UNIVERSITÄT PASSAU

Datenschutz in der Industrie 4.0

Neue Vorgaben durch die Europäische Datenschutzgrundverordnung

Kai Hofmann
Universität Passau

Zur Person

- Mitarbeiter am Lst. für ÖffR, IT-Recht und Rechtsinformatik
- Lehrstuhlinhaber: Prof. Dr. Gerrit Hornung, LL.M.

- Projekte am Lehrstuhl
  - mirKUL - Kollaborative Unterstützung von Arbeits- und Lernprozessen im Unternehmen mit mobilen interaktiven Multimedia-Anwendungen
  - MisPel - Multi-Biometriebasierte Forensische Personensuche in Lichtbild- und Videomassendaten - Teilvorhaben Rechtliche Anforderungen
  - SkIDentity – Vertrauenswürdige Identitäten für die Cloud

- Eigene Publikationen/Mitwirkung
  - Mitarbeit Umsetzungsempfehlungen Industrie 4.0
  - Unternehmensgeheimnisse in unternehmens-übergreifenden Netzwerken, InTeR 2014, 210

Gliederung

- Datenschutz und Industrie 4.0
- Hintergrund der Reform
- Legislatives Verfahren
- Überblick über wesentliche Regelungsbereiche
- Moderne DS-Instrumente

Datenschutz und Industrie 4.0

- Primär Austausch von unternehmensbezogenen Daten
  - Generiert von „intelligenten“ Objekten
  - Verarbeitung über Firmengrenzen
- Anwendungsbereiche des Datenschutzes
  - Mitarbeiterassistenzsysteme
  - Interaktion der Beschäftigten mit der „intelligenten“ Fabrik
  - Kundendaten
- Informationsschutz im weitesten Sinne
  - Einbeziehung von Unternehmensgeheimnissen
  - Übertragbarkeit datenschutzrechtlicher Prinzipien und Konzepte

Hintergrund der Reform

- Datenschutz-RL 95/46/EG, umgesetzt u.a. im BDSG
  - Erster Entwurf 1990
  - Verabschiedet 1995
- Keine adäquaten Lösungen für moderne Phänomene
  - Cloud Computing
  - Internet der Dinge
  - Big Data
- Keine einheitlichen Regelungen innerhalb der EU
- Unzureichender räumlicher Anwendungsbereich
- Enormes Vollzugsdefizit

Legislatives Verfahren

- Kommissionsentwurf 25.1.2012
- Parlament
  - Berichtsentwurf 16.1.2013
  - 3133 Änderungsanträge
  - Abstimmung im Innenausschuss 21.10.2013
  - Abstimmung im Parlament 12.3.2014
- Rat: anhaltende Diskussionen
- Trilogverhandlungen ab Sommer 2014
- Inkrafttreten wahrscheinlich 2018-2020

Überblick (I)

- Wechsel zur Verordnung
  - unmittelbare Geltung, kein Umsetzungsakt notwendig
  - Keine individuelle Beschwerde zum BVerfG, stattdessen EGMR
- Anwendungsbereich
  - Räumlich: Marktortprinzip
  - Sachlich: unklar, ob relativer oder absoluter Personenbezug
- Grundsätze des Datenschutzes
  - Aufrechterhaltung des Verbotsprinzips
  - Verarbeitung nur für konkrete Zwecke
  - Erforderlichkeitsprinzip
  - Integrität

Überblick (II)

- Rechtsgrundlagen der Datenverarbeitung
  - Nahezu unverändert, Art. 7 DS-RL nun Art. 6 DS-GVO-E
  - I 4.0: v.a. Einwilligung und Vertrag oder Kollektivvereinbarung
- Fokussierung auf Informationspflichten
  - Symbolhafte Informationen (Art. 13a)
  - Umfangreiche Informationspflichten (Art. 14)
- Zuständigkeit der Aufsichtsbehörden (One Stop Shop)
  - DS-RL: Zuständigkeit am Ort der Niederlassung, die Verarbeitung ausführt
  - DS-GOV-E: Nur am Ort der Hauptniederlassung (strittig)
  - Zurückdrängung der Kommission, stattdessen DSA

Überblick (III)

- Datenschutzbeauftragter
  - Schwelle zur Pflichtbestellung umstritten
  - Anreiz: keine Notwendigkeit vorheriger Konsultation der Aufsichtsbehörde
- Sanktionen
  - Verschuldensunabhängige Haftung 100 Mio. € oder 5 % Umsatz
  - Verschuldensabhängig für Inhaber von DS-Siegeln

Beispielhafte Verarbeitungssituationen

- Annahme: Interaktion von Beschäftigten mit vernetzten Gegenständen hinterlassen pers.bez. Daten

- Unternehmensübergreifende internationale Lieferkette
  - Einbindung von z.B. Zulieferer, Logistikdienstleister, Hersteller, ...
  - Standardisierter Datenaustausch zur Abstimmung
  - Echtzeitfähige Steuerung der Lieferkette
  - **Auslandsbezug; mehrere/gemeinsam Verantwortliche**

Bsp. 1: Internationale Lieferkette

- Bisherige Rechtslage
  - Erforderlich für Durchführung des Beschäftigungsverhältnisses
  - Interessenabwägung (str.)
  - Einwilligung (P: Freiwilligkeit)
  - Kollektivvertragliche Regelung
- DS-GVO-E: Öffnungsklausel Art. 82
  - Zum Zweck der Erfüllung des Arbeitsvertrages
  - Einwilligung (P: Freiwilligkeit)
  - Kollektivvereinbarung
- Verantwortlichkeit
  - Wer Zweck und Mittel festsetzt
  - Keine Neuerung

Datenübermittlung ins Ausland

- Übernahme der Instrumente von DS-RL und BDSG
  - Angemessenheitsbeschluss der Kommission
  - Standard-Datenschutzklauseln
  - Binding Corporate Rules
  - Individuelle Genehmigung von Vertragsregeln

- Neu in der DS-GVO-E Parl
  - Datenschutzsiegel für Verantwortlichen UND Empfänger

Zertifizierung und Siegel

- Bisher
  - Ansätze in § 9a BDSG
  - Auditierung/Zertifizierung durch das ULD
  - EuroPriSe
- Konkretisierung durch Parlamentsentwurf
  - Gegenstand: Einklang des Verfahrens mit DS-GVO-E
  - Umfang: DS-Grundsätze, DS durch Technik, Datensicherheit
- Verfahren
  - Zertifizierungsmonopol der Aufsichtsbehörden
  - Möglichkeit (nicht Pflicht), akkreditierte Prüfer einzuschalten
  - 5 Jahre gültig

Zertifizierung und Siegel (II)

- Anreize
  - Privilegierung für Datenübermittlung ins Ausland
  - Garantien für Auftragsdatenverarbeitung
  - Werbeeffekt
    a) Aber: Keine Möglichkeit der Übererfüllung
    b) Lediglich Bestätigung der Rechtskonformität
  - Berücksichtigung bei der Verhängung von Geldbußen
- Kritik/Unklarheit
  - Nur Prüfung von Verfahren (Auditierung), nicht von Produkten (Zertifizierung)

Siegel in Wertschöpfungsketten

- Siegelvergabe an Beteiligte/Anwärter
  - Anwärter muss gesamtes Auditierungsverfahren durchlaufen
  - Erleichterung der Auditierung beim Einsatz von zertifizierter Software zum Datenaustausch
  - Produktzertifizierung unklar

- Siegelvergabe an das gesamte Netzwerk
  - Jeder Beteiligte muss grds. selbständig auditiert werden
  - Keine Auditierung eines ganzen Netzwerks möglich
  - Ausnahme evtl. gemeinsame Verantwortung

Datenschutz durch Technik (I)

- Technische Absicherung für rechtl. Anforderungen
  - Datenschutz mit, nicht gegen Technik
  - Prinzip: keine technische Möglichkeit – kein Verbot notwendig

Ansätze im BDSG

- § 9 BDSG – Datensicherheit
  - Vertraulichkeit, Integrität, Verfügbarkeit, …
  - Adressat: verantwortliche Stelle und Auftragsdatenverarbeiter

- § 3a BDSG – Datenvermeidung und Datensparsamkeit
  - Vorsorge durch DV-Systemgestaltung
  - Technische Umsetzung: Anonymisierung und Pseudonymisierung
  - Adressat: Hersteller und verantwortliche Stelle
  - Reiner Programmsatz, Nichtbeachtung folgenlos

Datenschutz durch Technik (II)

Ansätze in der DS-GVO-E

- Art. 30 – Datensicherheit
  - Wie § 9 BDSG
  - Adressat: verantwortliche Stelle und Auftragsdatenverarbeiter

- Art. 23 – Datenschutz durch Technik
  - Fortwährende Selbstprüfung
    a) Bei Festlegung von Zwecken und Mitteln
    b) Bei Verarbeitung selbst
  - Adressat: verantwortliche Stelle und Auftragsdatenverarbeiter
  - Umfassender Ansatz von Erhebung bis Löschung („Life Cycle Management“)
  - Technische Umsetzung des Erforderlichkeitsprinzip

- Nichteinhaltung bußgeldbewährt

Datenschutz durch Technik (III)

Nicht in DS-GVO-E enthalten

- Anforderungen an Hersteller technischer Systeme
- Vorgaben zur Ermöglichung anonymer Nutzung
- Allg. Bestimmung zu Pseudonymisierung und Anonymisierung
  - Nur bei Gesundheitsdaten
  - Sonst nur im Wege der Interessenabwägung zu beachten

Beispielhafte Verarbeitungssituationen

- Annahme: Interaktion von Beschäftigten mit vernetzten Gegenständen hinterlassen pers.bez. Daten

- Unternehmensübergreifende internationale Lieferkette
  - Einbindung von z.B. Zulieferer, Logistikdienstleister, Hersteller, ...
  - Standardisierter Datenaustausch zur Abstimmung
  - Echtzeitfähige Steuerung der Lieferkette
  - **Auslandsbezug; mehrere/gemeinsam Verantwortliche**

- Zustandsbasierte Wartung
  - Umfangreiche Datenerhebung an der jeweiligen Maschine
  - Datenweitergabe an spezialisierten Anbieter/Hersteller
  - Rückmeldung der aktuell notwendigen Wartungsaufgaben
  - **Auftragsdatenverarbeitung**

Bsp. 2: Fernwartung, Auftragsdatenverarb.

- Übermittlungsbefugnis erforderlich

- Auftragsdatenverarbeitung BDSG
  - Schriftliche, umfangreiche Auftragserteilung
  - Weisungsbefugnis des Verantwortlichen
    P: Konzernunternehmen
  - P: Kontrollbefugnisse des Verantwortlichen

- Auftragsdatenverarbeitung DS-GVO-E
  - Grundsätzlich wie BDSG
  - Nachweis mittels Siegel statt Kontrollrechte des Verantwortlichen
  - Nachweis über die Einhaltung von Verhaltensregeln

- EU-weites Konzernprivileg DS-GVO-E
  - Bei angemessenem DS-Niveau (Nachweis mit Verhaltensregeln)

Selbstregulierung

- Keine Rechtsetzung, nur Verhaltensregeln zur Anwendung der Verordnung

- Verfahren
  - Von Verbänden/Aufsichtsbehörden auszuarbeiten
  - Von Aufsichtsbehörden/Kommission anzunehmen

- Wirkung
  - Keine Bindung gegenüber den Branchenunternehmen
  - Rechtssicherheit gegenüber Aufsichtsbehörden
  - Konkretisierung der Informationspflichten
  - Nachweisfunktion für Garantien des Auftragsdatenverarbeiters

Datenschutzfolgenabschätzung

- Zweistufiges Verfahren
- Risikoanalyse (Vorfilter)
  - 5000 Betroffene in 12 Monaten
  - Regelmäßige und systematische Beobachtung von Betroffenen
  - …
- Abschätzung der Folgen für den Betroffenen
  - Beschreibung des Verfahrens
  - Bewertung hinsichtlich der Erforderlichkeit zur Zweckerreichung
  - Risikoeinschätzung
  - Beschreibung der Abhilfemaßnahmen (Datenschutz durch Technik)
- Überprüfung alle 2 Jahre

Data Breach Notification

- An die Aufsichtsbehörde
  - Jeder Verstoß
  - Keine Beschränkung wie in § 42a BDSG
- An die Betroffenen
  - Nur bei wahrscheinlicher Beeinträchtigung der Privatsphäre/Interessen des Betroffenen
  - Lässt sich abwenden, wenn vorher technische Sicherheitsvorkehrungen angewendet wurden
    a) Verschlüsselung
    b) Pseudonymisierung

Beschäftigtendatenschutz

- Öffnungsklausel für die Mitgliedsstaaten

- Aber: „im Einklang mit den Regelungen“
  - Reichweite der Öffnungsklausel unklar
  - Mindestanforderungen in Art. 82 Abs. 1c DS-GVO-E (Parl)

- Profiling
  - Denkbar bei Assistenzsystemen
  - Jedenfalls ein Widerspruchsrecht
  - Bei rechtlicher oder ähnlicher Wirkung
    a) Nur mit Einwilligung des Betroffenen
    b) Kollektivvereinbarung nicht ausreichend

Datenschutz in der Industrie 4.0

Neue Vorgaben durch die Europäische Datenschutzgrundverordnung

Kai Hofmann

Kai.Hofmann@uni-passau.de

http://www.jura.uni-passau.de/hornung.html