

Transfer von personenbezogenen Daten im (internationalen) Konzern?

1. Rahmenbedingungen	1
2. Prüfschritte im Unternehmen	2
a. Klären des Sachverhalts: Wer erhält Daten von wem?	2
b. Ist der Empfänger bzw. Abrufer der Daten eine andere juristische Person?	2
c. Gibt es eine Rechtsgrundlage für die Überlassung der Daten?	2
d. Und wenn der Empfänger in einem Drittstaat sitzt?	3
3. Zusammenfassung.....	4

1. Rahmenbedingungen

Es ist einer der wichtigsten Grundsätze im Datenschutzrecht: Jeder Umgang mit personenbezogenen Daten ist nur zulässig, wenn es dafür eine Rechtsgrundlage gibt („Verbot mit Erlaubnisvorbehalt“).

Das gilt auch, wenn Daten von einer Konzern-Gesellschaft an eine andere übermittelt werden. Es macht dabei übrigens keinen Unterschied, ob die Daten weitergegeben oder abgerufen werden (beispielsweise von Servern oder aus der Cloud).

Entscheidend ist, wem die jeweiligen Daten gehören.

Für jedes personenbezogene Datum muss es eine verantwortliche Stelle geben. Stellen wir uns eine Meier GmbH in Deutschland vor. Es könnte zum Beispiel sein, dass die Meier GmbH zur Wagner International gehört und ihre Personaldaten nicht auf eigenen Servern in einem eigenen Serverraum speichert, sondern Infrastruktur der Wagner International nutzt:

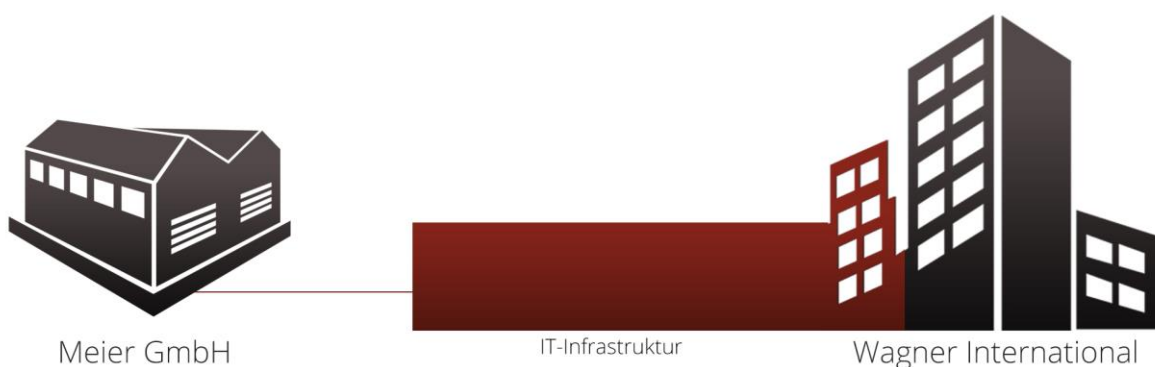


Abb. 1

Wagner International stellt IT-Infrastruktur zur Verfügung, die unter anderem von der Meier GmbH genutzt wird.

Andere (Konzern-) Unternehmen gelten aus datenschutzrechtlicher Sicht als „fremde Stellen“. Sie dürfen nur dann Daten erhalten, wenn es dafür eine datenschutzrechtliche Rechtsgrundlage gibt - das gilt in unserem Beispiel auch für die Wagner International. Noch etwas komplizierter wird es, wenn die Wagner International außerhalb Europas sitzen sollte.

2. Prüfschritte im Unternehmen

a. Klären des Sachverhalts: Wer erhält Daten von wem?

Wer ist „Eigentümer“ der Daten (verantwortliche Stelle)? An welche anderen Stellen werden die Daten übermittelt bzw. wer kann sie abrufen? Diese Fragen müssen für jede Kategorie von personenbezogenen Daten geklärt werden.

Die Klärung dieses Schritts kann viel Arbeit machen, ist aber unbedingt notwendig, um die datenschutzrechtliche Lage sauber zu klären. Wenn mehrere Unternehmen eines Konzerns involviert sind (Beispiel: Personaldaten aller Tochterunternehmen der Wagner International werden auf zentralen Servern gespeichert), sollte eine Übersicht in Matrix-Struktur erstellt werden, in der die einzelnen Zugriffsmöglichkeiten und -rechte festgehalten sind.

Bei der Vergabe von Zugriffsrechten spielen der Zweck und die Erforderlichkeit eine entscheidende Rolle: So benötigen beispielsweise Mitarbeiter der Meier GmbH vor Ort unter Umständen bestimmte private Kontaktdaten von Kollegen, um Vertretungen im Schichtdienst organisieren zu können. Das Management der Wagner International benötigt solche Daten jedoch in aller Regel nicht und sollte daher auch keinen Zugriff darauf haben.

b. Ist der Empfänger bzw. Abrufer der Daten eine andere juristische Person?

Gehört der Empfänger bzw. Abrufer zu einer anderen rechtlichen Person?

Wenn nicht, können Sie hier stoppen – ansonsten prüfen Sie weiter.

Beachten Sie, dass es keine Rolle spielt, ob das Unternehmen zum selben Konzern gehört oder völlig fremd ist: Im Datenschutz gibt es nach aktuell geltendem Recht kein Konzernprivileg: Jedes andere Unternehmen wird wie eine „fremde Stelle“ angesehen.

c. Gibt es eine Rechtsgrundlage für die Überlassung der Daten?

Die Daten dürfen nur dann übermittelt oder abgerufen werden, wenn das Datenschutzgesetz dies erlaubt. Dies ist für jeden Empfänger separat zu prüfen.

Wenn die Datenverarbeitung quasi outgesourct wird und das andere Unternehmen nach Weisung handelt, muss geprüft werden, ob die Voraussetzungen des § 11 BDSG (Auftragsdatenverarbeitung/ADV) vorliegen und eingehalten werden. Man kann sich das dann vorstellen wie einen klassischen Rechenzentrums-Betrieb durch einen Dienstleister.

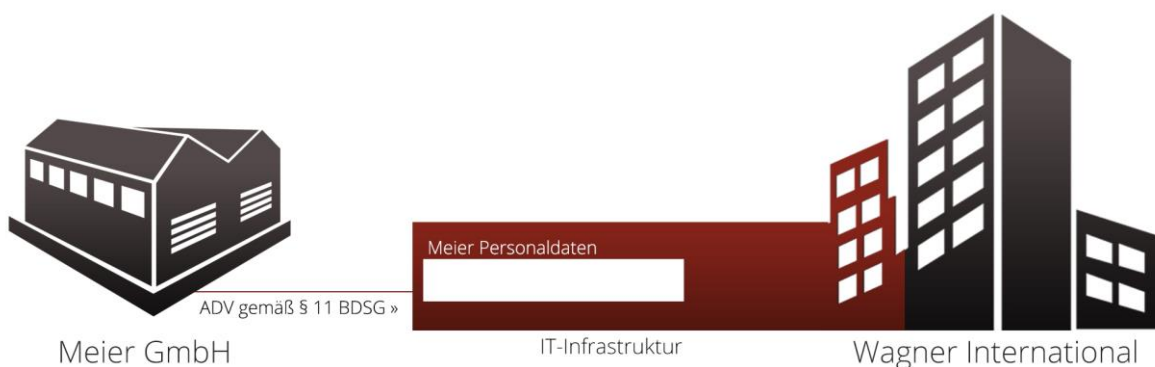


Abb. 2

Die Wagner International ist in dieser Konstruktion Auftragnehmer der Meier GmbH im Rahmen einer Auftragsdatenverarbeitung gem. § 11 BDSG.

In Betracht kommt auch § 32 BDSG (wenn Daten von Mitarbeitern übermittelt werden *müssen*, um die Pflichten aus dem Arbeitsvertrag erfüllen zu können) oder § 28 Abs. 2 Nr. 1 BDSG (wenn eine Abwägung ergibt, dass die berechtigten Interessen der Unternehmen schwerer wiegen als etwaige Schutzinteressen der Betroffenen – beispielsweise bei einer zentralen Führungskräftebetreuung und -entwicklung oder einem konzernweiten Skill-Management durch die Wagner International aus unserem Beispiel).

Unter Umständen gibt es hier auch Mischformen, d.h. die Wagner International stellt IT-Infrastruktur im Rahmen einer Auftragsdatenverarbeitung für die Meier GmbH aus Deutschland zur Verfügung. Und von der Meier GmbH werden darüber hinaus auf Grundlage der oben genannten Abwägung Daten zur Qualifikation des Führungspersonals an die Konzernmutter übermittelt.

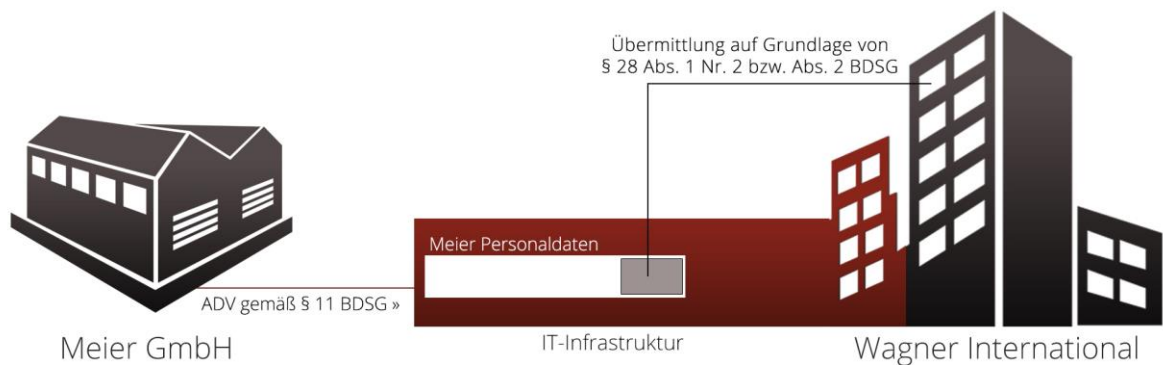


Abb. 3

Unter Umständen hat die Wagner International darüber hinaus das Recht, bestimmte Daten zu eigenen Zwecken zu verarbeiten (hier z.B. Qualifikationsdaten der Mitarbeiter).

d. Und wenn der Empfänger in einem Drittstaat sitzt?

Wenn Daten an einen Empfänger übermittelt werden, der außerhalb der EU bzw. des EWR sitzt, kommt noch eine zusätzliche Voraussetzung hinzu. Der Gesetzgeber geht davon aus, dass in solchen so genannten Drittstaaten das Datenschutzniveau geringer ist – deshalb müssen die Daten hier noch besser geschützt werden. Zu der Prüfung der allgemeinen Rechtsgrundlage (siehe Schritt 3) muss noch eine weitere Prüfung vorgenommen werden („2-Stufen-Prüfung“).

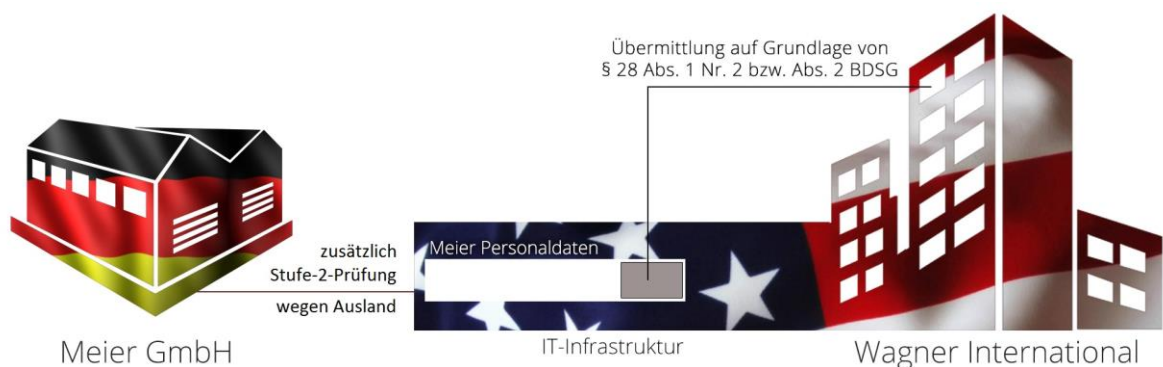


Abb. 4

Noch komplexer wird das Thema, wenn die Konzernmutter oder andere Konzernunternehmen ihren Sitz im (außereuropäischen) Ausland haben.

Mögliche Rechtsgrundlagen für den Transfer in einen Drittstaat sind:

- EU-Standardvertrag:
Die EU-Kommission hat drei Musterverträge veröffentlicht. Schließen Datenexporteur und Datenimporteur einen solchen EU-Standardvertrag unverändert ab, verpflichten sie sich darin zu einem sicheren Umgang mit personenbezogenen Daten. Ein solcher Vertrag kann auch zwischen mehreren Vertragsparteien (Konzernunternehmen) abgeschlossen werden.
Für Standard-Konstellationen stellen die EU-Standardverträge eine relativ einfache und eher schnell umzusetzende Lösung dar.
- Binding Corporate Rules:
Wenn verbindliche Unternehmensregeln (Binding Corporate Rules) in Kraft sind, die den Umgang mit personenbezogenen Daten konzernweit regeln, und wenn diese Regeln von der Datenschutz-Aufsichtsbehörde genehmigt wurden, stellen diese eine geeignete Rechtsgrundlage dar. Diese Möglichkeit ist aufgrund des hohen einmaligen Aufwands eher für große, internationale Konzerne geeignet.
- Weitere Möglichkeiten:
Das Gesetz nennt in § 4c BDSG noch weitere Möglichkeiten, wann ein Datentransfer an einen Empfänger in einem Drittstaat zulässig ist: Beispielsweise wenn jeder Betroffene seine schriftliche Einwilligung erteilt hat oder wenn die Datenübermittlung erforderlich (notwendig) ist, um den Vertrag mit dem Betroffenen durchführen zu können. In Konzernen greifen diese Ausnahmen aber häufig nicht.
- Hinweis: Auf „Safe Harbor“ kann nicht mehr zurückgegriffen werden.
Bis Oktober 2015 stellte es eine Rechtsgrundlage dar, wenn der Empfänger der Daten in den USA saß und sich der „Safe-Harbor“-Selbstzertifizierung unterworfen hatte. Der Europäische Gerichtshof (EuGH) hat Anfang Oktober 2015 entschieden, dass Safe Harbor in der damaligen Form keinen geeigneten Schutz für die personenbezogenen Daten der Betroffenen darstellte. Aktuell arbeiten USA und EU an einem neuen Abkommen (dem sogenannten „Privacy Shield“), das Safe Harbor ersetzen soll [Stand 13. Februar 2016].

3. Zusammenfassung

Mit der zunehmenden Digitalisierung in vielen Lebens- und Arbeitsbereichen wächst auch das Volumen an Daten, das weltweit ausgetauscht wird. Hierbei ist, wie auch sonst, das Datenschutzrecht zu beachten.

Für den Datenaustausch zwischen Unternehmen desselben Konzerns gelten dabei keine Erleichterungen: Es muss der datenschutzrechtliche Maßstab angelegt werden, der auch zwischen völlig fremden Unternehmen gilt.

Die konkreten Voraussetzungen, die im Einzelfall zu beachten sind, hängen von der genauen Fallbeschreibung ab. Bitte sprechen Sie uns an, wenn Sie Fragen zum Umgang mit personenbezogenen Daten in einer Unternehmensgruppe haben.