynamik erschweren Kontrolle

Die folgende Abbildung skizziert die Grundzüge des geplanten Datenhauses des BKA.

Mandantenfähiges Datenhaus für die deutschen Polizeien



Im mandantenfähigen Datenhaus werden die Daten der einzelnen Polizeien des Bundes und der Länder zentral vorgehalten. Die Verantwortung für die Daten verbleibt beim jeweiligen Datenbesitzer. Während verbundrelevante Daten für alle Verbundteilnehmer sichtbar sind, sind Daten ohne Verbundrelevanz nur für den jeweiligen Datenbesitzer einsehbar. Darüber hinaus wird ein dynamisches Zugriffsmanagement implementiert, das die Eingriffstiefe des Datenzugriffs steuert und im Rahmen der gesetzlichen Schranken sicherstellt (Umsetzung des Grundsatzes der hypothetischen Datenneuerhebung).

Mit dieser Maßnahme wird das strategische Ziel „Stärkung des Datenschutzes durch Technik" erreicht.

Stärkung? Des Datenschutzes?

*Stärkung des **Datenschutzes** durch Technik*

Durch die Umsetzung des Programms Polizei 2020 wird der Datenschutz maßgeblich gestärkt. Mit der neuen Informationsarchitektur werden die Anforderungen aus dem Urteil des Bundesverfassungsgerichts vollumfänglich umgesetzt. Die Sicherheit der gespeicherten Daten hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit sowie Authentizität hat dabei höchste Priorität.

- Mit dem Programm Polizei 2020 wird ein verbesserter, intelligenter Datenschutz verwirklicht. Personenbezogene Daten werden nicht mehrfach in verschiedenen Dateien gespeichert, sondern nur einmal.
- Der Zugriff auf die Daten wird über dynamische und zielgerichtete Berechtigungskonzepte reglementiert, die weitaus differenzierter und grundrechtsschonender sind als die aktuellen Regelungen. Eine umfassende Protokollierung erfolgt lückenlos an zentraler Stelle.
- Damit wird ein modernes, differenziertes und dynamisches Zugriffsmanagement etabliert, was den Anforderungen an einen zielgerichteten und passgenauen Datenschutz entspricht. Daten werden zentral verwaltet und mit einer Kennzeichnung einer differenzierten, zweckgebundenen Verarbeitung zugänglich gemacht.
- Im Hinblick auf die IT-Sicherheit werden geeignete Schutzmaßnahmen in Anlehnung an die KRITIS-Kriterien (Empfehlungen für Betreiber Kritischer Infrastrukturen) des BSI definiert. Dabei wird die Konformität zu den Vorgaben des IT-Grundschutzes sichergestellt. Die aus der Zentralisierung resultierenden Anforderungen an die IT-Infrastruktur (sichere Netze, Verfügbarkeit, Performance) werden berücksichtigt.

Informationssicherheit: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität

Aber „Datenschutz durch Technikgestaltung“ bisher nicht überzeugend

Überblick

1. Datenschutz – wie geht‘s?
2. Polizei 2020
3. Trends 2021+
4. Herausforderung Kontrolle
5. Fazit

Trends für „Smart Policing"

- Daten, Daten, Daten
  - Mehr Quellen, z. B. über Dienstleister oder vernetzte Geräte in der Umgebung („Internet of Things")
  - Mehr Verknüpfungsmöglichkeiten
- Big-Data-Analysen und KI-Methoden
  - Biometrische Auswertungen
  - Emotionserkennung
  - Predictive Policing
- Community Involvement
- IT-Systeme ⇔ Entscheidungen

Risiko für die Rechte und Freiheiten natürlicher Personen

Bild: Wokandapix via Pixabay

Überblick

1. Datenschutz – wie geht's?
2. Polizei 2020
3. Trends 2021+
4. Herausforderung Prüfung
5. Fazit

Die typischen Korrektive im Datenschutz: funktionieren sie?

Die Rolle der polizeilichen Datenschutzbeauftragten

Erhöhter Schwierigkeitsgrad gegenüber anderen behördlichen DSB:

- wenige Personen
- sensible Daten
- interne Prüfungen würden als Misstrauen empfunden
- Kommunikation mit Aufsichtsbehörden tw. kritisch beäugt

- Beschwerden werden bearbeitet
- Doppelrolle DS-Operationalisierung

„Vertrauen" ist die falsche Kategorie

Herausforderung „Prüffähigkeit"

- Systemgestaltung, die eine Prüfung erlaubt oder sogar unterstützt, z. B.
  - mit Dokumentation, Datenschutz-Folgenabschätzung
  - mit Protokollierung
  - ggf. mit Quellcode

- Prüfteams mit ausreichender Expertise und ausreichenden Ressourcen

These: Ohne technische Prüftools werden viele künftige Kontrollen nicht (mehr) funktionieren.

Immer mehr gesetzliche Prüfpflichten der Aufsichtsbehörden als Ex-post-Kontrolle

Prüfpflichten

Gegenstand der Prüfung	Aufsichtsbehörde	Prüfturnus
Bundesgesetzliche Prüfpflichten		
Maßnahmen nach § 34, §§ 38 ff., § 64 BKAG u. Datenübermittlungen nach § 27 BKAG, Zugriffe auf INPOL nach § 15 BKAG	BfDI	alle 2 Jahre
Antiterrordatei (ATD)	jew. Aufsichtsbehörde	alle 2 Jahre
Rechtsextremismusdatei (RED)	jew. Aufsichtsbehörde	alle 2 Jahre
Verarbeitung d. Fluggastdaten/passenger name records (PNR)	BfDI	Muster alle 2 Jahre, im Übrigen regelmäßig (nicht ausdrücklich geregelt)
Prüfpflichten zu EU-Rechtsinstrumenten		
Schengener Informationssystem (SIS II)	jew. Aufsichtsbehörde	Datenverarbeitungsvorgänge im N.SIS II: alle 4 Jahre (BKA) im Übrigen (v.a. Datenabrufe u. -weiterverarbeitung): regelmäßig
Visa-Informationssystem (VIS)	jew. Aufsichtsbehörde	Datenverarbeitungsvorgänge im N-VIS: alle 4 Jahre (BVA), Abfragen der Sicherheitsbehörden nach VIS-Zugangsbeschluss alle 4 Jahre; im Übrigen: regelmäßig
European Dactyloscopy System (Eurodac)	jew. Aufsichtsbehörde	jährlich
Europäisches Strafregisterinformationssystem (ECRIS)	BfDI (§ 9 Abs. 1 BDSG)	regelmäßig (nicht ausdrücklich geregelt)
ECRIS-TCN	BfDI (§ 9 Abs. 1 BDSG)	Datenverarbeitungsvorgänge in den nationalen Strafregister- u. Fingerabdruck-Datenbanken: alle 4 Jahre; im Übrigen: regelmäßig
Einreise-/ Ausreisesystem (Entry-/Exit-System – EES)	jew. Aufsichtsbehörde	Datenverarbeitungsvorgänge in d. nat. Grenzinfrastruktur: alle 3 Jahre (Zentralbehörde i.S.d. Art. 39 Abs. 1 VO); im Übrigen: regelmäßig
Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)	BfDI (§ 9 Abs. 1 BDSG)	alle 3 Jahre
Interoperabilität zw. EU-Informationssystemen: - Grenzen und Visa - pol. und justiz. Zsarbeit, Asyl und Migration)	jew. Aufsichtsbehörde	Überprüfung d. CIR-Zugangsprotokolle: alle 6 Monate Datenverarbeitungsvorgänge d. nat. Behörden: alle 4 Jahre jährliche Veröffentlichung der Anzahl von Anträgen auf Wahrnehmung der Betroffenenrechte durch die Aufsichtsbehörde
Prümer Vertrag – Austausch v. Fingerabdruck-, DNA- und Kfz-Daten	BfDI (§ 7 PrümVtrAG)	regelmäßig (nicht ausdrücklich geregelt)
Landesrechtliche Prüfpflichten S-H		
- Verdeckte Maßnahmen - Übermittlungen an Drittstaaten	LfD SH	mind. alle 2 Jahre stichprobenartige Überprüfungen

Prüfungen von Verbundsystemen: Koordinierung nötig

Teilansicht der Bund-Länder-Koordinierung

Bild: Gerd Altmann via Pixabay // Logos

Überblick

 Bild: athree23 via Pixabay

1. Datenschutz – wie geht's?
2. Polizei 2020
3. Trends 2021+
4. Herausforderung Kontrolle
5. Fazit

Konzept „Kontrolle" nötig

- In Polizei 2020 Datenschutz einbauen;
  aus dem Tätigkeitsbericht des BfDI 2020:

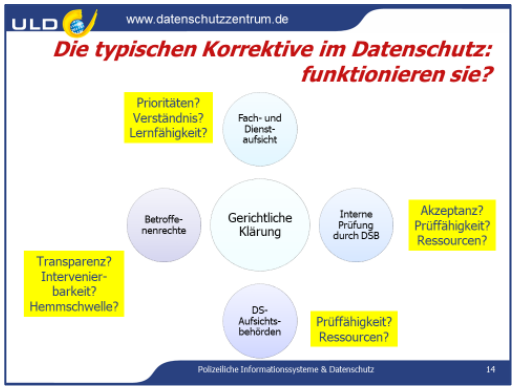
> Mit dem Programm Polizei 2020 besteht die Chance, neue technische Grundfunktionalitäten des Datenschutzes als „Basisdienste" zu implementieren. Notwendig sind z. B. ein „Basisdienst Zwecktrennung", ein „Basisdienst Datenqualität" und ein „Basisdienst Aufsicht und Kontrolle", der insbesondere Protokollierungsdienste enthält.

Man mag dies erweitern:
Basisdienste für Nichtverkettung, Transparenz, Intervenierbarkeit

- Das funktioniert nicht allein mit Technik!

Gesamtkonzept „Kontrolle" nötig

- Ex-post-Kontrolle mit Mini-Teams der DS-Aufsicht reicht nicht.
- Eigenkontrolle des Verantwortlichen:
  - Polizeiliche DSB stärken
  - (Stichproben-)Prüfung als Normalfall etablieren
  - Konstruktive Fehlerkultur entwickeln
  - Lernen



- Datenschutz und geeignete Prüfmöglichkeiten implementieren
- Transparenz (und Intervenierbarkeit) für die betroffenen Personen, z. B. Kontrollquittungen*), Funkzellen-Transparenz-System**) – Offenheit für Rechtewahrnehmung, gesellschaftlicher Diskurs

*) Aden, BT-Ausschuss für Inneres und Heimat, Ausschussdrs. 19(4)863 B, 05.06.2021
**) https://fts.berlin.de/

Kontrolle als Chance (nicht nur rechtsstaatliche Notwendigkeit)