UNIKASSEL
VERSITÄT

ITeG
Wissenschaftliches Zentrum für Informationstechnik-Gestaltung

provet
Projektgruppe verfassungsverträgliche Technikgestaltung

Datenanalysesysteme bei der Polizei im Lichte des neuen Datenschutzrechts

Forum Privatheit
Die Fortentwicklung des Datenschutzes

3. November 2017

Inhalt

Aufgaben der Polizei und unterstützende IT-Anwendungen

Aufgabenbereich	Ziel der Anwendung
• Strafverfolgung	• frei verfügbare Daten
• Gefahrenabwehr	• eigene Daten
• Doppelfunktionale Maßnahmen	• Daten im Besitz
• Prävention	• Daten bei dritten Stellen, die nicht frei verfügbar sind

Datenanalyse

Daten pflegen und prüfen

- z.B. Abfrage, um aus unvollständigen Daten (Datenfragmenten) z.B. brauchbare Kontaktdaten von Verdächtigen, Organisationen, Geschädigten und Zeugen (VOGZ) zu ermitteln.
- z.B. Abfragen, um Aussagen und Sachverhaltsdarstellungen überprüfen zu können.

Hintergründe ermitteln

- z.B. Abfrage um den Background von VOGZ zu ermitteln, z.B. um Aussagen bewerten zu können, Vernehmungen vorzubereiten, Motive zu erkennen.

Verbindungen erkennen

- z.B. Abfrage um Beziehungen und Verbindungen zwischen VOGZ untereinander und mit Produkten aufdecken zu können.

Beispiel 1: Linked Data Kriminalitätsanalyse

LiDaKrA
BMBF-Forschungsprogramm
„Schutz vor organisierter Kriminalität“

GEFÖRDERT VOM
Bundesministerium
für Bildung
und Forschung

Heute (Funktionsumfang I)

- Sammlung und Organisation großer, unsortierter Datenmengen
- Durchsuchung offener Internetquellen (Common web, Darknet)
- gleichzeitige Abfrage/Suche mehrerer offener Datenquellen
- Linking und Fusionierung von Suchergebnissen

Geplant (Funktionsumfang II)

- Erweiterte Analyse
- Einbindungsmöglichkeit auch anderer Quellen
- Extraktion von PIOS Entitäten
- Ranking der Ergebnisse
- Daten-Integration und Kriminalitätsanalyse (Hinweisgeber)

provet
UNIKASSEL
VERSITÄT

Beispiel 2: MUSKAT – Multisensoriell gestützte Erfassung von Straftätern in Menschenmengen bei komplexen Einsatzlagen

Muskat

- Sicherheit in komplexen Einsatzlagen erhöhen
  - Szenario: Fußball-Risikospiele
- Erforschung eines modularen und autarken Kommunikations- und Sensorsystems
  - Entscheidungsunterstützungssystem (Decision Support System)
  - Verbesserte Kommunikation zwischen den Einsatzkräften
  - Hochwertige und Lückenlose Beweissicherung
  - Optisch visuelle Verfolgung

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

provet

UNIKASSEL VERSITÄT

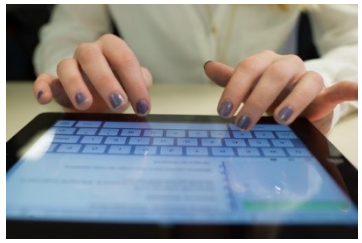
Schutz des Privaten und Datenschutz

- Das Grundrecht auf informationelle Selbstbestimmung (Art. 2 I iVm Art. 1 I GG) gewährleistet „die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen“, BVerfGE 65,1.
- Durch die europ. Charta der Grundrechte ebenfalls Privatheit und personenbezogene Daten geschützt, siehe Art. 7 und 8 GrC.
- Der Staat hat nicht das Recht, den Menschen zwangsweise in seiner gesamten Persönlichkeit zu registrieren. Profilbildung soll verhindert werden.
- Geschützt ist jede Form der Erhebung, Kenntnisnahme, Speicherung, Verwendung, Weitergabe oder Veröffentlichung von personenbezogenen Daten.
- Jeder Datenumgang (Erheben, Speichern, Verändern, Übermitteln) braucht Ermächtigung oder Einwilligung.

.

Grundrechtsbetroffenheit und Bedeutung

- Ein Eingriff in Grundrechte ist auch anzunehmen, wenn die aus öffentlich zugänglichen Quellen stammende Daten durch ihre systematische Erfassung, Sammlung und Verarbeitung einen zusätzlichen Aussagewert erhalten
- Dies ist der Fall, wenn diese Daten mit anderen Daten verbunden werden und dadurch der Aussagegehalt der verknüpften Daten insgesamt zunimmt. (Rspr. BVerfG).
- Rechtlich ist nicht alles zulässig und rechtspolitisch nicht alles wünschenswert, was technisch machbar wäre.
- Rechtsstaatliche Begrenzungen führen hierbei zwangsläufig zu Beschränkungen und Mehraufwand – das ist gerade ihr Sinn.
- Für eine wirksame rechtliche Eingrenzung einschlägiger Strafverfolgungsmaßnahmen müssen bestehende Befugnisse stets restriktiv ausgelegt werden zur.

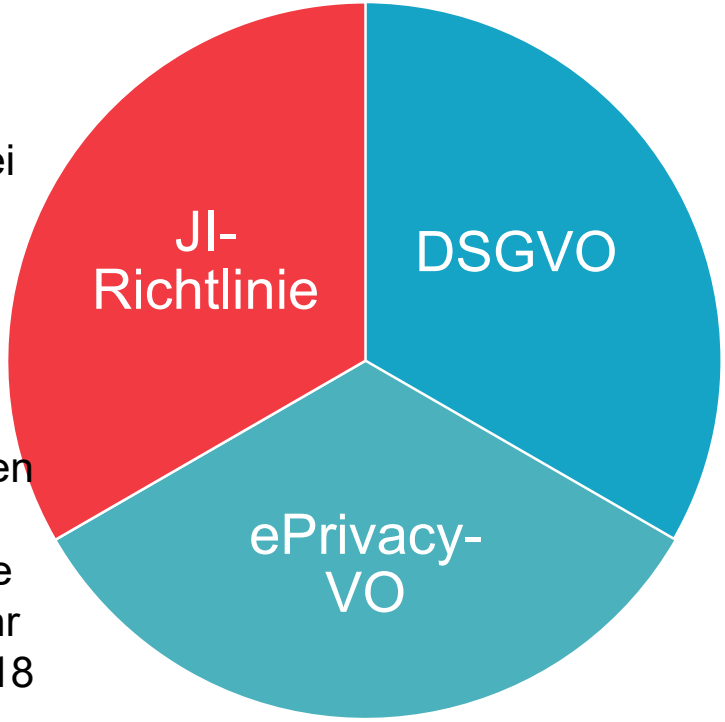


Universität Kassel / Studio Blofield

Novellierung des europäischen Rechtsrahmens

JI-Richtlinie

- (EU 2016/680)
- Richtlinie zum Schutz natürlicher Personen bei Verarbeitung personenbezogener Daten zum Zwecke der Verhütung Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr
- soll bis zum 06. Mai 2018 in nationales Recht umgesetzt werden.



Datenschutz-Grundverordnung

- (EU 2016/679)
- direkt anwendbar ab 25. Mai 2018

ePrivacy-Verordnung

- (EU 2017/???)
- soll direkt anwendbar ab 25. Mai 2018 sein.

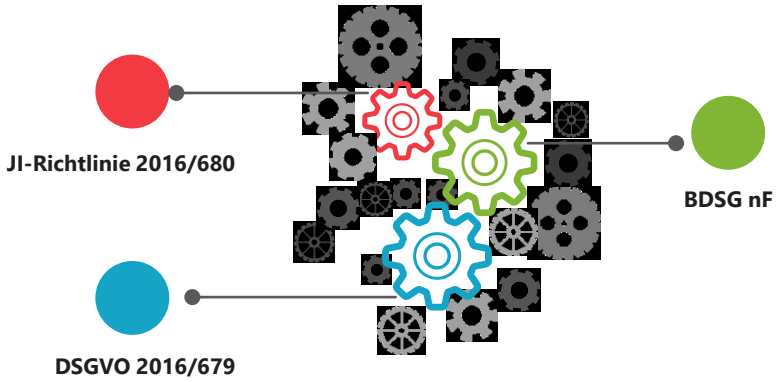
provet
UNIKASSEL VERSITÄT

Ko-Regulierung im Datenschutzrecht

JI-Richtlinie 2016/680
Ist in deutsches Recht umzusetzen.

BDSG nF
Enthält im dritten Teil die Umsetung der JI-RL für den Bund.

Datenschutz-Grundverordnung
Wird direkt anwendbar sein. Gilt nicht für den Anwednunsgbereich der JI-RL.



Teil 3 des neuen Bundesdatenschutzgesetzes

- Teil 3 BDSG nF setzt JI-Richtlinie auf Bundesebene um.
- JI-Richtlinie wird auch in bereichsspezifischen Gesetzen umgesetzt werden (zB. BKAG, BPolG).
- Umsetzung in den Ländern steht aus, zu erwarten ist das BDSG nF **Vorbildfunktion** haben wird.
- Anwendungsbereich nach § 45 BDSG nF Verarbeitungen zu Strafverfolgung, Gefahrenabwehr und Ordnungswidrigkeiten.
- Geregelt wird das „wie“ der Verarbeitung, das „ob“ bleibt spezialgesetzlichen oder bereichsspezifischen Regelungen vorbehalten.
- Ausnahmen: Einwilligung, Weiterverarbeitung.

Teil 3 des neuen Bundesdatenschutzgesetzes

- Anwendungsbereich, Begriffsbestimmungen (§§ 45 und 46 BDSG nF).
- Aussagen zu Rechtsgrundlagen der Verarbeitung, Zweckbindung und -änderung (§§ 47 bis 51 BDSG),
- Ausformungen der Betroffenenrechte (§§ 55 bis 61 BDSG),
- Festlegung unterschiedlich akzentuierter Pflichten der Verantwortlichen
  - Anforderungen an Auftragsverarbeitungsverhältnisse (§ 62 BDSG),
  - Datensicherheit und Meldungen von Verletzungen des Schutzes personenbezogener Daten (§§ 64 bis 66 BDSG),
  - Instrumente zur Berücksichtigung des Datenschutzes (Datenschutz-Folgenabschätzung, Anhörung der oder des Bundesbeauftragten, Verzeichnis von Verarbeitungstätigkeiten, Protokollierung, §§ 67 bis 70 und 76 BDSG),
  - Berichtigungs- und Löschungspflichten (§ 75 BDSG);
- Datenübermittlungen an Stellen in Drittstaaten und an internationale Organisationen (§§ 78 bis 81 BDSG).

Automatisierte Einzelentscheidungen

- Vorgaben zu automatisierten Einzelentscheidungen und Profilingverbot in § 54 BDSG nF.
- Setzt Art. 11 JI-Richtlinie um.
- Automatisierte Einzelentscheidungen mit nachteiligen Rechtsfolgen sind idR Rechtsakte mit Auswirkung.
- Erhebliche Beeinträchtigungen können auch interne Zwischenfestlegungen oder –auswertungen sein, die Ausflüsse automatisierter Prozesse sind.
- Polizeiliche Generalklauseln dürften in der Regel nicht als Ermächtigungsgrundlage ausreichen.
- Für die Verarbeitung von Daten besonderer Kategorien ist dies in §54 Abs. 2 BDSG nF ausdrücklich klargestellt.

Bedingtes Profilingverbot

- Profilbildung erfolgt, um bestimmte Verhaltensweisen zu analysieren oder vorherzusagen.
- Der Begriff „Profiling“ ist methodenoffen und trifft sehr unterschiedliche Formen der Datenauswertung.
- Profiling definiert in § 46 Nr. 4 BDSG nF. Entspricht Definition in Art. Art. 3 Nr. 4 JI-RL und Art. 4 Nr. 4 DSGVO.
- Ausdrücklich Verboten ist nur das Profiling aufgrund von besonderen Kategorien personenbezogener Daten.
- rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung.
- Unbestimmter Rechtsbegriff „diskriminiert“.
- Ausdrücklich gilt dieses Verbot nur im Zusammenhang mit automatisierten Einzelentscheidungen.

Zusammenfassung

- Die europäische Neuordnung des Datenschutzrechts reicht in die Datenverarbeitung bei Polizeien und Strafverfolgungsbehörden.
- Sie fordert Anpassungen sowohl im Datenschutzrecht als auch im Sicherheits- und Ordnungsrecht und dem Strafprozessrecht.
- Gesetze in diesem Anwendungsfeld sind zukünftig auch an den europäischen Grundrechten zu messen.
- Erforderlich ist bspw. größere Genauigkeit hinsichtlich Normenklarheit (BVerfG) und Anlassbezogenheit (EuGH).
- Der Einsatz neuer Datenanalyse und Entscheidungsunterstützungssystem muss gerechtfertigt sein und rechtsverträglich ausgestaltet werden.
- Aller diesbezüglichen staatlichen Maßnahmen und Möglichkeiten sind in der Überwachungsgesamtrechnung beachtenswert.

Universität Kassel / Studio Blofield

Quellen

Johannes, P.C. / Weinhold, R., Das neue Datenschutzrecht bei Polizei und Justiz, Nomos-Verlag, Baden-Baden - *in Vorbereitung für Dezember 2017.*

Roßnagel, A. (Hrsg.), Das neuen Datenschutzrecht, Nomos-Verlag, Baden-Baden – *erscheint Dezember 2017.*

Kochheim, D., Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, C.H. Beck, 2015.

Krause, B., „Retrograde“ Auskunftsverlangen der Strafverfolgungsbehörden an Postdienstleister, NZWiSt 2017, 60.

Decker, C., Muskat – nicht nur ein Gewürz, Bundespolizei kompakt, 3-2015, 29.

Richter, P., Weinhold, R., Krüger, M., Geske, K., Von Kameras und Verdrängung: Rechtliche Anknüpfungspunkte für ein Recht auf Stadt unter besonderer Diskussion der Videoüberwachung öffentlicher Räume, Kritische Justiz 2016, 30

provet
UNIKASSEL VERSITÄT

Thank You!

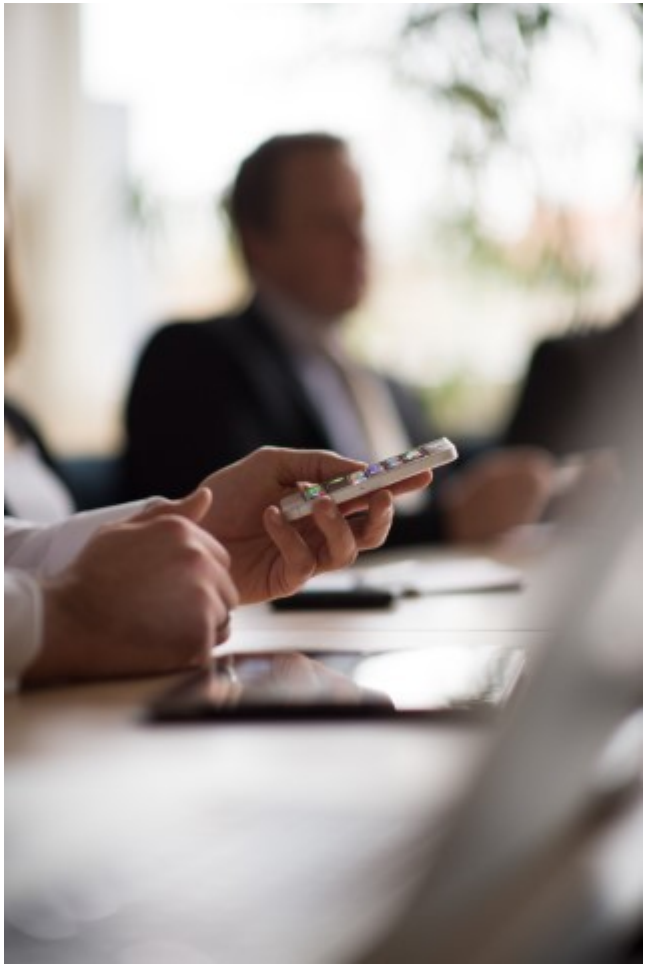
Questions? Feel free to contact me!

Paul C. Johannes, LL.M.
Rechtsanwalt

Universität Kassel
Wissenschaftliches Zentrum für Informationstechnik-Gestaltung (ITeG)
Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
Pfannkuchstr. 1
DE-34121 Kassel

+49 (0) 561 804 6083
paul.johannes@uni-kassel.de
http://provet.uni-kassel.de
@lawful_de

ORCID iD 0000-0002-6403-6024



Universität Kassel / Studio Blofeld

provet
UNIKASSEL VERSITÄT