Datenschutzgrundverordnung - Grenzen der unbegrenzten Datenverarbeitungsmöglichkeiten?

2. Big Data-Konferenz an der FH-Kiel

Harald Zwingelberg

Kiel, 23. Juli 2016

VALCRI

VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

ULD

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Gliederung

- Big Data
- Standarddatenschutzmodell
  - Übersicht Gewährleistungsziele
  - Nichtverkettbarkeit und Zweckbindung
  - Transparenz
  - Intervenierbarkeit
- Fazit und mögliche Lösungsansätze für Big Data Unternehmer

Big Data Definition

- Zur Vermeidung von Wiederholungen:
  - Volume - riesige Datenmengen
  - Variety - Vielfalt von Herkunft und Datenarten
  - Velocity - Geschwindigkeit der Erhebung
  - Veracity - Zuverlässigkeit von Quellen und Daten

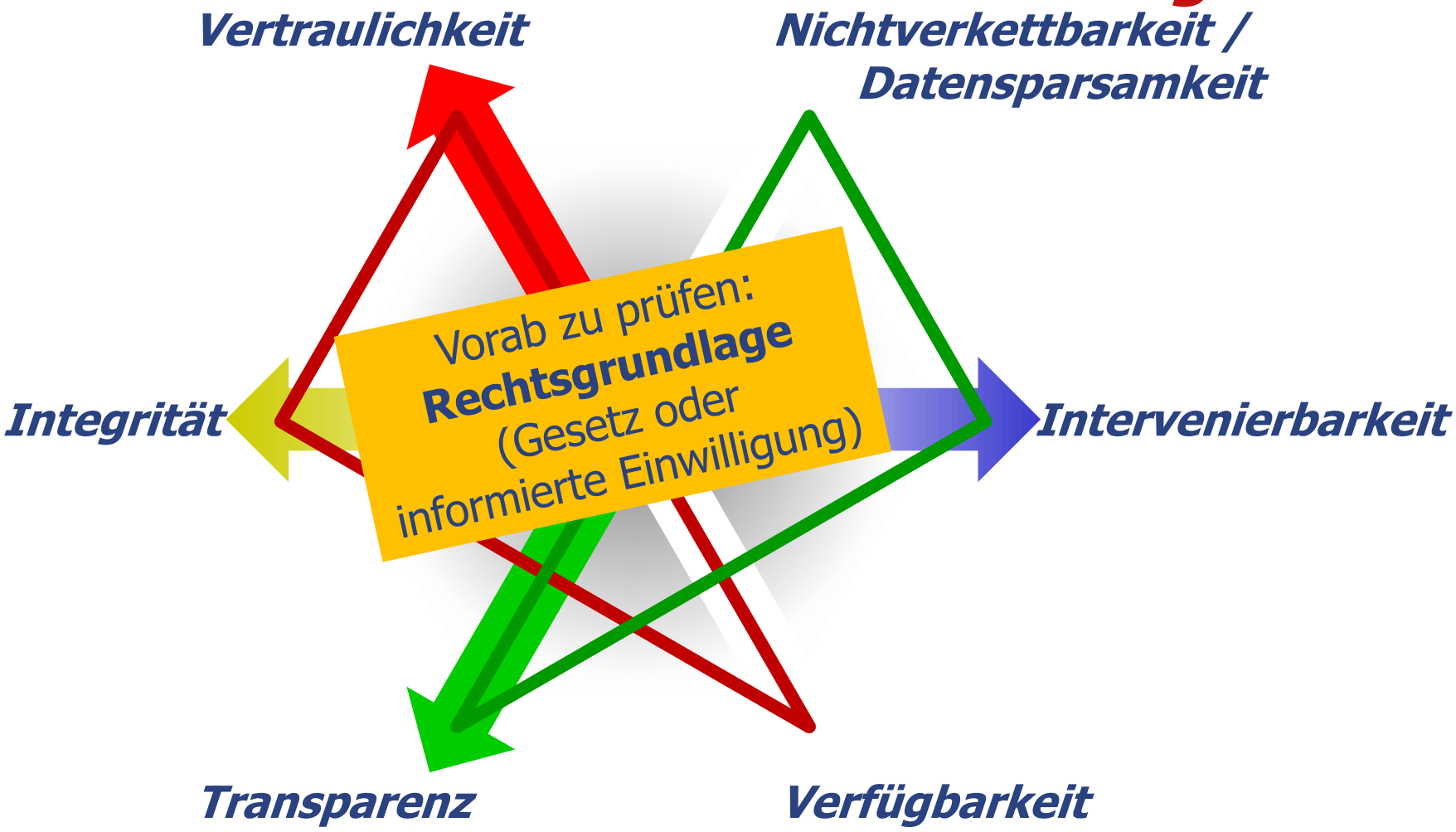
- Potentielle Konflikte mit dem Datenschutz:
  - Volume - Datenminimierung, Zweckbindung
  - Variety - Beschränkungen, z.B. Gesundheitsdaten
  - Velocity - Datensicherheit
  - Veracity - unbeabsichtigte Personenbeziehbarkeit

Standarddatenschutzmodell (SDM) und Gewährleistungsziele

- Das Standarddatenschutzmodell ist eine von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfohlene und im eigenen Prüfbetrieb angewandte Methode zur Beurteilung der Datenschutzkonformität von **Verfahren, Prozessen und Organisationen**.

Volltext zum SDM, weitere Nachweise:
https://www.datenschutzzentrum.de/sdm

Standarddatenschutzmodell (SDM) und Gewährleistungsziele



Nichtverkettbarkeit und Zweckbindung

Gewährleistungsziel Nichtverkettbarkeit und Big Data

- „Das Gewährleistungsziel Nichtverkettbarkeit bezeichnet die Anforderung, dass Daten nur für den **Zweck** verarbeitet und ausgewertet werden, für den sie erhoben werden."
- „Das Datenschutzrecht fordert, [..] dass eine Verarbeitung nach Zwecken getrennt ermöglicht werden muss (Funktionstrennung) bzw. dass die Daten je nach Verarbeitungszweck voneinander getrennt gespeichert werden (Datentrennung). Ggf. muss der Datenbestand durch Duplizierung und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden."

Quelle: Handbuch SDM, S. 12 f,
https://www.datenschutzzentrum.de/uploads/sdm/SDM-Handbuch.pdf

Positionen zum Zweckbindungsgrundsatz

- Das Zweckbindungsprinzip
  - war bereits zentraler Leitgedanke im Volkszählungsurteil des BVerfG (1983),
  - ist grundrechtlich verankert, Art. 8 II EU-GRCh.
- Praxisrelevant: Nur an einem konkreten Zweck lässt sich die Erforderlichkeit bestimmen.
- Erfahrungswert: Die Einwilligung der Betroffenen hängt vom Zweck und der Haltung zu diesem Zweck ab.

Zweckbindung in der DS-GVO

- Das Zweckbindungsprinzip wurde in der DS-GVO klar bestätigt und dem reinen risikobasiertem Ansatz eine Absage erteilt, Art. 5 (1) (b) DS-GVO.
- Aber Zweckänderung ist möglich, Art. 6 (4) DS-GVO, wenn
  - bestehende Einwilligung, den neuen Zweck umfasst,
  - neue Einwilligung vorliegt oder
  - Zweck mit ursprünglichem Zweck vereinbar ist und
  - Transparenz der Zweckänderung, Art. 13 (3), 14 (4)
- Bei der Beurteilung der Vereinbarkeit der Zwecke ist u.a. das Risiko für Betroffene zu berücksichtigen und die getroffenen Schutzmaßnahmen.

Transparenz

Gewährleistungsziel Transparenz

Transparenz bezeichnet die Anforderung, dass sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme hat.

Quelle: Standarddatenschutzmodell, S. 13.

Gewährleistungsziel Transparenz und Big Data

- Informationen sind vollständig, präzise und allgemeinverständlich den Betroffenen zugänglich zu machen, Art. 12 DS-GVO.
- Katalog der erforderlichen Informationen in der Art. 13
- Bei Erhebung beim Betroffenen ist direkt zu informieren.
- Zwecke, Speicherdauer oder Kriterien für Festlegung der Dauer

⇒ Löschfristen und Zwecke sind vorab zu definieren. Das gilt zwar schon jetzt ist aber künftig proaktiv zu beauskunften.

Gewährleistungsziel Transparenz und Big Data

- Bei Erhebung „hinter dem Rücken“ ist nachträglich zu informieren, Art. 14

- Information bei Erhebung ohne Kenntnis der Betroffenen
  - Aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen, Art. 14 (2) (f) DS-GVO.

  ⇒ Auch Daten aus öffentlichen Quellen lösen damit die Informationspflicht aus.

  ⇒ Erforderlich daher: Prozess, zur Information der Betroffenen

  ⇒ Informationen über Rechtsgrundlage, Einwilligung, Quelle der Erhebung sind mit den Daten zusammen zu speichern.

Ausnahmen zugunsten von Big Data

- Transparenz ist kompliziert? Ja.

- Auswege über die Ausnahmen in Art. 14 (5) (b) denkbar?
  - Auskunftspflicht entfällt, sofern „ sich die Erteilung […] als unmöglich erweist oder einen unverhältnismäßigen Aufwand erfordern würde […]
    Regelbeispiele dieser Ausnahme: insbesondere für öffentliche Archive, Forschungszwecke und Statistik. Wohl kein Privileg für Datenverarbeitung zur rein gewinnorientierten (Werbe-)Zwecken.

  - Jedenfalls wird regelmäßig kein unverhältnismäßiger Aufwand vorliegen. Alle Prozesse für die Umsetzung von Betroffenenrechten müssen ohnehin etabliert sein. Gerade bei Big Data kann (Rechen-)Aufwand eher nicht berücksichtigt werden.

Gewährleistungsziel Transparenz und Big Data

- Datenschutz durch Technikgestaltung zur Umsetzung

  ⇒ Informationen über Rechtsgrundlage der Einwilligung und Quelle der Erhebung sind mit den Daten mitzuführen.

  ⇒ Auch um die Rechte auf Auskunft, Berichtigung und Löschung umzusetzen (Intervenierbarkeit) bedarf es entsprechender Prozesse, um Daten eines Betroffenen zu lokalisieren.

  ⇒ Es ist ein standardisierter Prozess sinnvoll, um die Daten mit den erforderlichen Meta-Informationen anzureichern. Dazu gibt es bereits Ausarbeitungen, Stichwort: „sticky policies".

Gewährleistungsziel Transparenz

- **Erweiterter Transparenzbegriff u.a. für Ermittlungsbehörden**

VALCRI
VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

  - Nicht nur Datenschutzperspektive sondern z.B. auch (Straf-)Prozessrecht – Vollständige Nachvollziehbarkeit einer späteren Verurteilung von der Erhebung erster Indizien bis zum Urteil

  - Ethik – Entscheidungen durch Big Data müssen nachvollziehbar sein.

Hinweis: im Polizeibereich gilt nicht die DS-GVO sondern die zeitgleich verabschiedete Datenschutz Richtlinie.

Intervenierbarkeit

⇒ Es **müssen** Prozesse definiert und etabliert sein, um allen Betroffenenrechten entsprechen zu können:

- Art. 15 Auskunftsrecht
- Art. 16 Berichtigen von Daten
- Art. 17 f Löschen und Sperren
- Art. 21 Widerspruchsrecht

⇒Für Nutzer einfache Geltendmachung dieser Rechte

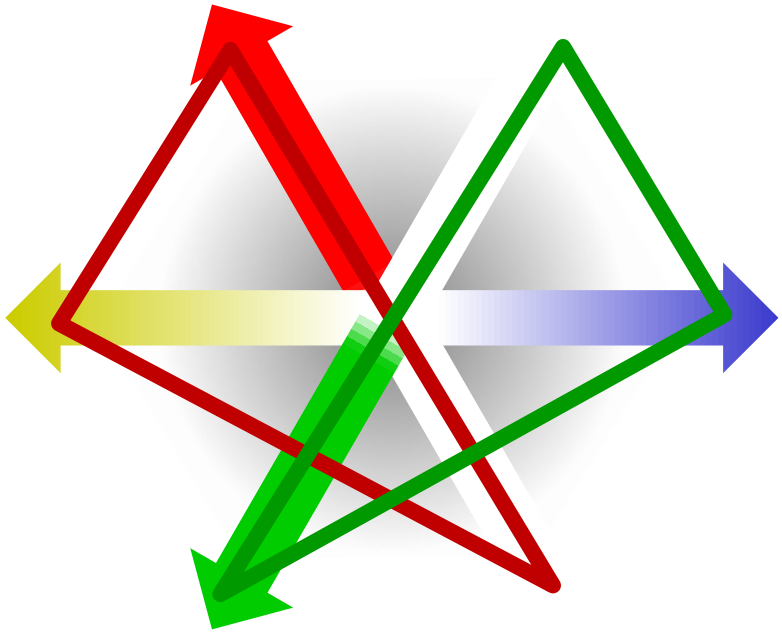
⇒ Wünschenswert: standardisierte Methode zur Kommunikation über Einwilligungen und Benachrichtigung von Betroffenen und Entgegenname von Widersprüchen

Big Data ./. Datenschutz

Vertraulichkeit
- Keine unbefugte Kenntnisnahme statthaft
- Achtung bei externen Anbietern / Verarbeitung in Drittstaaten

Integrität
- Besonders für Angaben zur Herkunft und Empfängern wichtig.
- Korrektheit der Daten

Transparenz
- Dokumentation
- Vorab definierte Zwecke
- Klar definierte Verfahren
- Mitteilung an Betroffene



Nichtverkettbarkeit
- Personenbezug vielfach durch Verkettung doch herstellbar
- Zweckbindung ist wichtig wird aber von Anbietern als „systemwidrig" für Big Data angesehen
- Zwecke müssen definiert sein

Intervenierbarkeit
- Rechte auf Auskunft, Berichtigung, Löschung
- Widerspruchsrecht
- Getrennte Datenhaltung
- Keine Verkettung / Profilbildung
- Kontrollmöglichkeit der verantwortlichen Stelle

Verfügbarkeit
- Begreifbarkeit der Daten, also die semantische Erfassbarkeit

Fazit

- Die partielle Öffnung der Zweckbindung kann Big Data Unternehmen unterstützen, ist aber keine Universalerlaubnis:
  - Transparenzanforderungen wurden gestärkt und beeinflussen die Rechtmäßigkeit der weiteren Datenverarbeitung. (Transparenz)
  - Einflussmöglichkeiten der Betroffenen gestärkt (Intervenierbarkeit)
  - Privacy by Design: Technische Schutzmaßnahmen nach Stand der Technik erforderlich

Mögliche Lösung: Datenschutz durch Technikgestaltung

- Big Data bleibt ein für den Datenschutz ein „Big Problem“
- Zwingend sind Garantien für Betroffene:
  - Anonymisierung, Pseudonymisierung – aber nahezu unmöglich bei Big Data wegen Verkettbarkeit
  - Datenminimierung
  - Sticky policies, nötige Informationen mitführen
  - Transparente Unterrichtung Betroffener
  - Zugriffsschutz, Protokollierung, Rollenkonzepte
  - Bereichsspezifische gesetzliche Rechtsgrundlagen mit klar definierten Einschränkungen und Garantien (z.B. Krebsregister, Statistikämter)

Quellen

Dieser Vortrag beruht auf laufenden Arbeiten aus drittmittelgeförderten Forschungsprojekten am ULD:

iTESA – intelligent Traveller Early Situation Awareness

http://www.smart-data-itesa.de

Forum Privatheit

https://www.forum-privatheit.de/form-privatheit-de/index.php

VALCRI – Visual Analytics for sense-making in Criminal Intlligence Analysis

http://valcri.org

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

EUROPEAN COMMISSION

Mehr zum Thema

- Artikel des ULD zum Thema Big Data
  https://www.datenschutzzentrum.de/plugin/tag/big-data

- Sommerakademie des ULD, 2013
  "Big Data: Informationelle Fremd- oder Selbstbestimmung?!"
  https://www.datenschutzzentrum.de/sommerakademie/2013/

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt:
Harald Zwingelberg
hzwingelberg@datenschutzzentrum.de
www.datenschutzzentrum.de
0431/988-1222