Anwendungsbereich der DSGVO

Ein US-Unternehmen (Verantwortlicher) beauftragt ein deutsches Rechenzentrum (als Auftragsverarbeiter) mit der Speicherung seiner US-Kundendaten/Mitarbeiterdaten auf Servern in Deutschland.

Ist die DSGVO auf das US-Unternehmen anwendbar?

- Art. 3 Abs. 1 DSGVO: Nein, weil das deutsche Unternehmen keine „Niederlassung“ des US-Unternehmens ist
- Art. 3 Abs. 2 DSGVO: Nein, weil es nicht um „betroffene Personen in der EU“ geht

Ist die DSGVO auf das deutsche Rechenzentrum anwendbar?

- Art. 3 Abs. 1 DSGVO: Ja, weil Verarbeitung im Rahmen der Niederlassung eines Auftragsverarbeiters in der EU

Die US-Muttergesellschaft (Verantwortlicher) beauftragt seine deutsche Tochtergesellschaft (als Auftragsverarbeiter) mit der Speicherung von US-Kundendaten/Mitarbeiterdaten auf Servern in Deutschland.

Ist die DSGVO auf das US-Unternehmen anwendbar?

- Art. 3 Abs. 1 DSGVO: Ja, weil das deutsche Unternehmen (da Tochtergesellschaft) eine „Niederlassung“ des US-Unternehmens ist.
- Art. 3 Abs. 2 DSGVO: Nein, weil es nicht um „betroffene Personen in der EU“ geht

Ist die DSGVO auf das deutsche Unternehmen anwendbar?

- Art. 3 Abs. 1 DSGVO: Ja, weil Verarbeitung „im Rahmen der Tätigkeit einer Niederlassung“ eines Auftragsverarbeiters in der EU
- D.h. das deutsche Unternehmen muss (als Auftragsverarbeiter) die DSGVO einhalten

Personenbezogene Daten

„über“ = „die sich auf … beziehen“

Die zuständige Behörde besteuert einen Immobilieneigentümer anhand des Wertes der Immobilie. Ist dieser Wert ein personenbezogenes Datum?

> Ja. Bei Verwendung in dieser Weise bezieht sich der Immobilienwert auf den Eigentümer.

Fotos vom Zustand einer Wohnung, die von der Hausverwaltung allen Eigentümern in betreffenden Eigentümergemeinschaft zur Verfügung gestellt werden.

> Personenbezogen, wenn die anderen Eigentümer den Eigentümer und/oder Bewohner der fotografierten Wohnung kennen.

Arzneimittelstudie: Arzt übermittelt pseudonymisierte Daten an den Hersteller des Arzneimittels. Liegen für den Arzt bzw. für den Hersteller personenbezogene Daten vor?

> Arzt: Ja, weil er den Schlüssel besitzt.
>
> Hersteller: Nein, wenn er den Schlüssel unter keinen Umständen erhalten kann.

Einwilligung

Übermittlung von Passagierdaten durch Airline an US-Behörden. Wäre eine Einwilligung der Passagiere freiwillig?

> Nein, da sonst Flug nicht angetreten werden kann (erheblicher Nachteil).

Arbeitgeber verlangt Einwilligung des Arbeitnehmers zu einer Videoüberwachung mit der Begründung, dass die Überwachung auch der Sicherheit des Arbeitnehmers dient. Freiwillig?

> Nein, da Über-/Unterordnungsverhältnis und mögliche Nachteile bei Verweigerung der Einwilligung.

Kundenbindungsprogramm („Kundenkarte“), Einwilligung zum Erhalt von Werbung auf Basis der Auswertung der Einkaufsgewohnheiten als Gegenleistung für Preisvorteile. Freiwillig?

> In der Regel ja (nicht unumstritten): Anreize sollen nicht pauschal verboten werden.

Händler verlangt Einwilligung des Kunden für die Zusendung eigener Werbung und gleichzeitig für die Übermittlung der Kundenadresse an andere Händler für deren Werbezwecke. Wirksam?

> Nein, es wären getrennte Einwilligungen nötig, da zwei getrennte Zwecke.

Anklicken eines Kästchens auf Website zu einem vorformulierten Einwilligungstext?

> Ja, siehe auch Erwägungsgrund 32, ähnlich wenn ein vorformulierter Einwilligungstext unterzeichnet wird.

Nicht-Auskreuzen eines vor-angekreuzten Kästchens „Ich willige ein…“ (Opt-Out)?

> Nein, siehe Erwägungsgrund 32.

Anklicken eines Kästchens, mit dem die AGB „akzeptiert werden“?

> Nein, eine in AGB versteckte Einwilligung ist nicht wirksam, siehe Erwägungsgrund 42.

Nicht-Änderung von Browser-Voreinstellungen, die die Setzung von Tracking-Cookies

(Werbung!) ermöglichen?

> Nein, ist keine bewusste „Auswahl technischer Einstellungen“, siehe Erwägungsgrund 32.

Zweckbindung

Ein Unternehmen des öffentlichen Nahverkehrs macht bei seinen Busfahrern zu Beginn jeder Schicht Alkoholtests zur Prüfung der Fahrtauglichkeit. Die Fahrer werden mit einer ID-Karte identifiziert, es wird auch die Uhrzeit des Tests erfasst. Die Fahrer werden (nur) über diesen Zweck informiert. Darf der Arbeitgeber die erfasste Uhrzeit auch nutzen, um zu kontrollieren, ob die Fahrer ihre Arbeitszeit-Verpflichtung einhalten?

> Nein, das wäre ein ganz neuer Zweck, der mit dem ursprünglichen Zweck keine Verbindung hat („unvereinbar“).

Soziales Netzwerk mit Foto-Sharing-Funktion: Hochgeladene Fotos sollen nur für „Freunde“ sichtbar sein. Die Nutzer werden (zutreffend) nur über diesen Zweck der Verwendung der Fotos informiert. Später möchte der Netzwerk-Anbieter die Fotos künftig für werbliche Zwecke auswerten und ändert entsprechend die „Datenschutzbestimmungen“ für das Netzwerk. Ist der neue Zweck mit dem ursprünglichen vereinbar?

> Nein, Werbung ist ein völlig anderer Zweck als der ursprüngliche (Teilen der Fotos mit Freunden). Die Verarbeitung für Werbezwecke wäre nur mit Einwilligung zulässig, Art. 6 Abs. 4 DSGVO.

Datenschutzgrundsätze

In welchen Regelungen der DSGVO finden sich die folgenden Datenschutzgrundsätze wieder?

- Transparenz
  - Grundsätze, Art. 5 Abs. 1 lit. a) DSGVO
  - Transparente Information, Art. 12 DSGVO
  - Zertifizierung, Art. 42 DSGVO
  - Datenverarbeitung im Beschäftigungskontext, Art. 88 Abs. 2 DSGVO
- Zweckbindung
  - Grundsätze, Art. 5 Abs. 1 lit. b) DSGVO
  - Rechtmäßigkeit der Verarbeitung, Art. 6 Abs. 3 lit. b) DSGVO
  - Informationspflichten, Art. 13/14 Abs. 1 lit. c) DSGVO
  - Auskunftsrecht, Art. 15 Abs. 1 lit. a) DSGVO
  - Recht auf Berichtigung, Art. 16 DSGVO
  - Recht auf Löschung, Art. 17 Abs. 1 lit. a) DSGVO
  - DS-Folgeabschätzung, Art. 35 Abs. 1 DSGVO
  - Widerspruchsrecht, Art. 21 Abs. 3 DSGVO
  - Sicherheit der Verarbeitung, Art. 32 Abs. 1 DSGVO

- Datenminimierung & Datensparsamkeit
    - Art. 5 Abs. 1 lit. c) DSGVO
    - materialisiert sich in „privancy by design“ und „privacy by default“, Art. 25 DSGVO
    - „Pseudonymisierung“, Art. 4 Nr. 5 DSGVO
    - Sicherheit der Verarbeitung, Art. 32 Abs. 1 lit. a) DSGVO
- Verbot mit Erlaubnisvorbehalt
    - Art. 6 Abs. 1 DSGVO

Zulässigkeit der Datenverarbeitung

Der neugierige Arbeitgeber

A arbeitet als Paketzusteller bei DHL. Da es in der Vergangenheit im Unternehmen mehrfach zu unerlaubter Privatnutzung der Fahrzeuge sowie überflüssigen Parallelfahrten kam, sind alle Lieferwagen mit einem GPS-Ortungssystem ausgestattet worden.

Durch Herunterladen der zugehörigen kostenlosen App des Herstellers und Eingabe der auf den GPS-Trackern frei zugänglichen Seriennummer ist es möglich, die verschiedenen Kollegen jederzeit zu orten.

DHL behauptet nun, dass fast die gesamte Belegschaft „freiwillig“ in die Nutzung des GPS-Ortungssystems eingewilligt habe.

Zu Recht?

> Der Einsatz eines GPS-Ortungssystems durch das Unternehmen kann nicht auf die Einwilligung der Beschäftigten gestützt werden, da bei einer flächendeckenden Überwachung nicht von der erforderlichen Freiwilligkeit einer Einwilligung der Beschäftigten ausgegangen werden kann.
>
> Die Nutzung von Ortungssystemen, mit denen das Arbeitsverhalten von Beschäftigten dauerhaft kontrolliert wird, ist datenschutzrechtlich unzulässig, da Beschäftigte keineswegs einem permanenten Kontrolldruck ausgesetzt sein dürfen. Dies gilt nicht nur für die Überwachung durch den Arbeitgeber, sondern erst Recht durch die eigenen Kollegen.
>
> Nachstehende Punkte sind daher bei der Einführung und dem Betrieb des Ortungssystems von dem betroffenen Unternehmen zu beachten:
>
> - Schon bei der Planung und Ausgestaltung der Systeme ist der Grundsatz der **Datensparsamkeit** zu verfolgen: Nur die für die betrieblichen Zwecke wirklich erforderlichen Daten, nicht die überflüssigen, sind zu erheben. **Eine routinemäßige Ortung eines Fahrzeugs ist unzulässig, wenn sie unabhängig von den notwendigen Planungen erfolgt.** Der Einsatz von Ortungssystemen ist nicht erforderlich, wenn der Aufenthaltsort des Beschäftigten **auch anders** (etwa durch einen Anruf) erhoben werden kann.
> - **Die Zweckbestimmung muss klar dokumentiert und gegenüber den Beschäftigten in transparenter Weise kommuniziert werden.** Sie sind insbesondere über den Erhebungszweck und -umfang sowie über die

Auskunftsrechte hinsichtlich der gespeicherten Daten zu informieren. Entsprechend § 26 BDSG-neu sind die Beschäftigten, etwa durch eine Benachrichtigung oder eine Leuchtanzeige am Gerät, darüber in Kenntnis zu setzen, wann eine Ortung erfolgt. Ansonsten liegt eine verbotene heimliche Überwachung der Mitarbeiter vor.

- Die Beschäftigten sind über die Regelungen der Zugangsberechtigung zu den gespeicherten Daten sowie der Protokollierung der Speicherung und der Festlegung der Speicherungsdauer der Daten zu informieren.

Kinderfotos bei Facebook & Co.

Mutter M lädt ein „Töpfchenfoto“ Ihrer mittlerweile 16-jährigen Tochter T bei Facebook hoch. Darf Sie das? Wie kann sich T dagegen wehren?

(P1) Alle Bilder, die Sie ins Netz stellen, können dort auch andere herunterladen bzw. über Screenshots speichern. Selbst wenn das Bild später wieder gelöscht wird, kann es längst auf zig Rechnern abgespeichert sein.

(P2) Was viele Eltern nicht wissen: Auch Kinder haben, wie jeder andere Mensch auch, ein Persönlichkeitsrecht. Sie haben ein Recht darauf, dass ihre Ehre nicht verletzt wird und nicht einfach Bilder von ihnen im Internet landen. Das Persönlichkeitsrecht ist auch nicht von einem Alter abhängig.

Die Folge des Persönlichkeitsrechts ist, dass Eltern ihre Kinder eigentlich vor der Veröffentlichung der Bilder um Erlaubnis fragen müssen.

Ganz kleine Kinder wissen nicht, was ihre Eltern tun. Juristen sprechen davon, dass den Kindern die „Einsichtsfähigkeit“ fehlt. Nach dem Gesetz tragen die Eltern nämlich die persönliche Sorge für das Kind und vertreten ihren Sprössling bei rechtlichen Angelegenheiten. Im Klartext heißt das: Für kleine Kinder können die Eltern selbst die Einwilligung in die Veröffentlichung der Bilder erteilen.

Achtung: Wenn die Kids die nötige „Einsichtsfähigkeit“ erreicht haben, können sie sich an der Entscheidung über die Veröffentlichung der Fotos beteiligen. Bei Kindern ab ca. 13 bis 14 Jahren kann man davon ausgehen, dass sie die nötige Einsicht und Reife haben.

In der Praxis gibt es so gut wie keine Fälle, in denen Kinder ihre eigenen Eltern wegen ungenehmigten Bildveröffentlichungen abmahnen oder verklagen.

Dennoch stehen den Kindern u.U. folgende Rechte zu:

- Beseitigung und Unterlassung
- Geldentschädigung
- Strafrechtliche Konsequenzen (KUG)

WhatsApp

Studentin S nutzt auf ihrem Smartphone „WhatsApp“ um mit ihren Freunden und Kollegen privat zu kommunizieren. Im Rahmen der Installation von WhatsApp muss S den AGB der WhatsApp Inc. zustimmen, in denen es u.a. heißt:

*„**Adressbuch.** Du stellst uns regelmäßig die Telefonnummern von WhatsApp-Nutzern und deinen sonstigen Kontakten in deinem Mobiltelefon-Adressbuch zur Verfügung. Du bestätigst, dass du autorisiert bist, uns solche Telefonnummern zur Verfügung zu stellen, damit wir unsere Dienste anbieten können.“*

Wie beurteilt sich die Situation aus Datenschutzsicht?

Abwandlung: S nutzt WhatsApp, um dienstlich mit Ihren Kollegen zu kommunizieren. Dabei versendet sie auch Dateianhänge.

Nach Art. 2 Abs. 2 DSGVO findet die **DSGVO keine Anwendung** auf die Verarbeitung personenbezogener Daten, **wenn natürliche Personen ausschließlich persönliche oder familiäre Tätigkeiten ausüben.**

➔ Das Verhalten der S ist datenschutzrechtlich unbedenklich.

Abwandlung: Für die Abwandlung gilt die Ausnahme des Art. 2 Abs. 2 DSGVO nicht, da WhatsApp geschäftlich genutzt wird. Die DSGVO ist anwendbar.

Die Datenverarbeitung bedarf daher einer Rechtsgrundlage oder einer Einwilligung. Eine Rechtsgrundlage ist nicht ersichtlich. Zwar kann in der gegenseitigen Mitteilung der Mobilfunknummern und deren Speicherung eine konkludente Einwilligung gesehen werden; nachweisbar ist diese aber nicht.
Zusätzlich: **Auftragsverarbeitung** – Voraussetzungen des Art. 28 DSGVO liegen nicht vor – **unzulässig!**

Exkurs: Klausel der AGB ist überraschende Klausel i.S.d. § 305c Abs. 1 BGB – wird nicht Vertragsbestandteil!
Denn: Man kann WhatsApp faktisch gar nicht wirklich nutzen, ohne mehr oder weniger bewusst gegen die AGB zu verstoßen.

Datentransfer ins Ausland

Konzernprivileg?

Unternehmen Z gehört einem Unternehmensverbund an. Im Zuge der Globalisierung wurde die Unternehmenszentrale nach New York/ USA verlegt. Es ist deshalb erforderlich, die Beschäftigtendaten des gesamten Unternehmensverbunds an die neue Unternehmenszentrale zu übermitteln.

Was ist aus Sicht des Datenschutzes zu beachten?

In Art. 4 Nr. 19 DSGVO findet sich eine Definition des Begriffs des Konzerns („Unternehmensgruppe“):

> *„eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht”.*

Der **konzerninterne Datenaustausch** auf gesetzlicher Grundlage wird durch die DSGVO erheblich **vereinfacht und erleichtert:**

- Er richtet sich im Wesentlichen nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO („berechtigte Interessen“), wobei
- bei sensitiven Daten zusätzlich die Anforderungen des Art. 9 DSGVO zu beachten sind.

Der **konzerninterne Datenaustausch** ist durch **Erwägungsgrund 48 Satz 1 DSGVO** als „berechtigtes Interesse“ **privilegiert**. Erwägungsgrund 48 Satz 1 DSGVO erkennt für den Konzern “interne Verwaltungszwecke” als ein “berechtigtes Interesse” an:

> *„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt. ”*

Erwägungsgrund 48 Satz 1 DSGVO erleichtert den konzerninternen Datenaustausch, stellt ihn jedoch nicht von sämtlichen **datenschutzrechtlichen Anforderungen** frei:

- Es bedarf jeweils gemäß Art. 6 Abs. 1 Satz 1 lit. f) DSGVO einer **Abwägung** mit entgegenstehenden schutzwürdigen Interessen der Betroffenen.
- Für den Transfer an konzernangehörige Unternehmen in Drittstaaten gelten die Anforderungen der **Art. 44 ff. DSGVO** (vgl. Erwägungsgrund 48 Satz 2 DSGVO). Hier werden sich **Binding Corporate Rules (BCR)** regelmäßig als Gestaltungsmittel anbieten, deren Aufstellung in **Art. 47 DSGVO** geregelt ist.

- Nach Wegfall des Privacy-Shields können alternativ nur **Standardvertragsklauseln mit zusätzlichen Maßnahmen** abgeschlossen werden; **Art 46 Abs. 2 c) DSGVO**

Würde sich Ihre Beurteilung des Sachverhalts ändern, wenn die Konzernzentrale in Dublin, Irland wäre?

Datenübermittlung innerhalb EU = Datenübermittlung innerhalb Mitgliedsstaat

➔ Rechtsgrundlage erforderlich (vgl. Artikel 6 bzw. 9 DSGVO) erfolgen

Der **konzerninterne Datenaustausch** auf gesetzlicher Grundlage wird durch die DSGVO erheblich **vereinfacht und erleichtert:**

- Er richtet sich im Wesentlichen nach Art. 6 Abs. 1 Satz 1 lit. f DSGVO („berechtigte Interessen"), wobei
- bei sensitiven Daten zusätzlich die Anforderungen des Art. 9 DSGVO zu beachten sind.