UNTERNEHMEN UND DATENSCHUTZ

Workshop
München Juni 2016

DATENSCHUTZ

www.unternehmen-und-datenschutz.de

UNTERNEHMEN UND DATENSCHUTZ

Punkt 1: Ort der Datenerhebung 1/3

BDSG: Sitzlandprinzip (§ 1 Abs. 5 BDSG)=>

BDSG anwendbar, wenn:

innerhalb EU/EWG:
-Unternehmen Sitz in EU / EWR: seine Niederlassung (NL) in Deutschland (D) nimmt die Datenverarbeitung (DV) vor

-Unternehmen/NL in D lässt die DV von Unternehmen mit Sitz in EU / EWR durchführen (Auftragsdatenverarbeitung § 3 Abs. 8 S. 3 , § 11 BDSG)

Drittland:
-Unternehmen mit Sitz in Drittland: DV wird in Deutschland durchgeführt (Server in D zB)

UNTERNEHMEN UND DATENSCHUTZ

Punkt 1: Ort der Datenerhebung 2/3

BDSG: Sitzlandprinzip =>

BDSG nicht anwendbar, wenn:

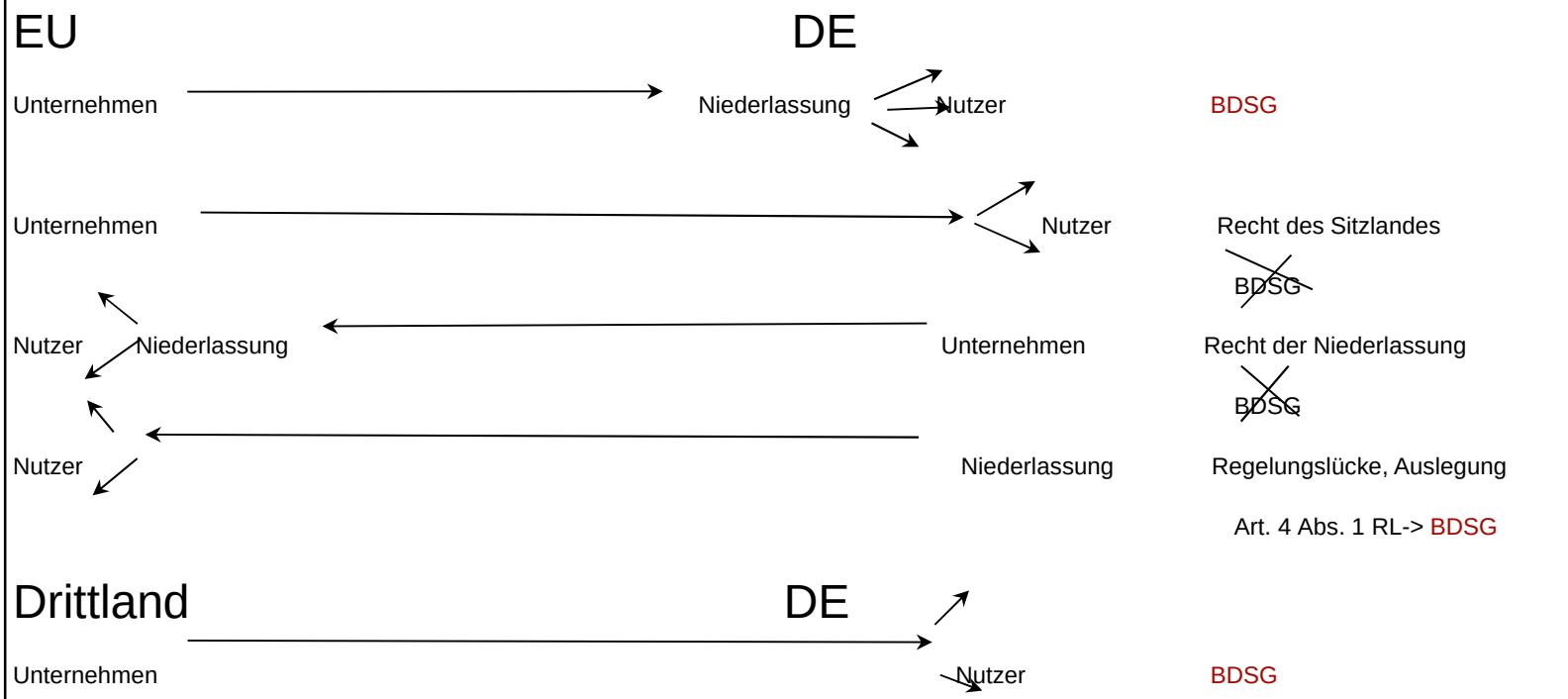
- die DV außerhalb Deutschlands in der EU/EWG, oder

- die DV außerhalb Deutschlands in einem Drittland durchgeführt wird

=> das am Sitz der verantwortlichen Stelle geltende Datenschutzrecht findet Anwendung

UNTERNEHMEN UND DATENSCHUTZ

Punkt 1: Ort der Datenerhebung 3/3



UNTERNEHMEN UND DATENSCHUTZ

Punkt 2: Voraussetzungen für zulässige Datenübermittlung in D 1/5
in D

BDSG: Verbot mit Erlaubnisvorbehalt **(§ 4 a I BDSG)**

Erlaubnis aus **Gesetz:** (Steuerrecht, HGB, normative Teile in Tarifverträgen, Betriebsvereinbarungen etc.); gilt nur deutsche Rechtsvorschriften

Erlaubnis aus **Einwilligung:**
- Schriftformerfordernis oder andere Form angemessen (elektronisch), Rsp. verlangt **Double opt in**

- Vorherige Information über Verwendungszweck und Datenübermittlung

- Einwilligung gemeinsam mit anderen Erklärungen ist besonders hervorzuheben

Rechtsfolge bei Verstoß: **OWi (§ 43 II BDSG: Bußgeld bis zu 50.000 €)**

UNTERNEHMEN UND DATENSCHUTZ

Punkt 2: Voraussetzungen für zulässige Datenübermittlung 2/5
in D

Unterschiedliche Einwilligungen je nach Medium und Zweck (UWG, TMG, TK, BDSG)

- Datenschutzrechtliche Einwilligung (bei Nutzung nach BDSG)

- Wettbewerbsrechtliche Einwilligung (bei Nutzung zu Werbezwecken)

- Telemedien Einwilligung (bei Nutzung eines Telemediums)

- Telekommunikations-Einwilligung (bei Nutzung durch Telekommunikations-anbieter)

Beachte: Der Betroffene ist über jeden beabsichtigten Verarbeitungszweck zu informieren, bei Änderung/Erweiterung u.U. Aktualisierung erforderlich

UNTERNEHMEN UND DATENSCHUTZ

Punkt 2: Voraussetzungen für zulässige Datenübermittlung 3/5
in D

Erlaubnis aus § 28 BDSG

- bei einem Vertragsverhältnis mit dem Betroffenen, wenn es dem Zweck des Verhältnisses dient (zB DV von Arbeitnehmerdaten)

- wenn die Datenerhebung zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und keine schutzwürdigen Interessen des Betroffenen überwiegen

- wenn Daten allgemein zugänglich sind außer schutzwürdige Interessen des Betroffenen würden offensichtlich überwiegen

Punkt 2: Voraussetzungen für zulässige Datenübermittlung 4/5
in ein Land der EU/EWG

Erlaubnis wegen „Angemessenen Datenschutzniveaus“ (§ 4b Abs. 1 BDSG):

Durch Umsetzung der EU-Datenschutzrichtlinie 95/46/EG in allen Mitgliedstaaten der EU und geltend für die EWR-Staaten Norwegen, Island, Liechtenstein: „Angemessenes Datenschutzniveau“

=> der Datenverkehr innerhalb der Mitgliedstaaten der Europäischen Union und mit den EWR-Staaten ist genauso zu behandeln ist wie die inländische Datenübermittlung und in diesem Rahmen zulässig

Punkt 2: Voraussetzungen für zulässige Datenübermittlung 5/5 in ein Drittland

Erlaubnis bei Angemessenheit des Schutzniveaus (§ 4b Abs. 2 BDSG):

- Wenn das Schutzniveau anerkannt ist und keine anderen schutzwürdigen Interessen des Betroffenen entgegenstehen

- bei Vorliegen einer Vereinbarung des Landes mit der EU, die ein angemess. Schutzniveau sicherstellt und der Übermittlungsempfänger dieser Vereinbarung beigetreten ist (Beispiel: „Safe Harbor Principles“ in USA)

- wenn der Betroffene eingewilligt hat oder die Übermittlung zur Erfüllung eines Vertrags mit dem Betroffenen notwendig ist (§ 4c BDSG)

- wenn das fehlende angemess. Schutzniveau durch ausreichende Garantien ausgeglichen, zBaus Vertragsklauseln und verbindlichen Unternehmens-regelungen (§ 4c BDSG): „Codes of Conduct“

UNTERNEHMEN UND DATENSCHUTZ

Punkt 2: Konzerninterne Datenübermittlung

- Kein Konzernprivileg !

- Übermittlung von personenbezogenen Daten innerhalb rechtlich selbständiger Unternehmen im Konzern wie unter fremden Unternehmen

- Lösungsansatz bei DV nach 28 BDSG für eigene Geschäftszwecke: Auftragsdatenverarbeitung nach § 11 BDSG:

  DV erfolgt durch ein anderes selbständiges Konzernunternehmen im Auftrag

  der Auftragnehmer (das Konzernunternehmen) hat Sitz innerhalb der EU / EWR (§ 3 Abs. 8 Satz 3 i.V.m. § 3 Abs. 4 Nr. 3 BDSG)

- Beachte: Funktionsübertragung kein § 11 BDSG; Auslagerung des gesamten Aufgabenbereichs Personalverwaltung an eine konzerninterne zentrale Personalverwaltung = *Funktionsübertragung* (h.M.)

UNTERNEHMEN UND DATENSCHUTZ

Punkt 2: Konzerninterne Datenübermittlung: Auftragsdatenverarbeitung

Wichtigsten Merkmale des § 11 BDSG

- Der Auftragnehmer (Konzerngesellschaft, die die DV durchführt) übernimmt nur die Speicherung und ggf. die Strukturierung der Daten (verlängerter Arm)
- Auftraggeber (Konzerngesellschaft, die die DV durchführen lässt) behält Bestimmungsrecht darüber, welche Daten gespeichert oder verarbeitet werden. Er erteilt Auftragnehmer Weisungen hinsichtlich Verarbeitung und Nutzung von Daten
- Eine Weitergabe von Daten an außenstehende Dritte (sog. Funktionsübertragung) ist nur mit Einwilligung des Betroffenen erlaubt
- Beachte **außerhalb D und EU und EWR**:
- § 11 BDSG Auftragsverarbeitung NICHT zulässig, gem. § 3 Abs. 8 BDSG ist das im Auftrag Daten verarbeitende Unternehmen IMMER DRITTER

UNTERNEHMEN UND DATENSCHUTZ

Punkt 3 Datenspeicherung-Aufbewahrungspflichten

Aufbewahrungspflichten nach Steuerrecht (§ 147 AO) oder Handelsrecht (§ 257 HGB) 6 (Geschäftsbriefe) oder 10 Jahre (Buchungsunterlagen)

Weitere Vorschriften im:

Produkthaftungsgesetz ProdHaftG
Steuerrecht EStG, KStG, GewStG
Zivilrecht BGB, ZPO
Aktiengesetz AktG
Banken- und Versicherungsgesetz
Beamtenrecht
Röntgenverordnung RöV
Verordnung über Entsorgungsfachbetriebe EfbV

UNTERNEHMEN UND DATENSCHUTZ

Punkt 3 Datenspeicherung-Aufbewahrungspflichten

10 Jahre aufbewahren

- Bücher, Journale, Konten

- Jahresabschlüsse, Lageberichte, Eröffnungsbilanzen und Inventare mit den zu ihrem Verständnis erforderlichen Unterlagen

- Buchungsbelege, z.B. Rechnungen, Bescheide, Zahlungsanweisungen, Reisekostenabrechnungen, Bewirtungsbelege, Kontoauszüge, Lohn- bzw. Gehaltslisten

6 Jahre aufbewahren

- Lohnkonten und Unterlagen (Bescheinigungen) zum Lohnkonto

- sonstige für die Besteuerung bedeutsame Dokumente (z. B. Ausfuhr- bzw. Einfuhrunterlagen, Aufträge, Versand- und Frachtunterlagen, Darlehensunterlagen, Mietverträge, Versicherungspolicen) und Geschäftsbriefe

UNTERNEHMEN UND DATENSCHUTZ

Punkt 4 Datenlöschung

Nach Grundlage in § 35 BDSG hat der Betroffene einen Anspruch auf Berichtigung, Löschung und Sperrung von Daten

- Begriff der personenbezogenen Daten nach § 3 Abs.1
- Pflicht, Daten zu löschen, § 35 Abs. 2 Nr. 1 bis 3
- Besonderheiten bei Auskunfteien und geschäftsmäßiger Datenerhebung und Datenspeicherung
- Besondere Regeln für die Bewertung von Kreditwürdigkeit
- Unterrichtungspflicht bei abgelehnten Verbraucherdarlehensverträgen

UNTERNEHMEN UND DATENSCHUTZ

Punkt 4 Pflicht zur Datenlöschung

- **Unzulässig gespeicherte personenbezogene Daten** : sofort

- **Daten werden für eigene Geschäftszwecke verarbeitet**: keine Löschung, aber dann wenn Speicherung nicht mehr notwendig dafür: sofort; außer es gibt Aufbewahrungspflichten

-**Daten werden geschäftsmäßig zum Zweck der Übermittlung verarbeitet** (Auskunfteien): am Ende des 4. des auf die erstmalige Speicherung folgenden Kalenderjahres Prüfung, ob Speicherung länger erforderlich, erledigte Sachverhalte (Kredit abbezahlt-Schufa): Prüfung nach 3. Jahr.

-**Daten, die zu löschen wären, jedoch die Löschung ist wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich**: Sperrung der Daten ausreichend

UNTERNEHMEN UND DATENSCHUTZ

Punkt 5 Datenübernahme Facebook (& Co.)

Die Datenübernahme von einem firmenfremden Account (zB Facebook) erfolgt ähnlich wie die Verwendung von Facebook Plugins

Erfordernis einer Einwilligungserklärung
- bei Facebook +
- beim Unternehmen, bei dem der Login-Vorgang erfolgt

E-Mail-Einwilligung: Erfordernis des **Double opt in**, daher Verifizierung der Emailadresse durch Aktivierungslink, sonst unzulässige Verwendung der Emailadresse (neben Verstoß gegen BDSG auch Abmahngefahr wegen unverlangter Werbung gem. § 7 II Nr. 2 UWG)

UNTERNEHMEN UND DATENSCHUTZ

Punkt 6: Einwilligung: Cookies

Der Nutzer muss in der datenschutzrechtlichen Einwilligungserklärung über den Einsatz von Cookies informiert werden

Inhalt:

- Information über die technische Nutzung von Cookies und Informationen zu Tracking von Nutzerverhalten

- Information über den Einsatz von Social Plugins (zB Facebook)

- Nach Umsetzung der Richtlinie 2009/136/EG über den Schutz personenbezogener Daten („Cookie-Richtlinie oder E-Privacy Richtlinie)

    - Bei Cookies bei denen personenbezogene und pseudonyme Daten gesammelt werden Einwilligung erforderlich;

    - Verwendung von Cookies im Onlineshop zur Optimierung des Bestellprozesses bleibt zulässig.

UNTERNEHMEN UND DATENSCHUTZ

Punkt 7 Auskunftsanspruch

Gemäß § 34 BDSG steht dem Betroffenen ein kostenloses Auskunftsrecht zu, über

- die zu seiner Person gespeicherten Daten und Herkunft der Daten

- Empfänger, an die Daten weitergegeben werden und

- Zweck der Speicherung

Voraussetzung: formloses Auskunftsersuchen

Frist für Auskunftserteilung: unverzüglich, dh ca. zwei Wochen angemessen, sonst Zwischenbescheid erforderlich

Rechtsfolge bei Verstoß: **OWi (§ 43** I Nr. 8a,b,c, II **BDSG: Bußgeld bis zu 50.000 €)**

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8

Sonderthemen

a) Technische Daten

b) Financial Services

c) Devices

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8a Technische Daten

- Schutz der Daten durch erhebende Stelle oder Auftragsdatenverarbeiter durch technische und organisatorische Maßnahmen (§ 9 BDSG)
- Gewährleistung der gesetzlichen Anforderungen (Anlage zu § 9 Satz1)
- 8-Punkte-Katalog:

  Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle sowie Kontrolle der getrennten Verarbeitung bei unterschiedlicher Zweckbindung
- Datenschutz-Audits nach § 9a BDSG zur Verbesserung des Datenschutzes und der Datensicherheit mit Bezug auf Datenschutzkonzept sowie technische Einrichtungen

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8a Technische Daten

Konkrete Vorgaben der Anlage des § 9 BDSG

1. Zutrittskontrolle (Hochsicherheitstrakt, Key Card)
2. Zugangskontrolle (Passwörter)
3. Zugriffskontrolle (funktionsgebundener Zugriff)
4. Weitergabekontrolle (Verschlüsselungsverfahren)
5. Eingabekontrolle (Sicherheitssoftware)
6. Auftragskontrolle (Protokollierung von Anweisungen)
7. Verfügbarkeitskontrolle (Brandschutz)
8. Datentrennungskontrolle (Datenseparierung)

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8a Technische Daten

Anlage des § 9 BDSG

1. Zutrittskontrolle

Ziel, Unbefugten den körperlichen Zugang zu Datenverarbeitungsanlagen zu verwehren

Sicherstellung durch Kontrolle des Zugangs und Absicherung der Zugangswege

Maßnahmen (nicht abschließend):

- Zutrittsberechtigung der Benutzer für die Räumlichkeiten
- automatische Abmeldungen des Terminals nach längerer Untätigkeit
- Berechtigungsausweise/Besucherausweise
- Einrichtung von Sicherheitsbereichen
- Bewachungsanlagen/-personal

Punkt 8a Technische Daten

Anlage des § 9 BDSG

2. Zugangskontrolle

Ziel, die Benutzung von Datenverarbeitungssystemen durch Unbefugte zu verhindern

Sicherstellung durch Festlegung von Benutzerrechten

Maßnahmen (nicht abschließend):

- sicheres Passwortverfahren und Benutzerkennung
- Verschlüsselung
- Protokollierung unerlaubter Aktivitäten der Benutzer
- Verzicht auf Zugriff über Wählleitung

Punkt 8a Technische Daten

Anlage des § 9 BDSG

3. Zugriffskontrolle

Ziel, den Zugriff der Benutzer eines Datenverarbeitungssystems ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zu beschränken

Sicherstellung durch Beschränkung des Zugriffs auf Daten, die zur konkreten Aufgabenerfüllung erforderlich sind

Maßnahmen (nicht abschließend):

- sicheres Passwortverfahren und Benutzerkennung
- Zuordnung der Benutzer zu bestimmten Terminals, Festlegung der Befugnisse
- Protokollierung unerlaubter Aktivitäten der Benutzer
- zeitliche Begrenzung der Zugriffsmöglichkeit

Punkt 8a Technische Daten

Anlage des § 9 BDSG

4. Weitergabekontrolle

Ziel, die unbefugte Bearbeitung (Lesen Kopieren, Löschen) von Daten zu verhindern

Sicherstellung sicherer Übertragung von personenbezogenen Daten und sicherem Transport von Datenträgern

Maßnahmen (nicht abschließend):

- Kontrolle der Datenübertragungsprogramme, Protokollierung von Datenübertragungen
- Verschlüsselung der Daten und verschlüsselter Transportweg (VPN)
- schriftliche Regelungen über Umgang mit Datenträgern
- Protokollierung des Verbleibs von Datenträgern
- Verbot der Verwendung privater Datenträger
- Verbot der Mitnahme dienstlicher Datenträger nach Hause

Punkt 8a Technische Daten

Anlage des § 9 BDSG

5. Eingabekontrolle

Ziel, nachträglich feststellen zu können, welche Daten zu welchem Zeitpunkt von wem eingegeben worden sind

Sicherstellung durch maschinelle Aufzeichnungen und sonstige Unterlagen (keine ständige Protokollierung angemessen und somit erforderlich)

Maßnahmen (nicht abschließend):

- Programmgesteuerte Festlegung der Befugnisse zur Kenntnisnahme, Eingabe etc.
- Passwortverfahren, Benutzerkennung
- Protokollierung von Eingaben, Zugriffen und Zugriffsversuchen
- Einsatz von Sicherheitssoftware
- Vermerk der Eingabe in den Erfassungsunterlagen (z.B. durch Handzeichen)

Punkt 8a Technische Daten

Anlage des § 9 BDSG

6. Auftragskontrolle

Ziel, dass im Auftrag verarbeitete Daten nur entsprechend den jeweiligen Weisungen verarbeitet werden

Maßnahmen (nicht abschließend):

- Protokollierung der jeweiligen Anweisungen
- Abgleich der jeweiligen Verarbeitung mit den darauf bezogenen Anweisungen

7. Verfügbarkeitskontrolle

Ziel, Schutz der Daten vor zufälliger Zerstörung (Wasserschäden, Brand)

Sicherstellung durch entsprechende Sicherheitsvorkehrungen

Maßnahmen (nicht abschließend):

- Auslagerung von Sicherheitskopien
- Erstellung von Katastrophenplänen

Punkt 8a Technische Daten

Anlage des § 9 BDSG

8. Trennungskontrolle

Ziel ist die technische Sicherstellung der zweckbestimmten Verarbeitung

Sicherstellung durch Trennung (keine zwingende räumliche Trennung, logische Trennung genügt)

Maßnahmen (nicht abschließend):

- Softwaremäßige Mandanten-/Kundentrennung
- Trennung über Zugriffsregelungen

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8b Financial Services

- Für IT-Outsourcing im Finanzbereich sind die Vorschriften des KWG zu beachten: Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten, Notfallkonzept

- Def. nach 25 a Abs. 2 KWG (Kreditwesengesetz) : Die „Auslagerung von Aktivitäten und Prozessen auf ein anderes Unternehmen, die für die Durchführung von Bankgeschäften, Finanzdienstleistungen oder sonstigen institutstypischen Dienstleistungen wesentlich sind“

- IT-Outsourcing erfolgt idR über Auftragsdatenverarbeitung: Hier sind die Vorschriften des § 11 BDSG zu beachten, insbesondere die Regeln zur grenzüberschreitenden Datenübermittlung. Beachtung Bankgeheimnis vereinbaren

- Falls ein selbständiges Finanzunternehmen nur Kooperationspartner ist (keine Auftragsdatenverarbeitung nach § 11 BDSG), richtet sich die Datenübermittlung nach den Vorschriften wie unter fremden Unternehmen

UNTERNEHMEN UND DATENSCHUTZ

Punkt 8c Einsatz von Mobile Devices

Risiken beim Einsatz von Mobile Devices (z.B. Tablets und Smartphones)

-Erleichterung von Angriffen auf Infrastruktur

-Einschleusen von Viren und Trojanern sowie Schadsoftware

-Gefahren durch Einsatz von Apps Dritter

-Cloud-Dienste mit weit reichenden Rechten (z.B. Zugang zu Adressbüchern)

-Durchgängige datenschutzkonforme Sicherheitsarchitektur (z.B. Einsatz von Verschlüsselungsverfahren)

-Auftragsdaten-Vereinbarungen mit anderen Stellen (§ 11 BDSG)

UNTERNEHMEN UND DATENSCHUTZ

Unternehmen und Datenschutz

Wall&Kollegen Karlsplatz 7
80335 München

FON 089 30 90 589-0
FAX 089 30 90 589-11