DSRI Deutsche Stiftung für Recht und Informatik

Die Verknüpfung von Datenbanken

Eine Analyse aus datenschutzrechtlicher Sicht

Institut für Rechtsinformatik, Hannover
Delventhal, Gerjets, Korte, Schlee und Stoklas

Herbstakademie 2020

www.dsri.de

Übersicht

- EU-Sicherheitspolitik: Der Informationsaustausch und die Verknüpfung von EU-Informationssystemen
- Der Informationsaustausch und die Verknüpfung von behördlichen Datenbanken auf nationaler Ebene
- Interoperabilität von Datenbanken und vergleichbaren Systemen im privatwirtschaftlichen Bereich

Verknüpfung von Datenbanken – erhöhtes Risiko oder notwendige Maßnahme?

- Interoperabilität – Fähigkeit zur Zusammenarbeit
- Grundsätze der Datenverarbeitung
  - Erheblich erweiterter Pool von Daten
  - Unterschiedliche Verantwortliche und eine hohe Anzahl von Nutzenden
  - IT-Sicherheit, Kontrollmechanismen und effektiver Rechtsschutz
- Steigerung des Risikos nicht nur durch höhere Datenmenge
  - Analyse durch effizientere Software (vgl. Hessendata = Palantir)
  - Hoher Detailgrad der Daten (Profiling?)

Problematik: Stehen Risiken und Zwecke im Ausgleich und sind die getroffenen risikomindernden Maßnahmen ausreichend?

EU-Sicherheitspolitik: Der Informationsaustausch und die Verknüpfung von EU-Informationssystemen

EU-Sicherheitspolitik: Der Informationsaustausch und die Verknüpfung von EU-Informationssystemen

- Verordnungen (EU) 2019/817 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen **Grenzen und Visa**
- Verordnung (EU) 2019/818 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen **(polizeiliche und justizielle Zusammenarbeit, Asyl und Migration)**

EES, VIS, ETIAS, SIS

Eurodac, SIS, ECRIS-TCN, EUROPOL

→ Inhaltlich weitestgehend gleich

Komponenten der Interoperabilitäts-VOen

- Europäisches Suchportal (ESP)
  - Einheitliche Suchmaske für verschiedene Datenbanken:
    - EES, VIS, ETIAS, Eurodac, SIS, ECRIS-TCN, Europol- und Interpol-Datenbanken
  - „rascher, unterbrechungsfreier, effizienter, systematischer und kontrollierter Zugang“
- Gemeinsamer Dienst für den Abgleich biometrischer Daten (BMS)
  - Abgleich biometrischer Templates über verschiedene Systeme hinweg
  - Soll insbesondere CIR und SIS stärken
  - Ersetzt entsprechende Funktionalitäten in EES, VIS, SIS, EURODAC sowie ECRIS-TCN

Komponenten der Interoperabilitäts-VOen

- Gemeinsames Identitätsregister (CIR)
  - Individuelle Datei für jede in EES, VIS, ETIAS, Eurodac oder ECRIS-TCN erfasste Person
    - Ersetzt insoweit entsprechende Funktionalitäten in den genannten Systemen
  - Enthält einen Detektor für Mehrfachidentitäten (MID), um diese innerhalb der Datenbanken der EU-Systeme aufzuspüren

Datenschutzrechtliche Implikationen / Zusammenfassung

- Zweckbindung: (P)?
  - Zwecke der Interoperabilitäts-VO sind mit denen der ursprünglichen Rechtsgrundlagen kompatibel
  - Wenn sich ein Verantwortlicher darauf berufen kann, dann erst recht der Gesetzgeber
- Protokollierungspflicht für Abfragen; erweiterte Pflicht für Abfragen im CIR
- Anforderungen an Datenqualität
- Regelmäßige Evaluation der Systeme, statistische Auswertungen
- Verfahren für Betroffenenrechte (z.B. Informationsportal)
- Aber: Allgemeine Verhältnismäßigkeit?

Der Informationsaustausch und die Verknüpfung von behördlichen Datenbanken auf nationaler Ebene

Der Informationsaustausch und die Verknüpfung von behördlichen Datenbanken auf nationaler Ebene

- Polizeiliches Informationsystem, „INPOL“
  - länderübergreifende Verbunddatei, betrieben vom BKA
  - Personen- und Sachfahndungsdateien, Haftdateien, Kriminalaktennachweisen, DNA-Analyse-Dateien sowie Dateien, die erkennungsdienstliche Daten beinhalten
  - Zugriff u.a. durch BKA, Bundespolizei, Landespolizeidienst-stellen, Zollbehörden
  - Daten werden z.B. von den jeweiligen Stellen in eigener Verantwortlichkeit dezentral erhoben und in das Verbundsystem eingespeist
  - Reform: „Polizei 2020“
- Ausländerzentralregister
  - 26 Mio. personenbezogene Datensätze zu 10,6 Mio. Menschen
  - dient mehr als 14.000 Behörden und Organisationen als Informationsquelle

Datenschutzrechtliche Implikationen

- Grundsätze der Datenverarbeitung:
  - INPOL:
    - Zweckbindung: Erhebung der Daten zu repressiven Zwecken, Weiterverarbeitung z.T. zu präventiven Zwecken
    - Polizei 2020:
      - privacy by design-Ansatz bei Berechtigungskompetenzen und Protokollierung
      - Optimierung der „Datenhaltung“ im Verbundsystem
      - Datenminimierung, Richtigkeit und Integrität

Datenschutzrechtliche Implikationen

- AZR:
  - Zweckbindungsgrundsatz: erweiterte Zugriffsmöglichkeiten durch verschiedenste Stellen
  - Datenqualität und Monitoring-Mechanismen: Vergleich zu den Interoperabilitäts-VOen zeigt Handlungsbedarf auf
    - Kontrollmechanismen durch Aufsichtsbehörden nicht deutlich

Zusammenfassung

- Grundsätze der Datenverarbeitung
  - Zweckbindung
  - P: Transparenz hinsichtlich der Löschfristen
- Datenqualität
- Kontrollmechanismen der Aufsichtsbehörden

Interoperabilität von Datenbanken und vergleichbaren Systemen im privatwirtschaftlichen Bereich

Datenschutzrechtliche Anforderungen an Geschäftsmodelle mit der Verknüpfung von Datenbanken de lege lata

- Rechtsgrundlagen für Interoperabilität
  - Das Herstellen von Interoperabilität fällt unter Art. 4 Nr. 2 DSGVO
  - Dementsprechend muss eine Rechtsgrundlage für die Verarbeitung vorliegen
    - Da Verknüpfungsprozesse nicht immer vorhersehbar sind, bietet sich dafür vor allem das berechtigte Interesse nach Art. 6 Abs. 1 lit. f DSGVO an
    - Es muss also ein berechtigtes Interesse vorliegen und die Interessen der betroffenen Person darf nicht überwiegen
    - Sollte mit der Verarbeitung eine Änderung des Zwecks einhergehen, ist auch Art. 6 Abs. 4 zu beachten

Interoperabilität als Betroffenenrecht

- Interoperabilität als Konzept findet in der DSGVO vor allem im Rahmen des Betroffenenrechts „Datenportabilität“ in Art. 20 DSGVO Erwähnung
- Sind die Voraussetzugen des Art. 20 DSGVO gegeben, müssen die Daten unter anderem in einem „interoperablen“ Format zur Verfügung gestellt werden
  - Es geht also weniger um Interoperabilität ganzer Datenbanken, sondern um die „Weiterbenutzbarkeit“ von Daten
  - Es soll an dieser Stelle wettbewerbs-und datenschutzfördernd wirken; bei der Verknüpfung von Datenbanken wirkt Interoperabilität dagegen regelmäßig datenschutzgefährdend
- Eine Rolle spielt hier auch Art. 20 Abs. 2 DSGVO: die direkte Übermittlung von Daten könnte die Interoperabilität von Systemen erhöhen und damit möglicherweise datenschutzgefährdend wirken

Die Verknüpfung von Datenbanken und Interoperabilität im Anwendungsfall

- **Tracing-Apps**
  - entwickelt zur Eindämmung der Covid-19-Pandemie
  - Entwicklung und Betrieb durch staatliche Institutionen – Einwilligung zur Verarbeitung personenbezogener Daten beim Nutzer
    - Parallele zu privatwirtschaftlichen Geschäftsmodellen
  - Europäischer Datenschutzausschuss (EDSA): Anregung zur Schaffung eines interoperablen Rahmens (z.B. zur Benachrichtigung von Reisenden):
    - Datenschutzkonforme Verarbeitung lediglich einer Mindestmenge an Informationen
    - Steigerung der Effektivität der Anwendungen
    - Trotz technischer Herausforderungen und ggf. Einholung zusätzlicher Einwilligung:
      - Berücksichtigung aller Voraussetzungen zur Stärkung des Vertrauens und für erhöhte Nutzungsbereitschaft

Die Verknüpfung von Datenbanken und Interoperabilität im Anwendungsfall

Telematik-Tarife in der KFZ-Versicherung

- Derzeit Umsetzung mit durch den Versicherer bereitgestellten Sensoren zur Analyse des Fahrverhaltens
  - zukünftig Transfer von Daten durch Vernetzung (Forschungsprojekte CampaNEO und SmashHit)
- Datenschutzrechtliche Einordnung teilweise schwierig:
  - Vielzahl an Automobilherstellern und Versicherern sowie Plattformen und technische Dienstleister
  - ggf. gemeinsame Verantwortlichkeit (Art. 26 DSGVO) und Auftragsverarbeiter (Art. 28 DSGVO)
  - Feststellung der Verantwortlichkeit insbesondere für Betroffenenrechte der Person (Art. 12 ff. DSGVO) bedeutsam
    - Klare Zuteilung von Verantwortlichkeit und Haftung bei Zusammenführung von Datenbanken notwendig (z.B. durch Vereinbarung gem. Art. 26 DSGVO)
  - Rechtsgrundlage insbesondere Art. 6 Abs. 1 lit. b) DSGVO

Zusammenfassung

- Das Herstellen von Interoperabilität stellt datenschutzrechtlich prinzipiell eine “normale Datenverarbeitung“ dar
- Konkreter Mehrwert durch Interoperabilität in Anwendungsfällen
- Gleichwohl müssen relevante Fragen z.B. hinsichtlich der Verantwortlichkeit der Verarbeitung und der Betroffenenrechte vorab geklärt werden
- Langfristig bereichsspezifische Regelungen zur Beseitigung von Rechtsunsicherheit und Förderung der Verknüpfung von IT-Systemen denkbar
- Implementierung von Sicherheiten wie einer verpflichtenden Datenschutz-Folgenabschätzung i.S.d. Art. 35 DSGVO zugunsten der Betroffenen

Fazit

- Die Vernetzung bzw. Interoperabilität führt zu komplexen Datenverarbeitungsvorgängen und Datenflüssen
- Die Qualität des Eingriffes in die Grundrechte wird dadurch nicht nur unerheblich gesteigert
- Grundsätze der Datenverarbeitung werden nicht gewahrt und auch die Verhältnismäßigkeit fehlt teilweise
- Rechtedurchsetzung ist für den einzelnen Betroffenen schwer
- Zwecke können legitim sein, aber bedürfen ausreichender Maßnahmen, um die Rechte und Freiheiten des Einzelnen zu wahren.

Korrekturhinweis:
FN 45: Statt „Ebd.“ müsste es richtigerweise „Kehr, Datei Gewalttäter Sport, S. 32“ heißen.