DER KONZERNINTERNE AUSTAUSCH PERSONENBEZOGENER DATEN IM LICHTE DER DSGVO

Sabine Brunner

Rechtsanwaltsanwärterin, PwC Legal Austria – oehner partner rechtsanwaelte gmbh
Erdbergstraße 200, 1030 Wien, AT
sabine.brunner@pwc.com; http://pwclegal.at

Schlagworte: ***Datenschutz, Datenschutzrecht, Datenschutz-Grundverordnung, DSGVO, DSG, Konzern, Unternehmensgruppe, Datentransfer, Datenübermittlung***

Abstract: *In Zeiten der globalen Vernetzung ist es beinahe unverzichtbar, konzernintern und grenzüberschreitend personenbezogene Daten natürlicher Personen auszutauschen. Dabei wird in der Praxis häufig übersehen, dass es innerhalb des Konzerns kein Privileg hinsichtlich der Datenübermittlung gibt. Dies wird sich auch nicht durch die ab Mai 2018 geltende Datenschutz-Grundverordnung ändern. Im vorliegenden Beitrag werden Empfehlungen und Stolpersteine aus der Praxis aufgezeigt und gleichzeitig auch eine Art «Guideline» für den rechtssicheren Umgang mit konzerninternen Datentransfers dargelegt werden.*

1. Einleitung

In Zeiten der globalen Vernetzung und internationaler Konzernstrukturen ist es beinahe unverzichtbar, grenzüberschreitend personenbezogene Daten natürlicher Personen innerhalb von Konzernunternehmen auszutauschen. Dabei wird in der Praxis häufig übersehen, dass es innerhalb des Konzerns kein Privileg im Hinblick auf die Datenübermittlung gibt. Ein solches findet sich weder im derzeit (noch) geltenden Datenschutzgesetz 2000 (DSG 2000)[1], noch wurde ein solches Privileg durch den europäischen Gesetzgeber in der Datenschutz-Grundverordnung (DSGVO)[2] statuiert. Dies führt im Ergebnis dazu, dass trotz der vermeintlichen Nähe zwischen den Konzernunternehmen kein gänzlich «freier» Datenverkehr zulässigerweise erfolgen kann. Der vorliegende Beitrag soll daher eine Art «Guideline» für einen DSGVO-konformen Umgang mit konzerninternen Datentransfers liefern.

2. Konzerninterne Datentransfers im Lichte der DSGVO

Die DSGVO selbst nimmt nur sehr eingeschränkt auf Konzerne und damit in Zusammenhang stehende Datenübermittlungen Bezug.[3] In Art. 4 Abs. 19 leg. cit. wird die «Unternehmensgruppe» als eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht, definiert. Erwägungsgrund 48 der DSGVO spricht schließlich nur davon, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse daran haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Dieser Erwägungsgrund wird unter Punkt 2.1.2. noch näher behandelt.

---

1 DSG 2000, BGBl I 1999/165.

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl L 119/1, 1.

3 Spindler 2016, S. 941.

Mangels ausdrücklicher Privilegierung sind Datenübermittlungen im Konzern also grundsätzlich wie Übermittlungen an Dritte zu behandeln. Es stellt sich jedoch die Frage, welcher Lösungsansatz sich in der Praxis für welche Zwecke am besten eignet.

2.1. Datentransfers innerhalb der EU

Handelt es sich um eine Unternehmensgruppe, deren Gesellschaften ausschließlich im EU-Raum niedergelassen sind, bedarf es keiner vorherigen Genehmigung der Datenschutzbehörde für den Transfer personenbezogener Daten zwischen den Konzerngesellschaften. Voraussetzung für die Zulässigkeit der Übermittlung ist allerdings die Rechtmäßigkeit der Datenverarbeitung: Entweder stützt man den Datentransfer auf einen der Rechtfertigungstatbestände des Art. 6 Abs. 1 DSGVO oder man macht zum Zwecke der Datenübermittlung vom Konstrukt der Auftragsverarbeitung gem. Art. 4 Z. 8 i.V.m. Art. 28 DSGVO Gebrauch. Bei besonderen Kategorien personenbezogener Daten sind für Übermittlungen zusätzlich die strengeren Rechtfertigungstatbestände des Art. 9 Abs. 2 DSGVO zu beachten.

Im Falle von gesetzlich oder vertraglich begründeten Datenübermittlungen stellen sich in der Praxis kaum Schwierigkeiten. Daher werden im Folgenden insbesondere die Themen der Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO und des berechtigten Interesses gemäß Art. 6 Abs. 1 lit. f DSGVO diskutiert.

2.1.1. Einwilligung der betroffenen Person

Eine Möglichkeit für den rechtskonformen Transfer innerhalb von Konzerngesellschaften ist das Einholen von Einwilligungen der betroffenen Personen. In der Praxis zeigen sich dabei jedoch zwei wesentliche Herausforderungen: Einerseits können Einwilligungen jederzeit widerrufen werden, andererseits wird im Zusammenhang mit der Übermittlung von Mitarbeiterdaten die Freiwilligkeit einer Zustimmung durchaus angezweifelt.[4] Im Zusammenhang mit Mitarbeiterdaten ist in der Praxis auch zu berücksichtigen, dass für die konzerninterne Übermittlung gegebenenfalls der Abschluss einer Betriebsvereinbarung notwendig sein kann. Dies ist jedoch nur in bestimmten Konstellationen, z.B. bei der Einführung elektronischer Personaldatensysteme, der Fall.[5]

Die Einwilligung stellt daher vorrangig für die Übermittlung von Kunden-, Interessenten- oder Geschäftspartnerdaten eine geeignete Rechtsgrundlage dar. In diesem Fall ist jedoch zu beachten, dass Einwilligungserklärungen strengen Erfordernissen unterliegen, wie insbesondere der Anführung sämtlicher Empfänger von personenbezogenen Daten. In der Praxis empfiehlt es sich daher, in Zustimmungserklärungen den Link zu einer Auflistung aller Konzerngesellschaften als Empfänger auf einer Webseite vorzusehen, um beim Hinzukommen weiterer Gesellschaften keine neuerliche Einwilligung einholen zu müssen.[6]

2.1.2. Berechtigtes Interesse der Konzerngesellschaft

Vor allem im Zusammenhang mit Mitarbeiterdaten können – neben der Erfüllung des Dienstvertrages gem. Art. 6 Abs. 1 lit. b DSGVO – beispielsweise auch überwiegende Konzerninteressen i.S.v. Art. 6 Abs. 1 lit. f DSGVO den konzerninternen Datentransfer rechtfertigen. Dahingehend hält die DSGVO im Erwägungsgrund 48 fest, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse daran haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Allerdings lässt die DSGVO offen, was unter «internen Verwaltungszwecken» zu verstehen ist.

Im Rahmen des DSG 2000 hat die damalige Datenschutzkommission, nunmehrige Datenschutzbehörde, unter anderem für folgende Zwecke ein berechtigtes Interesse für die konzerninterne Übermittlung anerkannt: Personalbereitstellung, Spesen- und Reisekostenabrechnung, Mitsprache bei der Zuteilung von Belohnungen

---

4 Artikel-29-Datenschutzgruppe 2017, S. 7; Feiler/Schlacher 2017, S. 28; Fellner 2017, S. 3.

5 A.A. Feiler/Schlacher 2017, S. 29.

6 Feiler/Schlacher 2017, S. 28; Knyrim 2008, S. 151.

an Konzernmitarbeiter, Verwaltung des Serverzugangs, Verwaltung von freiwilligen Vergütungs- und Beteiligungsplänen, Anmeldung zu und Verwaltung von Schulungen, interne Kommunikation, Leistungsbeurteilung, Ermittlung der erfolgsabhängigen Vergütung, Potentialanalyse und Karriereplanung sowie Entwicklung von Organisationsplänen für Projektplanung und Planung von Auslandseinsätzen.[7] Ein berechtigtes Interesse wurde auch im Rahmen dauerhafter Matrixorganisationen, beispielsweise zur Mitwirkung an der Beurteilung durch Manager anderer Konzerntöchter, denen die Mitarbeiter funktional unterstellt sind, anerkannt.[8]

In der Praxis ist außerdem zu beachten, dass den Betroffenen in diesem Fall auch ein Widerspruchsrecht gem. Art. 21 DSGVO zusteht, auf das sie spätestens zum Zeitpunkt der ersten Kommunikation in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden müssen.[9] Im Zusammenhang mit Mitarbeiterdaten könnte diese Information in einem bestehenden Arbeitsverhältnis durch Mailaussendung an die betroffenen Mitarbeiter erfolgen, bei Neueintritten könnte dies hingegen im Rahmen des Dienstvertrages abgewickelt werden.

2.1.3. Auftragsverarbeitung

Eine weitere Möglichkeit, um Daten konzernintern zu überlassen, ist die Auftragsverarbeitung gem. Art. 4 Z. 8 i.V.m. Art. 28 DSGVO. Diese Möglichkeit macht nur in einer bestimmten Konstellation Sinn, nämlich wenn die personenbezogenen Daten ausschließlich im Rahmen der Aufträge der verantwortlichen Konzerngesellschaft verarbeitet werden sollen. So kann es vorkommen, dass der IT-Service konzernweit durch eine Gesellschaft vorgenommen wird.

Werden die personenbezogenen Daten einer Konzerngesellschaft hingegen für deren eigene Zwecke oder für Konzernzwecke übermittelt, liegt keine Auftragsverarbeitung vor.[10] Darüber hinaus ist in der Praxis zu beachten, dass es des Abschlusses einer schriftlichen Vereinbarung zwischen den betroffenen Konzerngesellschaften bedarf und die Konzerngesellschaft, welche als Auftragsverarbeiter tätig wird, auch für die Einhaltung der Pflichten des Art. 28 DSGVO verantwortlich ist.

2.1.4. Gemeinsam für die Verarbeitung Verantwortliche

Die DSGVO sieht auch die Möglichkeit vor, dass mehrere Verantwortliche gemeinsam über Zwecke der und die Mittel zur Verarbeitung entscheiden und insbesondere die damit verbundenen Funktionen und die Aufteilung der Verpflichtungen in einer Vereinbarung entsprechend regeln.[11] Diese Regelung ähnelt in ihren Grundzügen dem derzeit noch geltenden Informationsverbundsystem des § 4 Z. 13 DSG 2000. Für Konzerne wird diese Konstellation in der Praxis nur eine untergeordnete Rolle spielen, beispielsweise, wenn mehrere Konzerngesellschaften gemeinsam eine Webseite betreiben, über die sie personenbezogene Daten erheben.[12]

2.2. Datentransfers in Drittstaaten

Sollen personenbezogene Daten an Konzernunternehmen mit Niederlassungen in Drittstaaten übermittelt werden, unterliegt dies zusätzlich noch strengeren Voraussetzungen. Dabei sind die Bestimmungen des Art. 44 ff. DSGVO zu beachten. Bei internationalen Konzernen empfiehlt sich vorrangig die Anwendung sogenannter «Binding Corporate Rules» (BCR). Jede Unternehmensgruppe sollte für ihre internationalen Datenübermittlungen aus der Union an Organisationen derselben Unternehmensgruppe genehmigte verbindliche interne Da-

---

7 DSK 6. September 2013, K178.415/0010-DSK/2013; DSK 13. Juli 2012, K178.465/0011-DSK/2012; DSK 19. März 2010, K178.378/0004-DSK/2010; DSK 18. November 2009, K178.343/0011-DSK/2009; DSK 25. April 2008, K178.297/0004-DSK/2008; DSK 6. Februar 2008, K178.256/0005-DSK/2008; DSK 15. Juni 2007, K178.234/0008-DSK/2007; DSK 23. Mai 2007, K178.239/0006-DSK/2007.

8 DSK 30. September 2011, K178.414/0006-DSK/2011.

9 Franzen 2017, S. 326.

10 Fellner 2017, S. 2.

11 Vgl. Art. 26 DSGVO.

12 Kieselmann 2016.

tenschutzvorschriften anwenden dürfen, sofern diese sämtliche Grundprinzipien und durchsetzbaren Rechte enthalten, die geeignete Garantien für die Übermittlungen personenbezogener Daten bieten.[13] Diese internen verbindlichen Datenschutzvorschriften sind von der Datenschutzbehörde zu genehmigen. Im Falle eines nachträglichen Hinzukommens weiterer Konzerngesellschaften bedarf es wohl keiner erneuten Genehmigung, dennoch ist eine vorherige Abstimmung mit der Datenschutzbehörde ausdrücklich zu empfehlen.[14] Darüber hinaus ist festzuhalten, dass diese BCR keine geeigneten Garantien für die Übermittlung an konzernexterne Unternehmen darstellen.[15]

3. Fazit

Trotz der Einführung eines EU-weiten Gesamtregelwerks sind konzerninterne Übermittlungen personenbezogener Daten auch künftig an gewisse Voraussetzungen bzw. Auflagen gebunden. Angesichts der hohen Geldbußen der DSGVO und des drohenden Reputationsschadens sind Konzerne daher gut beraten, besonderes Augenmerk auf ihre konzerninterne Datenschutz-Compliance zu legen. Welcher Lösungsansatz für den jeweiligen Datentransfer gewählt wird, sollte im Einzelfall jedenfalls sorgfältig abgewogen werden.

4. Literatur

Artikel-29-Datenschutzgruppe, Opinion 2/2017 on data processing at work, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (alle Websites zuletzt aufgerufen am 7. Januar 2018), 2017.

Feiler, Lukas/Forgó, Nikolaus, EU-Datenschutz-Grundverordnung, Verlag Österreich, Wien, 2016.

Feiler, Lukas/Schlacher, Elisa Maria, Konzerninterne Datenübermittlungen DSGVO-konform gestalten, Compliance Praxis 2017, Heft 1, S. 28–29.

Fellner, Georg, Verarbeitung von Arbeitnehmerdaten im Konzern. In: WEKA-Verlag Gesellschaft m.b.H. (Hrsg.), Praxiswissen Datenschutz, WEKA-Verlag Gesellschaft m.b.H., Wien, 2017, Register 3, Kapitel 6.

Franzen, Martin, Datenschutz-Grundverordnung und Arbeitsrecht, Europäische Zeitschrift für Arbeitsrecht 2017, Heft 3, S. 313–351.

Kieselmann, Sabrina, Für die Datenverarbeitung gemeinsam Verantwortliche – datenschutzrechtliche Absicherung nach Art. 26 DSGVO, http://www.it-sec.de/eng/Aktuelles-Termine/it.sec-blog/Fuer-die-Datenverarbeitung-gemeinsam-Verantwortliche-datenschutzrechtliche-Absicherung-nach-Art.-26-DSGVO, 2016.

Knyrim, Rainer, Datenschutzrechtliche Zustimmungserklärungen richtig formulieren und platzieren, In: Knyrim/Leitner/Perner/Riss (Hrsg.), Aktuelles AGB-Recht, Manz, Wien, 2008, S. 133–154.

Spindler, Gerald, Die neue EU-Datenschutz-Grundverordnung, Der Betrieb 2016, Heft 16, S. 937–947.

[13] Vgl. ErwGr. 110 DSGVO.

[14] Feiler/Forgó 2016, Art. 47 Rz. 7.

[15] Ebenda.