Neuordnung EU-Datenschutzrecht – zwei Seiten einer Medaille

Dr. Nicolai Besgen, MEYER-KÖRING
Jörg Rossen, Creditreform Bonn

12. Bonner Unternehmertage
Bonn, 12. Oktober 2017

Zeitachse

EU-Datenschutzgrundverordnung

- seit 25. Mai 2016 in Kraft
- **ab 25. Mai 2018 wirksam**

Neues Bundesdatenschutzgesetz

- neues BDSG* (DSAnpUG EU**)
  seit 5. Juli 2017 in Kraft
- **ab 25. Mai 2018 wirksam**

© Fotolia / Zerbor

Ziele

- **Schutz personenbezogener Daten**
- **Informationelle Selbstbestimmung**
- **Freier Verkehr personenbezogener Daten**

Grundsätze gemäß Art. 5 Absatz 1 EU-DSGVO

- Rechtmäßigkeit
- Datensparsamkeit
- Zweckbindung
- Datensicherheit
- Transparenz, Betroffenenrechte

Präzisiert!

* BDSG – Bundesdatenschutzgesetz
** DSAnpUG EU – Datenschutz Anpassungs- und Umsetzungsgesetz EU

Neue Rechtsgrundlagen
für die Verarbeitung personenbezogener Daten

Deutlich **gestiegene Bußgeld- und Haftungsrisiken** für Geschäftsführer und Datenschutzbeauftragte

Bußgeld (der höhere Wert)
- bis zu 20 Mio. Euro oder
- 4% des Jahresumsatzes

Änderungen umsetzen!

Die Zeit bis Mai 2018 nutzen!

Hohe Aufwände
für die Information von Betroffenen und die Dokumentation von Datenbestand, Datenflüssen und Datenverarbeitungs-prozessen

Höhere Sensibilität
bei Kunden und Geschäftspartnern

Neuordnung EU-Datenschutzrecht – Worum geht es?

Personenbezogene Daten

Alle Informationen, die sich auf eine betroffene Person beziehen.

» Primär: **Namen**, **Geburtsdatum/-ort**

Eine betroffene Person ist „eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die [jemand] aller Voraussicht nach einsetzen würde."

» Hierzu zählen: **Telefonnummern**, **Adressen**, **Kontonummern**, **Online-Kennungen** wie **E-Mail-Adressen** und **biometrische Daten**

» Aber auch: Unterschiedliche Datenfelder mit **Metadaten**, typischerweise **Geo-Daten** und **Datumsangaben**, **Cookie-IDs**, **User-IDs**, **IP-Adressen**, **MAC-Adressen**

Erweitert!

Räumlicher Anwendungsbereich

Verarbeitung personenbezogener Daten,

» im Rahmen eines Angebots, das sich an einen nationalen Markt in der EU richtet oder

» der Beobachtung des Verhaltens von Personen in der EU dient.

Damit Geltung für

» Unternehmen in der EU und

» außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind.

» **Marktortprinzip!**

Neu!

Rechenschaftspflicht

Art. 5 Absatz 2 EU-DSGVO

Der Verantwortliche ist für die Einhaltung des Absatzes 1 **verantwortlich und** muss dessen **Einhaltung nachweisen** können („Rechenschaftspflicht“).

Im Ergebnis:

- **Dokumentation!**
- **Dokumentation!**
- **Dokumentation!**

„Buchhaltung für Daten“

Ziel: Nachweis des Rechts an den Daten

- **Einwilligung** der betroffenen Person
- **Rechtsgrundlage**

Bestandsaufnahme von Verfahren mit personenbezogenen Daten

- Internes Verfahrensverzeichnis

Prüfung und **GAP-Analyse** der datenschutzrechtlichen Zulässigkeit aller Verfahren

Anpassung Datenschutzmanagement-System inkl. Dokumentation und Implementierung von Prozessen zur Vermeidung von Haftungsrisiken

- Informationspflichten
- Betroffenenrechte
- Auftragsdatenverarbeiter
- DS*-Folgeabschätzung
- Datensicherheit (TOM**)
- Datenschutzpannen

* DS – Datenschutz
** TOM – Technisch organisatorische Maßnahmen

Exkurs: Verfahren mit personenbezogenen Daten (1)

Dokumentationspflichten

Verfahrensverzeichnis

- **Interne Dokumentation** mit Angaben zum Zweck der Erhebung, den Datenarten, den Kategorien von Empfängern, sowie der Übermittlung in Drittstaaten
- Diese Pflicht trifft **auch Auftragsdatenverarbeiter** bezüglich der auftragsbezogenen Verarbeitung personenbezogener Daten

Dokumentation von **Sicherheitsvorfällen** und Meldung an Aufsichtsbehörde binnen 72h über Art der Datenschutzverletzung, betroffene Datenkategorien, Zahl der betroffenen Personen und ergriffene Maßnahmen

Datenschutz-Folgeabschätzung inklusive regelmäßiger Kontrolle (alle 2 Jahre)

Was ist ein Verfahren?

Der Begriff „Verfahren“ bezeichnet die **Gesamtheit an Verarbeitungen, mit deren Hilfe eine Zweckbestimmung oder ein Bündel zusammengehöriger Zweckbestimmungen realisiert wird**.

Ein Verfahren kann aus einer Vielzahl von DV-Programmen und Dateien bestehen.

Wesentlich für die Bestimmung des Verfahrens ist der **verfolgte Zweck der Datenverarbeitung**.

Exkurs: Verfahren mit personenbezogenen Daten (2)

Beispiele in der Administration

- Buchhaltung
- Bewerber-Management
- Dateiablage
- E-Mail
- Fahrtenbuch
- Kundendaten
- Marketing
- Newsletter
- Personal-Management
- Reisekosten-abrechnung
- Schulungen
- Social Media
- Terminkalender
- Urlaubsplanung
- Vorgangslisten
- Veranstaltungs-Management
- Vertragsablage
- Website
- Website-Analyse
- Weihnachtskarten
- …

Produkte und produktive Prozesse
(mit personenbezogenen Daten)

Inhalt der Verfahrensbeschreibung

- Name oder Firma der **verantwortlichen Stelle**
- Inhaber, Vorstände, **Geschäftsführer** oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der **Leitung der Datenverarbeitung** beauftragten Personen, **Datenschutzbeauftragter**
- **Anschrift** der verantwortlichen Stelle
- **Zweckbestimmungen** der Datenerhebung, -verarbeitung oder -nutzung
- Beschreibung der **betroffenen Personengruppen** und der diesbezüglichen Daten oder Datenkategorien
- **Empfänger** oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
- **Regelfristen für die Löschung** der Daten
- Geplante **Datenübermittlung** in **Drittstaaten**
- Allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die **Maßnahmen** nach § 9 BDSG **zur Gewährleistung der Sicherheit** der Verarbeitung angemessen sind.

Informationspflichten in der Datenschutzerklärung

1. Namen und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
2. **Kontaktdaten des Datenschutzbeauftragten**
3. Zwecke und **Rechtsgrundlage**
4. Ggf. die **berechtigten Interessen an** einer **Datenverarbeitung**
5. Ggf. Empfänger oder Kategorien von Empfängern der personalbezogenen Daten
6. Ggf. die Absicht einer Übermittlung in Drittstaaten oder an eine internationale Organisation
7. Weitere **Informationen**, die **notwendig** sind, **um** eine **faire** und **transparente Verarbeitung zu gewährleisten**
8. **Dauer der Datenspeicherung** bzw. Kriterien für die Festlegung der Dauer
9. Bestehen von Betroffenenrechten wie Auskunft, Berichtigung, Löschung, Sperrung, Widerspruchsrecht oder Datenübertragbarkeit
10. Widerrufsrecht bei einwilligungsbasierter Datenverarbeitung
11. Bestehen eines **Beschwerderechts bei einer Aufsichtsbehörde**
12. Ggf. **ob** die **Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben ist oder für den Vertragsschluss erforderlich ist**
13. Ggf. **Informationen** zum **Profiling sowie aussagekräftige Informationen über involvierte Logik sowie Tragweite und die angestrebten Auswirkungen**

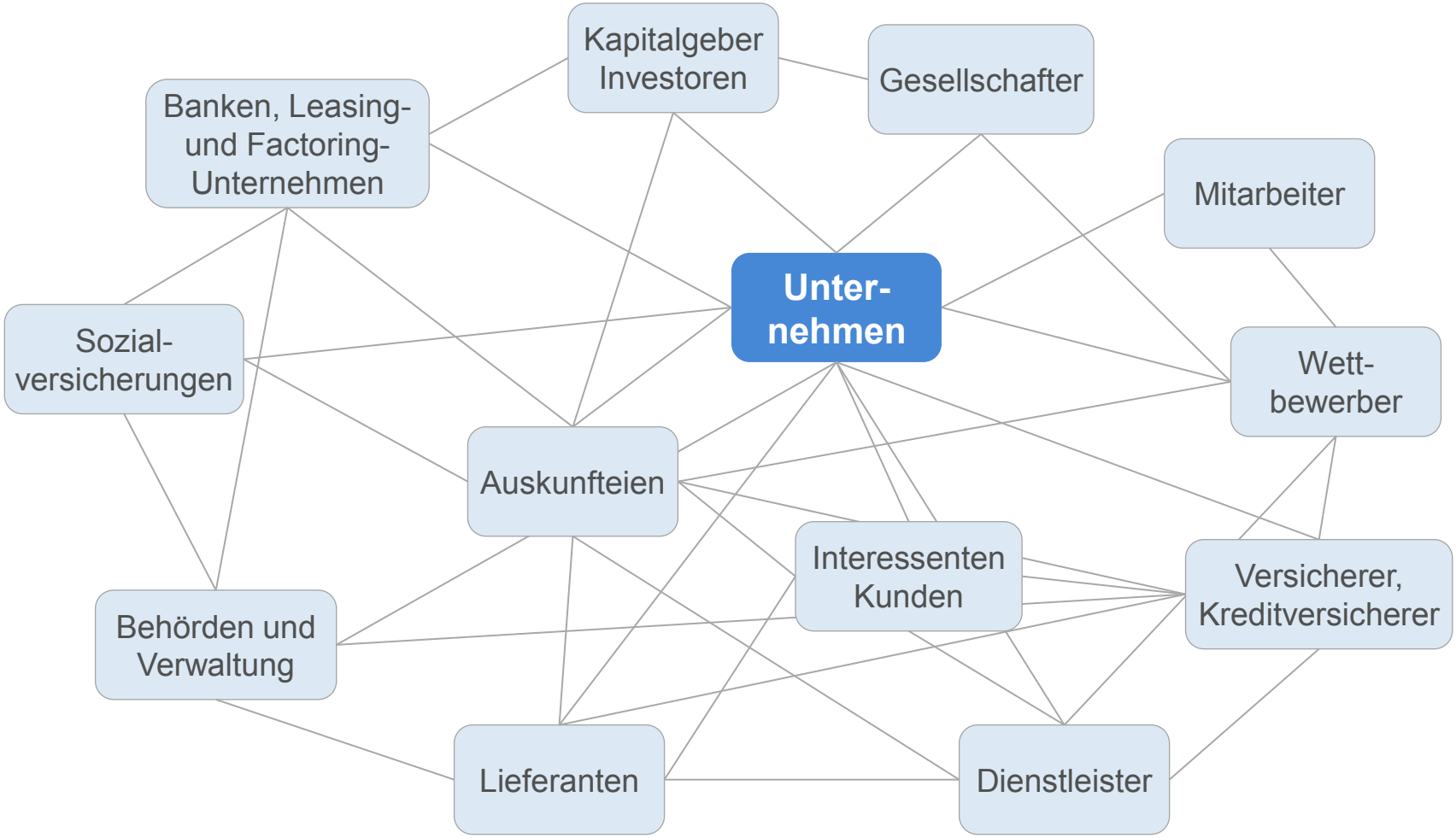
Welche Rechte hat die betroffene Person einer Datenverarbeitung

- → Informationsrecht
- → Auskunfts- und Widerspruchsrecht
- → Recht auf Berichtigung, Löschung (Vergessen werden) und Einschränkung
- → Recht auf Datenübertragbarkeit – Daten Portabilität

Neu!

Im Ergebnis: Einrichtung von Prozessen zur Wahrnehmung von Betroffenenrechten erforderlich!

Klares Rollenbild: Akteur oder als Unternehmer betroffene Person



Kontroll- und Überwachungsinteresse des Arbeitgebers versus Beschäftigtendatenschutz

→ Ausgangslage:

» Die Bestimmungen des Datenschutzes konkretisieren den Schutz des

– **allgemeinen Persönlichkeitsrechts**,

– des **Rechts auf informationelle Selbstbestimmung** und

– des **Rechts am eigenen Bild**.

→ Verhältnismäßigkeitsgrundsatz:

» Eingriffe in diese Rechte müssen einer Abwägung der beiderseitigen Interessen nach dem Grundsatz der **Verhältnismäßigkeit** standhalten.

» Eine **übermäßige Belastung der Arbeitnehmer** ist zu **vermeiden**.

DARF DER DAS 1: Verdeckte Überwachung durch Detektive BAG 29. Juni 2017 – 2 AZR 597/16

Arbeitgeber darf überwachen, um zu kontrollieren, ob Arbeitnehmer seinen Pflichten nachkommt. Dazu gehört auch die Aufdeckung einer Pflichtverletzung, die eine Kündigung des Arbeitsverhältnisses rechtfertigen kann.

- → Hier: Konkurrenztätigkeit und Erschleichen einer AU-Bescheinigung.
- → Es muss sich nicht um eine Straftat handeln.
- → Es ist aber zwingend ein auf konkreten Tatsachen gestützter Verdacht notwendig, um dem Verhältnismäßigkeitsgrundsatz zu genügen.

DARF DER DAS 2: Geldentschädigung wegen unzulässiger Detektivüberwachung BAG 19. Februar 2015 – 8 AZR 1007/13

Ein Arbeitgeber, der wegen des Verdachts einer vorgetäuschten Arbeitsunfähigkeit einem Detektiv die Überwachung eines Arbeitnehmers überträgt, handelt rechtswidrig, wenn sein Verdacht nicht auf konkreten Tatsachen beruht.

- → Hoher Beweiswert einer ärztlichen Arbeitsunfähigkeitsbescheinigung.
- → Daher begründete Zweifel an der Richtigkeit der ärztlichen Bescheinigung erforderlich.
- → Eine Verletzung des allgemeinen Persönlichkeitsrechts durch eine rechtswidrige Überwachung eines Arbeitnehmers einschließlich heimlicher Videoaufnahmen kann einen Geldentschädigungsanspruch begründen.

DARF DER DAS 3: Überwachung mittels Keylogger – Verwertungsverbot BAG 27. Juli 2017 – 2 AZR 681/16

Arbeitgeber installierte auf PC Software, die alle Tastatureingaben protokollierte und regelmäßig „Screenshots“ anfertigte (Keylogger). Die Auswertung führte zu privater Nutzung, u. a. Computerspiele und privaten E-Mails.

- → Fristlose Kündigung wegen Eingriffs in das Recht auf informationelle Selbstbestimmung unzulässig.
- → Umfassendes Beweisverwertungsverbot.
- → Keine Zulässigkeit nach BDSG.

DARF DER DAS 4: Heimliche Videoüberwachung
BAG 20. Oktober 2016 – 2 AZR 395/15

Eingriffe in das Recht der Arbeitnehmer **am eigenen Bild** durch verdeckte Videoüberwachung **sind** dann **zulässig**, wenn

- der konkrete Verdacht einer strafbaren Handlung oder einer anderen schweren Verfehlung zu Lasten des Arbeitgebers besteht,
- weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und
- sie insgesamt nicht unverhältnismäßig ist.
- Die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten zur Aufdeckung von Straftaten gem. § 32 Abs. 1 Satz 2 BDSG setzt lediglich einen "einfachen" Verdacht im Sinne eines Anfangsverdachts voraus, der über vage Anhaltspunkte und bloße Mutmaßungen hinausreichen muss.

DER DARF DAS, wenn …

Checkliste

1. Keine Dauerüberwachung ohne konkrete Anhaltspunkte
2. Konkreter Verdacht
3. Mildere Mittel vorher ausschöpfen
4. Vorgehen dokumentieren und Beweise sichern
5. Mitbestimmung Betriebsrat beachten

Fazit: Die heimliche Überwachung ist bei Einhaltung dieser Grundsätze auch zukünftig nach der EU-DSGVO weiterhin zulässig!

Kontakt

Creditreform Bonn Domschke & Rossen KG

Jörg Rossen

+49 228 2679456
j.rossen@bonn.creditreform.de

MEYER-KÖRING Rechtsanwälte Steuerberater

Dr. Nicolai Besgen

+49 228 7263640
besgen@meyer-koering.de