

Datentransfer im Unternehmen

Dauerremissionen
Prospekthaftung: Verjährung

Eigenhaftung des Gehilfen
Aus culpa in contrahendo

Werkvertrag
Warnpflichtverletzung
und Mitverschulden

Verdeckte Kapitalgesellschaft
Vermögensverwaltung

Arbeitsentgelt
Geheimhaltungsklauseln

Bank Burgenland
Wer billig kauft, kauft teuer

Datenschutz im Unternehmen

Datenschutz kann auch im Hinblick auf den Datenfluss innerhalb eines Unternehmens von Relevanz sein. Er wird in diesem Zusammenhang allerdings kaum als Problem wahrgenommen. Fraglich ist, unter welchen datenschutzrechtlichen Voraussetzungen Arbeitnehmerdaten unternehmensintern weitergegeben werden dürfen. Dies ist bislang kaum untersucht worden.

CLEMENS EGERMANN / SABINE HAUER

A. Datenschutzrechtliche Ausgangslage

1. Allgemeines

Das DSGVO¹⁾ enthält nur wenige Spezialbestimmungen zu Datenschutz im Beschäftigungskontext. Auch andere Gesetze wie das ArbVG, TKG sowie individual(arbeits)rechtliche Vorschriften sind beachtlich, auf die dieser Beitrag jedoch nicht eingeht. Datenschutzrechtliche Regelungen in den Mitgliedstaaten basieren gegenwärtig vor allem auf der RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutz-RL).²⁾ Deren Anwendbarkeit im Beschäftigungskontext wurde vom EuGH bestätigt.³⁾

Im Hinblick auf die geplante Datenschutzreform der EU wurde zuletzt der Entwurf der Datenschutz-Grundverordnung⁴⁾ (im Folgenden „Entwurf“) angenommen, der eine Reihe von Mindeststandards für die nationalen Rechtsvorschriften vorsieht. Grundsätzliches für den Datenschutz im Unternehmen ergibt sich aus deren Erwägungsgrund 124. Danach sollen die allgemeinen Grundsätze des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten auch im Kontext von Beschäftigung und sozialer Sicherheit gelten. Nach Art 82 des Entwurfs können die Mitgliedstaaten in den Grenzen der VO die Verarbeitung personenbezogener Arbeitnehmerdaten im Beschäftigungskontext gesetzlich regeln. Es werden daher im Bereich des unternehmensinternen Datenschutzes (vorerst) weiterhin die innerstaatlichen Regelungen zur Anwendung gelangen.

2. Zulässigkeit der Datenverwendung

Grundvoraussetzung jeder Übermittlung von Mitarbeiterdaten nach dem DSGVO ist zunächst, dass diese insb. *aus einer zulässigen Datenverarbeitung stammen* und durch Zweck und Inhalt der Übermittlung schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (§ 7). Schutzwürdige Geheimhaltungsinteressen werden dann nicht verletzt, wenn die Datenverwendung (dh jede Art der Handhabung von Daten, wie ermitteln, übermitteln, speichern, überlassen, auswerten) durch den Arbeitgeber

- lebenswichtigen Interessen des Mitarbeiters dient,
- wenn die Datenverwendung aufgrund einer Zustimmung des Mitarbeiters erfolgt oder
- wenn sich diese auf überwiegende Interessen anderer stützt (§ 8 Abs 1).

Zulässige Eingriffe in das Grundrecht dürfen ausschließlich in der *gelindesten zum Ziel führenden Art* vorgenommen werden (§ 1 Abs 2 und § 7 Abs 3).

Daten oder *personenbezogene Daten* iSd DSGVO sind Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist, zB Name, Geburtsdatum, Adresse, Geschlecht, Einkommen, Vermögen, Leumund, Lebensgewohnheiten, Intelligenzquotient, Fingerabdruck, genetische Merkmale, Bild, Stimme.

Lebenswichtige Interessen der Arbeitnehmer werden dem Arbeitgeber in der betrieblichen Praxis kaum einen Grund zur Rechtfertigung der Datenverwendung geben.

Die (jederzeit widerrufbare) *Zustimmung des Arbeitnehmers* zur Datenverwendung gilt nur dann als erteilt, wenn diese freiwillig erfolgt, dh ohne Zwang abgegeben wurde, und der Arbeitnehmer auch über die zu verwendenden Daten informiert ist. Erwägungsgrund 33 des Entwurfs führt dazu aus, dass die Einwilligung keine rechtswirksame Grundlage für die Verarbeitung liefert, wenn die betreffende Person keine echte Wahlfreiheit hat und somit nicht in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne dadurch Nachteile zu erleiden. Gerade im Arbeitsverhältnis fällt die Beurteilung der Freiwilligkeit der Zustimmung angesichts der schwächeren Position des Arbeitnehmers strenger aus. Datenschutzrechtlich wird es im Arbeitsverhältnis daher oft am Erfordernis einer gültigen Zustimmung fehlen, zumal diese eine volle Information über die Datenverwendung voraussetzt. Freilich wird dies in einem aufrechten Dienstverhältnis wohl selten releviert.

Die Zustimmung des Arbeitnehmers kann unterbleiben, wenn der Auftraggeber ein *überwiegendes berechtigtes Interesse* an der Datenverwendung hat. Dies liegt etwa dann vor, wenn die Verwendung von Daten zur Erfüllung von vertraglichen Verpflichtungen

Dr. Clemens Egermann ist Rechtsanwalt und Partner bei Barnert Egermann Illigasch Rechtsanwälte. Er ist insb. auf die Bereiche Arbeits-, Gesellschafts- und Immobilienrecht spezialisiert. Dr. Sabine Hauer ist Rechtsanwältin bei Barnert Egermann Illigasch Rechtsanwälte GmbH mit den Schwerpunkten Zivil-, Arbeits- und Immobilienrecht.

- 1) Alle Paragrafenzitate ohne nähere Angabe beziehen sich auf das DSGVO 2000.
- 2) AB L 1995/281, 31.
- 3) EuGH 20. 5. 2003, C-465/00, *Österreichischer Rundfunk*.
- 4) Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM (2012) 11.

bzw zur Geltendmachung von Rechtsansprüchen des Arbeitgebers vor einer Behörde erforderlich ist (§ 8 Abs 3). Diese Bestimmung ist die wichtigste Grundlage für die unternehmensinterne Datenverarbeitung.

Sensible Daten, dh Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben, unterliegen grundsätzlich einem allgemeinen Verwendungsverbot und dürfen nur unter den in § 9 abschließend aufgezählten Voraussetzungen verwendet werden; etwa wenn die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und nach besonderen Rechtsvorschriften zulässig ist. In diesem Zusammenhang besteht keine allgemeine Ausnahmeregel bei überwiegenden Interessen des datenschutzrechtlichen Auftraggebers.

Daten von Arbeitnehmern, die in der Freizeit des Arbeitnehmers ermittelt werden, können sensibel sein (zB der Besuch eines Gebetshauses). Bei Dienstreisen etwa kann die Ermittlung sensibler Daten nicht ausgeschlossen werden. Im Allgemeinen werden im Hinblick auf den Verhältnismäßigkeitsgrundsatz das Führen eines Fahrtenbuchs und Aufzeichnungen des Arbeitnehmers über die Dauer der auswärtigen Termine und Fahrtstrecken zulässig sein, um die Interessen des Arbeitgebers zu wahren, ebenso die Führung von Spesenabrechnungen. Auch Gesundheitsdaten der Mitarbeiter sind sensible Daten. Daten wie bspw Krankenzustände von Mitarbeitern sind für den Arbeitgeber zur Meldung der Sozialversicherung verpflichtend zu erheben und deren Verwendung sohin zulässig.

Informationen, die sensible Daten zum Inhalt haben, dürfen, soweit der Arbeitgeber durch Einwilligung des Arbeitnehmers oder sonst in zulässiger Weise von diesen Kenntnis erlangt, aufgrund ihrer strengen Zweckbindung nach dem Datenschutzrecht kein regulärer Teil einer Personalakte sein, sondern müssen getrennt vom sonstigen Inhalt der Personalakte aufbewahrt und gegen zweckfremde Kenntnisnahme besonders gesichert werden.

Der Schutz personenbezogener Daten umfasst nicht nur die Daten von aktuellen, sondern auch von ausgeschiedenen Mitarbeitern und Bewerbern. Bewerbungsunterlagen offen an verschiedene Abteilungen zu schicken, wird schon unter dem Aspekt der Verhältnismäßigkeit nicht zulässig sein, ist in der Praxis aber nicht unüblich. Gleiches gilt für das Weiterleiten von Bewerbungen, in denen ua auch sensible Daten als Anlage enthalten sind.

Im privaten Bereich ist immer der Rechtsträger (das Unternehmen) datenschutzrechtlicher *Auftraggeber*, ein einzelner Mitarbeiter, wie etwa der kaufmännische Vorstandsdirektor, in dessen Zuständigkeitsbereich auch das Rechnungswesen fällt, kann nicht Auftraggeber iSd DSG sein.⁵⁾

3. Zulässigkeit der Datenübermittlung

Ist der Arbeitgeber im rechtmäßigen Besitz von Mitarbeiterdaten, bedeutet dies nicht, dass eine unternehmensinterne Weitergabe uneingeschränkt zulässig

ist. Nicht nur die Verarbeitung, auch die *Übermittlung* von Daten ist nur unter bestimmten Voraussetzungen und unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes zulässig (§ 7 Abs 2 und 3). Für die Übermittlung von Daten innerhalb eines Unternehmens enthält das DSG keine Sonderbestimmungen.

Die *Zulässigkeit der Übermittlung* setzt im Allgemeinen voraus, dass die Daten

- aus einer zulässigen Datenanwendung stammen und
- durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden. Dies entspricht den Voraussetzungen für die *Datenverarbeitung*. Hinzu kommt die Voraussetzung des § 7 Abs 2 Z 2, wonach
- der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft zu machen hat.

Va bei den in den Standardanwendungen vorgesehenen Empfängerkreisen wird die ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis des Empfängers von Übermittlungen außer Zweifel stehen, sodass eine Glaubhaftmachung des Empfängers gegenüber dem Übermittelnden entbehrlich sein wird.⁶⁾

B. Unternehmensinterne Datenweitergabe

1. Datenübermittlung innerhalb des Unternehmens?

Übermittlung iSd DSG ist ua die Weitergabe von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insb auch das Veröffentlichen solcher Daten. Nun könnte man auf den ersten Blick meinen, dass es sich bei der unternehmensinternen Weitergabe, dh innerhalb derselben juristischen Person (als Auftraggeber), mangels Weitergabe von Mitarbeiterdaten an *Dritte*, gar nicht um eine Übermittlung iSd DSG handelt. Diese Ansicht wäre jedoch in dieser Allgemeinheit verfehlt: Unter den Begriff der Datenübermittlung fällt nach der ausdrücklichen Bestimmung des § 4 Abs 4 als dritte Übermittlungsform auch die Verwendung von Daten eines Auftraggebers *für ein anderes Aufgabengebiet* des Auftraggebers.

Der Begriff *Aufgabengebiet* ist im Gesetz nicht definiert und unklar. Im Schrifttum wird mitunter die Ansicht vertreten, ein Aufgabengebiet sei eines von mehreren Tätigkeitsfeldern eines Auftraggebers, das in seinem Umfang nach der Verkehrsauffassung geeignet sei, für sich allein den gesamten Geschäftsbereich eines Auftraggebers zu bilden. Im privaten Unternehmensbereich sei ein Aufgabengebiet in etwa mit dem Umfang einer Gewerbeberechtigung gleichzusetzen.⁷⁾ Sofern man dieser Meinung folgt, lässt sich daraus für die Beurteilung der Zulässigkeit der unternehmensinternen Übermittlung von Mitarbei-

5) *Dobn/Pollirer/Weiss/Knyrim*, DSG² § 4 Anm 5.

6) *Dobn/Pollirer/Weiss/Knyrim*, DSG² § 7 Anm 9.

7) *Knyrim*, Datenschutzrecht² 105 uVa RV DSG 2000 zu § 4 Z 12.

terdaten insofern nichts gewinnen, weil bei dieser Ansicht von Daten anderer Personen als Mitarbeiter (zB Kunden) ausgegangen wird.

Nach dem OGH kann die Gleichhaltung des Übermittels von Daten an andere Empfänger mit der Verwendung für ein anderes Aufgabengebiet nur darin liegen, dass der Betroffene, der einem privaten Rechtsträger Daten für einen bestimmten Tätigkeitsbereich anvertraut hat, nicht damit rechnen muss, dass diese für Zwecke verwendet werden, die mit dem Anlass des Anvertrauens in keinem engen wirtschaftlichen Zusammenhang stehen.⁸⁾ Dieser Ansicht ist zu folgen. Das Abstellen auf den jeweiligen Verwendungszweck ist auch im Hinblick auf die Beurteilung der Zulässigkeit der unternehmensinternen Übermittlung von Mitarbeiterdaten durchaus zielführend. Insoweit verschwimmen allerdings die Begriffe *Aufgabengebiet* und *Zweckbindung*. Im Ergebnis ist jeder Zweckwechsel eine Übermittlung und bedarf somit ergänzend einer besonderen rechtlichen Grundlage. So kann es aufgrund der Bestimmungen des AZG etwa zulässig sein, bestimmten Mitarbeitern Zeitaufzeichnungen der Arbeitnehmer zwecks Einhaltung der Aufzeichnungs-, Auskunfts- und Meldepflichten zu übermitteln. Dies gilt etwa auch für Aufzeichnungen des Arbeitnehmers über Dienstreisen (zB Fahrtenbucheinträge oder Aufzeichnungen über die Dauer der auswärtigen Termine und Fahrtstrecken).

Mangels klarer Abgrenzung des Begriffs *Aufgabengebiet* ist es für den Arbeitgeber im Einzelfall oft schwierig zu beurteilen, ob es sich bei der unternehmensinternen Weitergabe von Mitarbeiterdaten um eine Weitergabe innerhalb desselben Aufgabengebiets oder um eine *Übermittlung* handelt. Es kann also uU auch innerhalb des eigenen Unternehmens des Arbeitgebers eine *Datenübermittlung* vorliegen, wie bspw bei Weiterleitung von Mitarbeiterdaten an den Betriebsrat: Insb der Umstand, dass Organe der betrieblichen Interessenvertretung in der Standardanwendung *SA002 Personalverwaltung für privatrechtliche Dienstverhältnisse* als Empfängerkreis ausdrücklich definiert sind, lässt darauf schließen, dass keine Datenverwendung innerhalb desselben Aufgabengebiets, sondern eine *Übermittlung* vorliegt. Auch die Übermittlung von Mitarbeiterdaten an den Betriebsrat basiert auf gesetzlichen Sonderbestimmungen: Das ArbVG sieht für bestimmte Datenverarbeitungen, die Dienstnehmer betreffen, Informations- und Mitbestimmungsrechte des Betriebsrats vor. Nach § 9 Z 11 bleiben die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse unberührt. Zur Ausübung der Befugnisse des Betriebsrats ist diese *Übermittlung* von Arbeitnehmerdaten daher zulässig.

Für die Verwendung von Daten durch den Betriebsrat gelten im Übrigen dieselben datenschutzrechtlichen Bestimmungen wie für den Arbeitgeber.

2. Zweckbindungsgrundsatz

Unabhängig davon, ob es sich um eine Weitergabe innerhalb desselben Aufgabengebiets (und daher um *Datenverarbeitung*) oder um *Übermittlung* handelt, ist – da Voraussetzung sowohl der Datenverarbeitung

als auch der Datenübermittlung – stets der *Zweckbindungsgrundsatz* nach § 6 Abs 1 Z 2 zu beachten. Danach dürfen Daten ua nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise *weiterverwendet* werden.

Zunächst gilt für die *Weiterverwendung* (Weitergabe) von Daten innerhalb des Unternehmens grundsätzlich, dass diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (zB Rechnungswesen und Controlling) oder der Analyse und Planung dienen, jedenfalls nicht als eigener Verwendungszweck zu sehen sind, der mit dem Zweck der ursprünglichen Datenermittlung „unvereinbar“ ist.⁹⁾ Die Weiterleitung von Kundendaten an die Controlling-Abteilung ist damit zulässig. Ebenso wird etwa die Weitergabe von Mitarbeiterdaten aus der Standardanwendung *SA002* an die Personalabteilung zur Durchführung der Lohnverrechnung oder zur Einhaltung von gesetzlichen Meldepflichten (zB an den Sozialversicherungsträger) idR zulässig sein. Eine Weiterleitung an andere Abteilungen oder Mitarbeiter des Unternehmens oder gar eine unternehmensweite Veröffentlichung der Daten des betroffenen Mitarbeiters ist von diesem Zweck nicht gedeckt und deshalb unzulässig. So wäre etwa die Weitergabe dieser Daten zB an die Marketingabteilung zur Schaltung eines Inserats in der internen Firmenzeitung vom ursprünglichen Zweck nicht erfasst. Da hier bereits die Voraussetzung des überwiegenden Interesses bzw Erfüllung vertraglicher Pflichten nicht vorliegt, muss eine gültige Zustimmung des betroffenen Mitarbeiters eingeholt werden.

3. Zusammenspiel von Übermittlung und Zweckbindung

Insgesamt stellt sich die Definition des Begriffs *Aufgabengebiet* iZm der Übermittlung als besondere Ausformung des Zweckbindungsgrundsatzes dar. Wenn man davon ausgeht, dass die Übermittlung definitionsgemäß den Zweckwechsel umfasst, stellt sich die (wohl rein theoretische) Frage, ob die terminologische Unschärfe des Begriffs der *Datenweiterverwendung* idS § 6 Abs 1 Z 2 nicht in sich schon eine Übermittlung bezeichnet, zumal die gesetzliche Definition der *Datenverwendung* in § 4 Z 8 sowohl das *Verarbeiten* als auch die *Übermittlung* von Daten umfasst. Dass die Übermittlung im Verarbeitungsbegriff nicht inkludiert ist – und insoweit vom Sprachgebrauch der EU-Datenschutz-RL abweicht –, hat seine Ursache in den unterschiedlichen Zulässigkeitsvoraussetzungen für diese beiden Tätigkeiten im DSGVO.

C. Sicherstellung des Datenschutzes

Schon aufgrund der datenschutzrechtlichen Verpflichtung zum Datengeheimnis (§ 15) sollten interne Verhaltensrichtlinien eine Beschreibung enthalten, welche Gruppen von Arbeitnehmern welche personenbezogenen Daten über welche Personengrup-

8) OGH 25. 2. 1992, 4 Ob 114/91.

9) *Dohr/Pollirer/Weiss/Knyrim*, DSGVO § 6 Anm zu Abs 1.

pen unter welchen Voraussetzungen an wen weitergeben dürfen. In diesem Zusammenhang ist es erforderlich, die technischen Möglichkeiten so auszugestalten, dass nur solche Zugriffe zu den einzelnen Datenanwendungen möglich sind, die für einen bestimmten Arbeitsplatz bzw für eine bestimmte Aufgabe erforderlich sind (zB Zugriff zu Personaldateien nur für Mitarbeiter der Personalabteilung). Das Datengeheimnis muss, insb bei Zugriffsmöglichkeiten auf sensible Daten, Maßnahmen der Datensicherheit nach § 14 nach sich ziehen. Dabei ist die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen, die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden, und die Mitarbeiter sind über ihre nach dem DSG und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu beleh-

ren (§ 14 Abs 2 Z 1 bis 3). Darüber hinaus sind weitere technische Datensicherheitsmaßnahmen wie etwa Zutritts- und Zugriffsberechtigungen vorzusehen (§ 14 Abs 2 Z 4 bis 7).

SCHLUSSSTRICH

Entgegen weit verbreiteter Praxis kann auch die Weitergabe von Arbeitnehmerdaten innerhalb eines Unternehmens als Verwendung von Daten für ein anderes Aufgabengebiet iSd § 4 Abs 12 DSG den Vorgaben des DSG an eine Übermittlung unterliegen. Der jeweilige Verwendungszweck ist stets dafür entscheidend, an welche interne Organisationseinheit Daten weitergegeben werden dürfen. Jede Übermittlung iSd DSG bedarf darüber hinaus auch einer besonderen rechtlichen Grundlage.