Karin Schuler

Mailserver im Konzernverbund: Wer garantiert das Fernmeldegeheimnis?

Gestaltungsmöglichkeiten bei zulässiger privater Nutzung

Grundsätzliche Problematik bei Konzern-Outsourcing

Immer mehr Konzerne entscheiden sich für eine Datenhaltung auf zentralen IT-Systemen. Häufig ist dies mit der Gründung einer eigenen Konzerngesellschaft verbunden, die für den Betrieb, meist auch für die Planung der IT-Infrastruktur zuständig ist (Konzern-IT). Die Beschäftigten derartiger IT-Gesellschaften sind teilweise die gleichen Personen, die zuvor in den IT-Abteilungen der Einzelgesellschaften oder der Konzernmutter tätig waren. Bleiben sie gar weiterhin in ihren alten Büros, fällt es dem betrieblichen Umfeld erfahrungsgemäß schwer, die grundlegende Änderung wahrzunehmen, die mit dem Wechsel der Gesellschaftsstruktur verbunden ist.

Da das Bundesdatenschutzgesetz kein Konzernprivileg kennt, unterliegt die Übermittlung personenbezogener Daten an Gesellschaften innerhalb eines Konzerns den gleichen Beschränkungen und Anforderungen wie an jedes beliebige andere Unternehmen, das nicht zum Konzern gehört. Eine Übermittlung kann also nur rechtmäßig erfolgen, wenn die verantwortliche Stelle eine Zulässigkeitsgrundlage findet. Diese ist, insbesondere in Bezug auf Beschäftigtendaten, nicht immer leicht zu ermitteln und in manchen Fällen schlichtweg nicht vorhanden. Eine Herleitung aus dem bestehenden Arbeitsvertrag ist in der Regel nicht ausreichend, um die Übermittlung von Beschäftigtendaten an ein Konzernrechenzentrum zu rechtfertigen. Den Interessen des Unternehmens, im Konzern zentrale Datenverarbeitung zu betreiben, stehen nämlich die berechtigten Interessen der Beschäftigten an der Übermittlung ihrer Daten an Dritte entgegen, mit denen kein Arbeitsverhältnis besteht. Ob die eigentlich nötige Einwilligung der Betroffenen (Beschäftigten) in einem Arbeitsverhältnis überhaupt rechtswirksam eingeholt werden kann, wird allgemein bezweifelt. Inwieweit eine Betriebsvereinbarung Zulässigkeitsgrundlage für die Datenübermittlung an die Konzern-IT sein kann, ist vom Einzelfall abhängig und muss jeweils geprüft werden.

Um die beschriebenen Schwierigkeiten zu vermeiden, gehen Unternehmen häufig einen anderen Weg und beauftragen die Konzern-IT im Rahmen einer Auftragsdatenverarbeitung gemäß § 11 BDSG. Der einfacher erscheinende Weg ist dies in der Praxis jedoch häufig nur deshalb, weil die damit verbundenen Pflichten nicht oder nur unzureichend erfüllt werden. Die vom Gesetz eröffnete Möglichkeit, Daten an einen Auftragnehmer zu übergeben, ohne eine Zulässigkeitsgrundlage für Übermittlung finden zu müssen, ist mit starken Beschränkungen versehen. Um die Rechte der Betroffenen durch diese erleichterte Übertragung personenbezogener Daten nicht zu gefährden, muss der Auftragnehmer vertraglich vergleichbar einer untergeordneten Abteilung gebunden werden: Er muss genaue Anweisungen erhalten, welche Verarbeitungsschritte er mit den Daten durchzuführen hat und welche Sicherungsmaßnahmen er zum Schutz dieser Daten ergreifen muss. Außerdem ist sicher zu stellen, dass der Auftraggeber nicht nur auf dem Papier sondern auch de facto »Herr der Daten« bleibt, wozu auch ein Kontrollrecht des Auftraggebers gehört. Dieses Kontrollrecht dient der Überprüfung, ob der geschlossene Vertrag eingehalten wird. Es muss insbesondere so gestaltet sein, dass der betriebliche Datenschutzbeauftragte und der Betriebsrat des Auftraggebers den ihnen zustehenden Zutritt zu den Daten verarbeitenden Systemen haben.

Grundsätzliche Problematik bei Mailservern

Eine besondere Situation ergibt sich in Bezug auf den Betrieb von Mailservern: Ist den Beschäftigten eines Konzernunternehmens die private Nutzung nicht untersagt, so entsteht ein Dienstleistungsverhältnis, durch das ein Unternehmen für diesen privaten Anteil des Mailverkehrs zum Diensteanbieter gemäß Telekommunikationsgesetz (TKG) wird. Dadurch sind diverse Vorgaben des TKG in Bezug auf die frühzeitige Löschung von Verbindungsdaten,[1] die Erfüllung von Informationspflichten[2] und allgemein die Einhaltung des Fernmeldegeheimnisses zu erfüllen.[3]

Die heute üblicherweise eingesetzten Mailserver-Produkte unterstützen die Unterscheidung zwischen privaten und dienstlichen E-Mails auf technischer Ebene nicht.[4] Weder die Gestaltung der Zugriffsrechte noch die Einstellungen der Protokollierung erlauben eine voneinander unabhängige und unterschiedliche Behandlung von privat und dienstlich erzeugten Verbindungsdaten und E-Mails. Haben die Beschäftigten nicht eingewilligt, für private Mails die Standards der dienstlichen Nutzung zu akzeptieren, bleibt wegen der mangelhaften technischen Möglichkeiten nur die Gleichbehandlung dienstlicher und privater Mails.

1 Vgl. § 96 (2) TKG.

2 Vgl. § 93 TKG.

3 Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommuniaktionsvorgang beteiligt ist oder war (TKG § 88).

4 Das Problem scheint zwar alle Anwender zu beschäftigen, wie man vielen Veröffentlichungen und den Erfahrungen der Praxis entnehmen kann, hat es aber bei den Herstellern ganz offensichtlich noch nicht das Bewusstsein der Entwicklungsabteilungen erreicht.

Dann müssen die für Dienstbetreiber (Provider) geltenden Anforderungen für den gesamten Mailverkehr umgesetzt werden.

Werden die Mailserver jedoch gar nicht im eigenen Hause, sondern zentral bei der Konzern-IT betrieben, müssen die beschriebenen Anforderungen dennoch garantiert werden. Es stellt sich die Frage, wer in einer solchen Konstellation für die Einhaltung zu sorgen hat, wer die vom TKG geschützten Teilnehmer sind und wer gegen wen den Anspruch auf Einhaltung des TKG geltend machen kann.

Im Folgenden werden zwei Wege skizziert, auf denen die beschriebene Konstruktion datenschutzgerecht gestaltet werden kann.

Konzern-IT als Auftragnehmer gem. § 11 BDSG

Wird der Betrieb der sonstigen informationstechnischen Systeme bereits im Rahmen von Auftragsdatenverarbeitung an die Konzern-IT vergeben, so liegt es nahe, den Betrieb der Mailserver und die Erbringung der TK-Dienstleistung ebenfalls mittels dieses Konstrukts zu beauftragen. Die Konzern-IT erhält in diesem Fall einen Auftrag gemäß § 11 BDSG, die TK-Dienstleistung für die jeweilige Konzerngesellschaft zu erbringen.

Da das TKG keine Festlegungen für den Fall der Auftragsdatenverarbeitung bei TK-Diensten trifft, ist das BDSG gemäß § 1 (3) in Bezug auf die Gestaltung einschlägig. Das bedeutet, dass die Beauftragung den üblichen Anforderungen gerecht werden muss:

- Der betriebliche Datenschutzbeauftragte muss sich von der Zuverlässigkeit und Geeignetheit des Auftragnehmers überzeugen.
- Es sind erforderliche und geeignete Schutzmaßnahmen gemäß § 9 BDSG festzulegen.
- Der Vertrag muss klare Verarbeitungsanweisungen, das Verbot anderweitiger Nutzung, die verbindliche Festlegung der § 9-Maßnahmen, Kontrollmöglichkeiten für den Auftraggeber und die Genehmigungspflicht für die Vergabe von Unteraufträgen enthalten.

In einem solchen Konstrukt ist die Konzern-IT als Auftragnehmer nicht Diensteanbieter im Sinne des TKG gegenüber privat nutzenden Beschäftigten der beauftragenden Konzerngesellschaft. Vielmehr ist dies die beauftragende Konzerngesellschaft selbst, die damit gegenüber ihren Beschäftigten allen Pflichten als Diensteanbieter genauso nachkommen muss, als würde sie selbst die Mailserver betreiben. Als Verantwortliche für die Einhaltung des Fernmeldegeheimnisses muss sie diese Pflichten daher vertraglich geeignet weiterreichen, wenn sie einen Dienstleister beauftragt. Sie darf sich auch nicht mit der schriftlichen Vereinbarung begnügen, sondern muss geeignet auf die Einhaltung der vereinbarten Schutzmaßnahmen hinwirken.

Die beauftragende Konzerngesellschaft ist in dieser Konstruktion lediglich Auftraggeberin einer Auftragsdatenverarbeitung, jedoch kein Teilnehmer im Sinne des TKG. Teilnehmer sind ausschließlich die Beschäftigten, insoweit sie das Mailsystem privat nutzen.

Eine eventuell abzuschließende Betriebsvereinbarung zum Betrieb des Mailsystems muss daher das eigene Konzernunternehmen verpflichten, die vereinbarten Gestaltungsmerkmale rechtssicher und angemessen vertraglich durchzusetzen.

Die skizzierte Rechtskonstruktion unter Zuhilfenahme von § 11 BDSG kann jedoch nur gewählt werden, wenn der Auftragnehmer die Trennung der Daten der unterschiedlichen, beauftragenden Konzerngesellschaften gewährleisten kann. Dies ist ein in der Praxis häufig missachtetes Erfordernis. Da jedoch bei gemeinsam genutzten TK-Einrichtungen (Mail-Server etc.) für mehrere Konzerngesellschaften das Trennungsgebot nach Nr. 8 des Anhangs zu § 9 BDSG nicht erfüllt werden kann, wäre eine Beauftragung nach § 11 BDSG unzulässig.

Konzern-IT als klassischer Provider

Ist es nicht möglich oder nicht gewünscht, die Telekommunikationsdienstleistung durch die Konzern-IT als Auftragsdatenverarbeitung zu gestalten, so kann eine Beauftragung auch nach »klassischem Muster« erfolgen. Dabei beauftragt die Konzerngesellschaft die Konzern-IT mit der Erbringung von TK-Diensten, wie sie dies auch gegenüber einem der am Markt tätigen großen Provider tun würde. Es ist allerdings im Einzelfall zu prüfen, wie die damit verbundene Übermittlung von Beschäftigtendaten rechtmäßig zu gestalten ist.

In diesem Konstellation hat die beauftragte Konzern-IT als Diensteanbieter im Sinne des TKG zu gelten und ist direkter Normadressat der Vorgaben des TKG, insbesondere in Bezug auf das Fernmeldegeheimnis und die Datenschutz-Bestimmungen. Sämtliche Erfordernisse an die sichere und datenschutzgerechte Erbringung der TK-Dienstleistung muss die Konzern-IT dann aus eigener Zuständigkeit erbringen. Hier ist besonders die Verpflichtung zur Ergreifung angemessener Schutzmaßnahmen gemäß Anhang § 9 BDSG zu nennen.

Als Teilnehmer (und Schutzobjekte) im Sinne des TKG haben bei dieser Lösung einerseits das beauftragende Unternehmen und andererseits alle Mitarbeiter zu gelten, die TK-Dienste nutzen. Die Vertragsbeziehung zwischen Diensteanbieter und Teilnehmer, die die Grundlage für die im TKG formulierten Rechte (z. B. das Recht auf Erfüllung der Informationspflicht gem. § 93 TKG) ist, besteht mit dem beauftragenden Konzernunternehmen unmittelbar (durch einen Dienstleistungsvertrag). Für den einzelnen Mitarbeiter, der ja ebenfalls Teilnehmer ist, besteht eine mittelbare Vertragsbeziehung zur Konzern-IT durch den mit dem Arbeitgeber, der Konzerngesellschaft, bestehenden Arbeitsvertrag.

Der Vertrag zwischen Konzerngesellschaft und Konzern-IT hat in diesem Fall auch den Charakter eines »Gruppenvertrags«, der es Mitarbeitern theoretisch ermöglicht, aufgrund der Vertragskette Gruppenvertrag – Arbeitsvertrag mit der Konzern-IT direkt in Kontakt zu treten, um eventuell Rechte als Teilnehmer geltend zu machen.

Da dies in der Praxis für den einzelnen Mitarbeiter vermutlich nicht einfach umzusetzen sein dürfte, ist es wichtig, diesbezüglich konkrete Schutzregelungen in eine eventuell abzuschließende Betriebsvereinbarung aufzunehmen.

Auswirkungen auf das RZ

Die Auswahl des rechtlichen Konstrukts hat, wie oben dargestellt, Auswirkungen auf die Verantwortung für Schutzmaßnahmen und datenschutzgerechte Gestaltung der Telekommunikationsdienstleistung. Sie bestimmt außerdem, wer als Teilnehmer zu gelten hat und daher Rechte aus dem TKG geltend machen kann. Für die Konzern-

IT besteht allerdings unabhängig vom gewählten Konstrukt die Notwendigkeit, die hohen Anforderungen von BDSG und TKG in Bezug auf die Erbringung von TK-Diensten erfüllen zu müssen. Gleichgültig, ob die zu ergreifenden Schutzmaßnahmen durch Vorgaben des beauftragenden Konzernunternehmens in Folge der Verpflichtung aus einer Auftragsdatenverarbeitung diktiert werden, oder ob sie als direkte Folge aus dem TKG umgesetzt werden müssen, muss die Organisation der Konzern-IT eine datenschutzgerechte Dienstleistung für alle beauftragenden Konzerngesellschaften ermöglichen.

Neben der Erfüllung der datenschutzrechtlichen Grundpflichten (Bestellen eines betrieblichen Datenschutzbeauftragten, Führen des Verfahrensverzeichnisses, Verpflichtung der Beschäftigten auf das Datengeheimnis) muss insbesondere das Trennungsgebot angemessen umgesetzt werden. Dies bedeutet in jedem Fall eine mindestens logische Trennung der Einrichtung, Administration und des Betriebs der Postfächer unterschiedlicher Konzerngesellschaften.

Im Falle von Auftragsdatenverarbeitung ist außerdem sicherzustellen, dass die Vorgaben des Auftraggebers jederzeit ohne Auswirkungen auf den Betrieb ähnlicher Systeme für andere Konzerngesellschaften möglich sind. Da Einstellungen von Protokollen, Löschfristen und die Festlegung von Zugriffsrechten jedoch aufgrund mangelhafter Produkteigenschaften meist nur für ein gesamtes System zu treffen sind, müssen unterschiedliche Konzerngesellschaften von der Konzern-IT auf jeweils eigenen Systemen, sprich: eigenen Mailservern geführt werden. Ein gemeinsamer Betrieb von Postfächern verschiedener Konzernunternehmen auf einem Mailserver würde den Status der Auftragsdatenverarbeitung gefährden, weil die Wahrnehmung der Auftragshoheit und die Bestimmung der Verarbeitungsumstände durch den Auftraggeber in weiten Teilen aufgrund technischer Beschränkungen nicht möglich wäre.