PSP

PETERS, SCHÖNBERGER & PARTNER

M B B

RECHTSANWÄLTE WIRTSCHAFTSPRÜFER STEUERBERATER

Teil 1:

Praxisrelevante Beispielsfälle und die Unbestimmtheit der DSGVO-Regelungen

1. Stellt das „Übermittelterhalten“ von personenbezogenen Daten ein „Erheben“ dar?

Praktischer Fall: Herr Müller, Einkäufer des Unternehmens Huber AG, übergibt einem Vertriebsmitarbeiter des Unternehmens Maier GmbH, Herrn Schulze, eine Visitenkarte von sich mit den Worten „Wenn Sie mal das Produkt X in Richtung Y weiterentwickeln, dann rufen Sie mich an“.

2. Wie muss ein Verantwortlicher mit besonderen Kategorien personenbezogener Daten von Bewerbern umgehen?

Praktischer Fall: Die Huber AG hat ein „Funktionspostfach“ (bewerbung@huber-ag-online.de) für die Zusendung von Bewerbungen eingerichtet, das bei allen Online-Stellenanzeigen genannt wird. In diesem Zusammenhang wird auch auf die Pflichthinweise der Art. 12, 13 DSGVO in der Datenschutzerklärung auf der Website hingewiesen, die die für eingereichte Bewerbungen maßgeblichen Informationshinweise enthalten. Die Datenschutzerklärung nennt als Rechtsgrundlage für die Verarbeitung der personenbezogenen Daten in der Bewerbung die Erforderlichkeit für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses (§ 26 Abs. 1 S. 1 BDSG). Frau Maier sendet der Huber AG eine E-Mail mit Ihrer Bewerbung, welche neben einem Foto auch die Angabe enthält, dass Frau Maier zu 60% schwerbehindert ist.

3. Inwieweit muss die Belehrung eines Mitarbeiters auf seine Position hin individualisiert werden?

Praktischer Fall: Frau Maier wird am Ende des Bewerbungsverfahrens von der Huber AG als Lohnbuchhalterin eingestellt. Sie erhält eine Formular-Belehrung, dass sie im Rahmen ihrer Arbeit mit personenbezogenen Daten zu tun haben wird und das Datenschutzrecht einhalten muss.

4. Laufende Daten während des Beschäftigungsverhältnisses

Praktischer Fall: Frau Maier ist in der Lohnbuchhaltung der Huber AG tätig. Die Buchhaltungssoftware zeichnet bei jeder Veränderung, die Frau Maier an den Datensätzen vornimmt, mit einem Zeitstempel auf, dass Frau Maier Änderungen vorgenommen hat. Dies wird bei Aufruf des Datensatzes, gleich durch wen, mit dem Zusatz „zuletzt bearbeitet von Maier am [Datum], [Uhrzeit]“ angezeigt. Frau Maier macht nach drei Jahren Betriebszugehörigkeit einen Auskunftsanspruch gegen die Huber AG geltend, welche personenbezogenen Daten von ihr gespeichert werden, und verlangt nach ihrem Austritt aus dem Unternehmen, dass diese in der Buchhaltungssoftware aufgezeichneten Daten gelöscht werden.

5. Muss dem Gegner bei Weitergabe des Falles an eine Konzernrechtsabteilung diese Übermittlung mitgeteilt werden?

Praktischer Fall: Die Maier GmbH ist eine Tochtergesellschaft der Huber AG. Herr Müller, Einkäufer bei der Maier GmbH, überlegt, Herrn Schulze, einen freiberuflichen Programmierer, der für die Maier GmbH Software programmiert hat, auf Herausgabe des Sourcecodes zu verklagen. Um die Angelegenheit rechtlich prüfen zu lassen, sendet er die maßgeblichen Informationen, darunter auch Namen und Korrespondenz mit Herrn Schulze, an die Rechtsabteilung der Huber AG.

6. Müssen auch interne Übermittlungsempfänger im Rahmen der Pflichthinweise angegeben werden?

Praktischer Fall: Die Huber AG klärt ihre Kunden, an die sie ihre Produkte veräußert, darüber auf, dass deren Daten mit Ausnahme von Transportdienstleistern nicht an Dritte weitergegeben werden. Die Kunden der Huber AG sind teils Unternehmen, teils natürliche Personen. Intern haben sämtliche Abteilungen der Huber AG auf die Kundendaten Zugriff, etwa die Verkaufsabteilung, die Buchhaltung, das Controlling, die Marketing-Abteilung, die Personalabteilung und die Abteilung zur Verwaltung der Huber-AG-eigenen Immobilien.

7. Wann liegt Auftragsverarbeitung vor, wann nicht?

Praktischer Fall: Die Lohnbuchhaltung eines Unternehmens wird an einen Steuerberater ausgelagert, der aber für das Unternehmen auch Steuererklärungen erstellt und einreicht.

Alternativ: Die Personalverwaltung eines Tochterunternehmens wird an eine zentrale Abteilung der Konzernmutter ausgelagert und in diesem Rahmen werden einzelne Fälle auch arbeitsrechtlich begutachtet.

8. Wie lange „hält“ die Interessenabwägung beim Direktmarketing?

Praktischer Fall: Die Huber AG betreibt eine CRM-Datenbank mit Kontaktdaten von Ansprechpartnern. Teils handelt es sich um Repräsentanten von Unternehmen, mit denen die Huber AG in Geschäftsbeziehung stand, steht oder gerne stehen würde. Teils handelt es sich um soziale oder politische Kontakte, etwa der Vertreter von Vereinen, die von der Huber AG gesponsert werden, oder von Personen des öffentlichen Lebens, mit denen die Huber AG den Kontakt pflegt. Solche Kontaktdaten ergeben sich aus E-Mail-Verkehren, Visitenkartenübergaben, Telefonaten und Ähnlichem. Die Huber AG geht davon aus, aufgrund ihres Interesses an Direktmarketing (hierzu zählt nicht nur kommerzielle Kommunikation im engeren Sinne, d. h. Werbung) die entsprechenden Daten aufgrund einer Interessenabwägung verarbeiten zu dürfen.

9. Ist das Schutzniveau der DSGVO verzichtsfähig?

Praktischer Fall: Siehe oben zu 2): Frau Maier sendet der Huber AG eine (unverschlüsselte) E-Mail mit Ihrer Bewerbung, welche neben einem Foto auch die Angabe enthält, dass Frau Maier zu 60% schwerbehindert ist.

Alternativ: Der Mandant sendet dem Anwalt verschiedene Unterlagen zu einem anstehenden Klageverfahren per E-Mail, der Anwalt beantwortet dies mit einem Schriftsatzentwurf per E-Mail an den Mandanten. Ggf. hat der Mandant im Rahmen der Begründung des Mandatsverhältnisses eine Erklärung unterzeichnet, dass ihm die Gefahren unverschlüsselten E-Mail-Verkehrs bekannt sind, er aber trotz dieser Gefahren unverschlüsselt E-Mails mit seinem Anwalt austauschen möchte.

10. Übermittlung in Drittländer: Beispiel Unternehmenskontakte

Praktischer Fall: Die Dow Inc. mit Sitz in den USA möchte Aktien an der Huber AG erwerben. Im Rahmen der Transaktion wird eine Unternehmensprüfung (Due Diligence) bei der Huber AG durchgeführt und zu diesem Zweck eine Liste erstellt, wer bei der Huber AG für welches Thema im Rahmen der Due Diligence als Ansprechpartner fungiert (Umwelt, IT, Produktion, Controlling, Steuern etc.). Die Liste, die Name, E-Mail-Adresse, Telefonnummer bei der Huber AG und Mobiltelefonnummer enthält, wird der Dow Inc. und ihren Beratern zur Verfügung gestellt.

11. Die Crux mit den „Verarbeitungsvorgängen“

Praktischer Fall: Die Huber AG erarbeitet ihr Verarbeitungsverzeichnis (Art. 30 DSGVO). Wie jedes Unternehmen verarbeitet sie Personaldaten der bei ihr beschäftigten Mitarbeiter. Wie viele „ Verarbeitungstätigkeiten“ umfasst die Verarbeitung von Personaldaten?

12. Die Datenkette

Praktischer Fall: Die Huber AG wurde von einer freiberuflichen Übersetzerin, Frau Schmidt, angeschrieben, der anbot, Übersetzungsdienstleistungen zu erbringen. Die Huber AG hat die Daten von Frau Schmidt daher in ihre Kontaktdatenbank übernommen und ihr Pflichthinweise nach der DSGVO zukommen lassen. Einige Zeit später erhielt die Huber AG ein Schreiben von Frau Schmidt, die mitteilte, sie sei nicht mehr als freiberufliche Übersetzerin tätig und die Huber AG möge bitte sämtliche personenbezogenen Daten über sie löschen. Dieses Schreiben gelangte bei der Huber AG nicht an die zuständige Stelle; die Daten wurden nicht gelöscht. Einige Zeit später fragt eine Tochtergesellschaft der Huber AG, die Müller GmbH, an, ob die Huber AG einen Übersetzer benennen könne. Die Huber AG gibt die Daten von Frau Schmidt an die Müller GmbH weiter.

13. Die Website als Flickenteppich

Praktischer Fall: Die Huber AG hat einen Online-Auftritt. Jeder Browser eines Internet-Nutzers, der die Website der Huber AG aufruft, wird durch den Code der Website zunächst dazu veranlasst, einen Zeichensatz (Font) – Teil der „corporate identity" der Huber AG – von Google-Servern nachzuladen. Weiter wird der Browser dazu veranlasst, bestimmte Java-Funktionsbibliotheken von Drittservern nachzuladen. Diese „Drittdatenquellen", welche der Browser abfragen muss, um die Website der Huber AG überhaupt darstellen zu können, erhalten vom Browser verschiedene Informationen, insbesondere die IP-Adresse des Rechners, auf dem der Browser läuft. Die Dritten haben ihr Einverständnis gegeben, dass ihre Seiten als „Drittdatenquellen" fungieren können, betreiben aber umfangreiches Tracking (Aufbau von Nutzerprofilen) mithilfe der Browser-Daten. Die Huber AG macht sich dazu keine Gedanken.

14. Wie tief schaut die DSGVO?, oder: Granularität

Praktischer Fall: Die Huber AG bewahrt Personalakten bis 10 Jahre nach dem Ausscheiden auf. Diese Angabe findet sich auch im Verarbeitungsverzeichnis sowie in den Pflichthinweisen gegenüber den Beschäftigten, die diesen zu Beginn des Anstellungsverhältnisses übergeben werden. Begründet wird dies damit, dass z. B. die in der Personalakte befindlichen Lohnabrechnungen entsprechenden steuerlichen Aufbewahrungsfristen unterliegen.

Teil 2:

Personenbezogene Daten auf Rechnungen

Muss das Datenschutz-Compliance-Management auch auf Rechnungen angewandt werden?

Welche personenbezogene Daten enthält eine Rechnung?

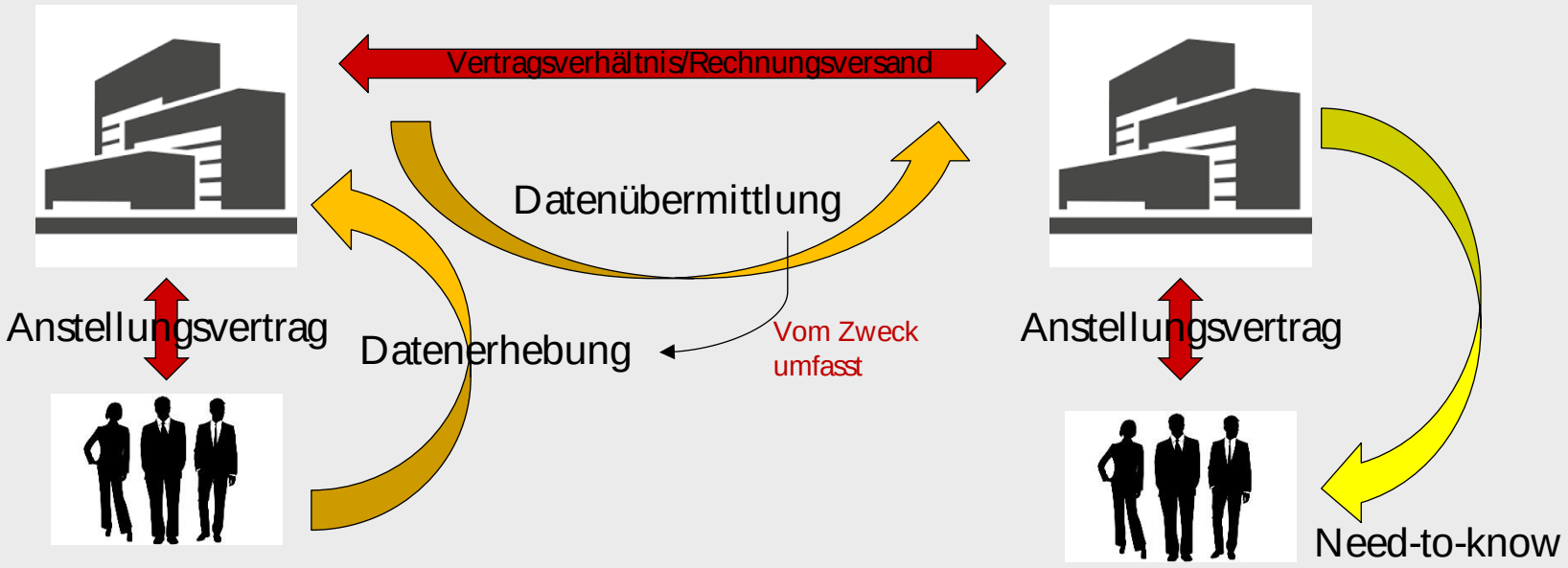
- **B2B-Eingangsrechnung und B2B-Ausgangsrechnung**
  - Briefkopfangaben des absendenden Unternehmens
  - Sachbearbeiter (Unternehmensangehörigkeit)
  - Betriebliche E-Mail-Adresse und betriebliche Durchwahl des Sachbearbeiters
  - Möglicherweise personenbezogene Daten in den Rechnungspositionen (Beispiel: „ Maßanfertigung Rollstuhl Herr XY“ in einer B2B-Lieferkette)
  - Möglicherweise personenbezogene Daten in Anlagen (Beispiel: Einzelverbindungsnachweis in Telefonrechnung für Mobiltelefon eines Mitarbeiters)
- **Zusätzlich B2C-Ausgangsrechnung**
  - Adressat (Privatperson)
  - Rechnungspositionen als personenbezogene Daten bezüglich des Empfängers (Privatperson)

Wie greift die DSGVO diese personenbezogenen Daten auf?

- **Gesetzliche Archivierungspflichten haben Vorrang** - Was archiviert werden muss, darf datenschutzrechtlich archiviert (d. h. weiterhin gespeichert) werden
- **Aber: Die personenbezogenen Daten unterliegen gleichwohl im Grundsatz dem „Regime des Datenschutzes" mit seinen spezifischen Problemstellungen, z. B.**
  - Es bedarf einer **datenschutzrechtlichen Legitimationsgrundlage** für die Aufnahme der personenbezogenen Daten in die Rechnung (z. B. das Beschäftigungsverhältnis im Falle von Mitarbeiterdaten wie Durchwahl, E-Mail)
  - **Zweckbindung beachten** (wenn eine Speicherung nur noch zu Zwecken der Erfüllung der gesetzlichen Aufbewahrungsfrist stattfindet, ist der Zugriff zu sperren)
  - Stellt der Empfang der Rechnung eine **Erhebung** der darin enthaltenen personenbezogenen Daten durch das rechnungsempfangende Unternehmen dar (dann Informationspflichten gegenüber dem Betroffenen) oder eine **Übermittlung** der Daten durch das rechnungsabsendende Unternehmen (dann wohl keine Informationspflichten, soweit in der Übermittlung als Teil der Rechnungen keine Zweckänderung liegt)?
  - **Pseudonymisierung** durch Absender („Maßanfertigung Rollstuhl Kunde 715" in der B2B-Lieferkette) möglich?
  - Die **Betroffenenrechte** (Auskunft, Berichtigung, Löschung etc.) beziehen sich auch auf die Daten in der Rechnung und die Übermittlung muss vom Übermittelnden protokolliert werden.

PSP MÜNCHEN

Datenfluss


Vertragsverhältnis/Rechnungsversand
Datenübermittlung
Anstellungsvertrag
Datenerhebung
Vom Zweck umfasst
Anstellungsvertrag
Need-to-know

Personenbezogene Daten auf Rechnungen – Rechtliche Prämissen

- **Öffentlich verfügbare personenbezogene Daten** unterliegen denselben Regelungen wie alle anderen personenbezogene Daten auch („*one size fits all*“ – auch in Bezug auf die Daten). Das Argument, dass diese Daten auch „anderswo verfügbar“ wären, kann daher die Anwendbarkeit der DSGVO nicht ausschließen.
- Es gibt in der DSGVO **keine Sonderregelungen** dafür, dass personenbezogene Daten „eigentlich gar nicht Gegenstand der Verarbeitung sind“, sondern dass diese als „aufgedrängte Daten“ bzw. „unverlangt zugesandte Informationen“ zum Verantwortlichen gelangen und dort gespeichert werden. In der Literatur finden sich im Zusammenhang mit dem Begriff der „Erhebung“ Aussagen wie
  - „*Nicht „erhoben“ werden Daten, die man nur bei Gelegenheit einer sonstigen Geschäfts- oder Verwaltungstätigkeit zur Kenntnis nimmt oder die einem aufgedrängt werden; hier kommt es zur Verarbeitung iSv Art. 4 Nr. 2 erst, wenn diese Daten auf einem Datenträger fixiert, also erfasst werden.*“
  - „*An dem von dem Begriff des Beschaffens geforderten aktiven und subjektiven Element fehlt es, wenn die Daten von dem Betroffenen selbst oder von Dritten ohne Aufforderung geliefert werden, dh der verantwortlichen Stelle „zuwachsen“. In diesen Fällen ist keine Erhebung gegeben, sondern handelt es sich um eine aufgedrängte Bereicherung bzw. Information. Sie wird datenschutzrechtlich erst dann relevant, wenn der Empfänger sie verarbeiten oder nutzen will. Insoweit müssen dann für diese Formen des Datenumgangs die gesetzlichen Voraussetzungen vorliegen.*“

PSP MÜNCHEN

Risikoabwägung in der DSGVO

- **Art. 24 DSGVO**
  - „Der Verantwortliche setzt **unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen** geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."
- **Art. 32 DSGVO**
  - „**Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen** treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten."
- **Abwägungsmerkmale**
  - Öffentliche Verfügbarkeit (Handelsregister: Briefkopfangaben)
  - Geringe Sensitivität der Daten im Sinne der Folgen bei „Datenpannen" (nur unternehmensbezogene Daten, keine „Privatdaten")
  - Grenzen der Zumutbarkeit (Aufwand und Kosten stehen außer Verhältnis zum Nutzen)

PSP MÜNCHEN

Personenbezogene Daten auf Rechnungen – Lösungsmöglichkeiten

- **Für Briefkopf- und Sachbearbeiterangaben:**
  - Risikoabwägung ergibt, dass keine besonderen technischen und organisatorischen Maßnahmen zum Schutz notwendig sind
  - Aufnahme in Rechnung vom Beschäftigtenverhältnis (Außenwirkung der Position im Unternehmen – „Funktionsträger“) abgedeckt
  - Datenvermeidung: Versicherung des ausstellenden Unternehmens gegenüber dem empfangenden Unternehmen im zugrundeliegenden Vertrag, dass personenbezogene Daten auf Rechnungen zu unterlassen sind bzw. zumindest eine datenschutzrechtliche Legitimationsgrundlage für die Übermittlung / Verarbeitung / Speicherung sichergestellt ist (Betroffenenrechte lassen sich dadurch allerdings nicht ausschließen)?
- **Für Rechnungspositionen:**
  - Anonymisierung / Pseudonymisierung (in der Lieferkette) möglich?
  - Bedenken: Konflikt mit Nachprüfbarkeit z. B. im Rahmen einer Betriebsprüfung
- **Für Anlagen:**
  - Weglassen (z. B. Einzelverbindungsnachweis „abbestellen“ – Gebot der Datenminimierung!) oder pseudonymisieren
- Bei **B2C-Rechnungen** stellen die „Kundendaten“ ohnehin personenbezogene Daten dar, die DSGVO-gemäß zu verarbeiten sind

PSP MÜNCHEN

Personenbezogene Daten auf Rechnungen – Schlussbemerkung

- Wichtig ist es, die Abwägung nicht nur vorzunehmen, sondern die wesentlichen Aspekte und Gründe im Rahmen der Risikoabwägung sowie das Ergebnis der Risikoabwägung und die sich daraus ergebenden Folgen zu **dokumentieren**.
- Es ist **unklar**, wie sich Datenschutzbehörden und Gerichte zur Nachvollziehbarkeit einer Abwägung und zur Rechtmäßigkeit des Abwägungsergebnisses äußern, wenn ein Unternehmen in der Folge de facto davon absieht, einzelne DSGVO-Regelungen auf bestimmte Daten anzuwenden, und dies mit der „Nicht-Risikobehaftetheit" der betroffenen personenbezogenen Daten bzw. Verarbeitungsvorgänge begründet.

Vielen Dank für Ihre Aufmerksamkeit

Referent

Dr. Axel-Michael Wagner
Rechtsanwalt

Peters, Schönberger & Partner
Rechtsanwälte Wirtschaftsprüfer Steuerberater
Schackstraße 2
80539 München
Tel.: + 49 89 3 81 72 - 0
Fax: + 49 89 3 81 72 - 204
E-Mail: psp@psp.eu
Internet: www.psp.eu

PSP
MÜNCHEN