Dietmar Jahnel

Das Versenden von e-Mails aus datenschutzrechtlicher Sicht

I. Einleitung

Bei der Versendung von e-Mails kommt es auf dem Weg vom Absender zum Empfänger zu einer Reihe von **Datenübermittlungen**. Der typische Ablauf sieht folgendermaßen aus:

- Der Absender verfasst den Inhalt der e-Mail auf seinem Arbeitsplatzrechner.
- Die Kommunikation beginnt mit der Übermittlung der Nachricht durch den Absender an den **Mail-Server** (SMTP-Server), der sich bei einem Internetserviceprovider (ISP) oder im Unternehmen selbst befinden kann.
- Der Mail-Server versendet die Nachricht an den Server der Zieladresse (**Zielserver**, POP-Server). Dieser Server kann wiederum bei einem ISP oder im Unternehmen selbst stehen.
- Am Zielserver wird die e-Mail in der Mailbox des Empfängers abgelegt und für ihn bereitgehalten, bis dieser die Nachricht tatsächlich auf seinen Rechner herunter lädt und dort uU speichert.

Der SMTP-Server kann sämtliche Aktionen protokollieren, dies muss aber nicht sein. Wird Protokoll geführt, entsteht für jede e-Mail eine Protokollzeile mit Angaben über Absender, Empfänger, Datum und Zeitpunkt der Versendung, Anzahl der übermittelten Bytes etc. Der Umfang der protokollierten Informationen lässt sich bei den meisten Mailservern einstellen. Ähnlich verhält es sich beim POP-Server, der ein Protokoll über alle eingehenden e-Mails anlegen kann, dem dann Absender, Empfänger sowie Datum und Uhrzeit der Übermittlung entnommen werden können.[1]

In diesem Beitrag werden die Übermittlungsvorgänge beim Versenden von e-Mails aus der Sicht des österr Datenschutzrechtes untersucht. Dabei wird davon ausgegangen, dass sich der Absender der Nachricht in Österreich aufhält. Alle anderen am Kommunikationsvorgang Beteiligten, sowohl Provider als auch Empfänger, können sich hingegen sowohl im Inland als auch im Ausland befinden.

[1] Vgl dazu *Gruber*, Überwachung der dienstlichen Verwendung von Internet und E-Mail, in: *Österreichische Juristenkommission* (Hrsg), Grundrechte in der Informationsgesellschaft (NWV, 2001) 167 (168 f).

II. Absender – Mailserver

Bei der Beurteilung des ersten Übermittlungsvorgangs der e-Mail vom PC des Verfassers der Nachricht an den Mailserver, sind zunächst die grundlegenden datenschutzrechtlichen Überlegungen anzustellen.

1. Personenbezogene Daten

Am Beginn steht dabei die Frage, ob personenbezogene Daten vorliegen und damit das DSG 2000[2] bzw datenschutzrechtliche Sonderbestimmungen überhaupt anwendbar sind. Nach der maßgeblichen Begriffsbestimmung des § 4 Z 1 DSG werden dabei unter personenbezogenen Daten „Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist" verstanden.

Da es bei der e-Mail prinzipiell um die Kommunikation zwischen einer Person als Absender und einer anderen Person als Empfänger geht, ist diese Voraussetzung regelmäßig erfüllt.

2. Internetserviceprovider - Begriff des „Betreibers"

In der Praxis werden beim Versenden von e-Mails die Dienste des ISPs auf verschiedene Arten in Anspruch genommen:

- Die e-Mail-Nutzung durch einen **Privatanwender** erfolgt auf der Grundlage eines Vertrages, den dieser mit einem Telekommunikationsanbieter, der als ISP fungiert, abgeschlossen hat.
- Am **Arbeitsplatz** besteht die Möglichkeit, dass der Arbeitgeber seinen Arbeitnehmern den Mailserver direkt über das Firmennetzwerk zur Verfügung stellt und damit selbst für den Internetzzugang sorgt.
- Die zweite Variante am **Arbeitsplatz** besteht darin, dass der Arbeitgeber für diese Zwecke einen Vertrag mit einem Telekommunikationsanbieter abgeschlossen hat.

Weiters ist daran zu denken, dass der e-Mail-Zugang am Arbeitsplatz rein dienstlich oder auch für Privatzwecke genutzt werden kann. Die arbeitsrechtlichen Fragen der Internetnutzung am Arbeitsplatz sind nicht Gegenstand dieses Beitrags,[3] sehr wohl aber die Fragen des Datenschutzes im Zusammenhang mit der Versendung von privaten e-Mails vom Arbeitsplatz.

Der Unterschied, ob der Zugang zum Internet durch einen externen ISP oder den Arbeitgeber selbst besorgt wird, ist für die weitere rechtliche Beurteilung von entscheidender Bedeutung. Dies deshalb, weil § 88 Abs 2 TKG[4] bestimmt, dass jeder **Betreiber** und alle Personen, die an der Tätigkeit des Betreibers mitwirken, zur Wahrung des Fernmeldegeheimnisses verpflichtet sind. Auch § 91 TKG, der die Überschrift „Datenschutz – Allgemeines" trägt, stellt auf

---

[2] BG über den Schutz personenbezogener Daten (Datenschutzgesetz 2000) BGBl I 1999/165 idF I 2001/136.

[3] Vgl dazu den Beitrag von *Posch* in diesem Band und jüngst *Laimer/Mayr*, Rechtsprobleme bei der Internetnutzung am Arbeitsplatz, ecolex 2003, 113 mit zahlreichen Hinweisen auf die Literatur zu diesen Thema.

[4] Bundesgesetz, mit dem ein Telekommunikationsgesetz erlassen wird, das Telegraphenwegegesetz, das Fernmeldegebührengesetz und das Kabel- und Satelliten-Rundfunkgesetz geändert werden sowie ergänzende Bestimmungen zum Rundfunkgesetz und zur Rundfunkverordnung getroffen werden BGBl I 1997/100 idF 2002/134.

den „Betreiber“ ab. Die Anwendbarkeit der **Sonderdatenschutzbestimmungen des TKG** ist also an den Begriff des Betreibers geknüpft. Dieser wird in § 87 Abs 3 Z 1 TKG als Anbieter von öffentlichen Telekommunikationsdiensten iSd 3. Abschnittes definiert. Unter „Telekommunikationsdienst“ versteht § 3 Z 14 TKG „eine gewerbliche Dienstleistung, die in der Übertragung und/oder Weiterleitung von Signalen auf Telekommunikationsnetzen besteht, einschließlich des Angebotes von Mietleitungen“.

IdZ war unklar, ob der **Arbeitgeber als ISP** unter den Begriff des Betreibers iSd TKG fällt. Dies wurde kürzlich vom OGH[5] klargestellt und im Wesentlichen mit folgender Argumentation verneint: Gem § 87 Abs 3 Z 1 TKG wird als „Betreiber“ der Anbieter von öffentlichen Telekommunikationsdiensten iSd 3. Abschnitts bezeichnet. Der 3. Abschnitt des TKG regelt in den §§ 12 bis 23 leg cit im Wesentlichen die anzeige- und konzessionspflichtigen Telekommunikationsdienste sowie deren Geschäftsbedingungen und Entgelte. § 3 Z 14 TKG, der den „Telekommunikationsdienst“ definiert, stellt dabei nicht auf die geschäftsmäßige, sondern die gewerbliche - auf Gewinnerzielung gerichtete - Dienstleistung ab. Daher kann der Arbeitgeber, der insoweit keinen „öffentlichen Telekommunikationsdienst“ (§ 87 Abs 3 Z 1 TKG) anbietet und auf den zudem die Bestimmungen des 3. Abschnitts des TKG keineswegs zutreffen können, auch dann nicht als Betreiber und damit als Normadressat iSd § 88 Abs 2 TKG angesehen werden, wenn er seinen Mitarbeitern das Führen privater Telefongespräche gestattet.

Diese Begründung wird – mE zu Recht – von *Thiele* kritisiert,[6] wenn auch dem Ergebnis der Urteils zuzustimmen ist. Kurz zusammengefasst handelt es sich seiner Meinung nach bei der Zurverfügungstellung eines (auch privaten) Internetzugangs durch den Arbeitgeber für seine Arbeitnehmer sehr wohl um eine gewerbliche[7] Dienstleistung iSd Definition des § 3 Z 14 TKG und damit um einen Telekommunikationsdienst. Um den Begriff des Betreibers nach § 87 Abs 3 Z 1 TKG zu erfüllen, ist es aber zusätzlich erforderlich, dass ein öffentlicher Telekommunikationsdienst angeboten wird. Weil der Arbeitgeber für seine Arbeitnehmer aber keinen **öffentlichen** Telekommunikationsdienst anbietet, stellt er auch keinen Betreiber iSd § 87 Abs 1 Z 1 leg cit dar. Entscheidend ist – nach dieser Meinung - also die fehlende Öffentlichkeit[8] und nicht die fehlende Gewerblichkeit. Das Ergebnis bleibt jedoch dasselbe: Der **Arbeitgeber**, der seinen Arbeitnehmern selbst einen Internetzugang zur Verfügung stellt, ist **kein Betreiber** nach dem TKG.

---

[5] OGH 13.6.2002, 8 Ob A 288/01p, wbl 2002/353, 518 (*Thiele*) = ecolex 2002/358, 904.

[6] *Thiele*, Anm zu OGH 13.6.2002, 8 Ob A 288/01p (wbl 2002/353, 518[522 ff]). An zwei Stellen ist die Argumentation allerdings nicht ganz schlüssig: **1.** Die im zweiten Absatz angesprochene „geschäftsmäßige“ Erbringung von Telekommunikationsdiensten ist dem österreichischen TKG fremd. Das TKG spricht in § 3 Z 14 von „gewerblich“ und in § 87 Abs 1 leg cit von „öffentlich“, der Begriff der „Geschäftsmäßigkeit“ ist im Gesetz nicht zu finden. **2.** Der Arbeitnehmer kann kein „Benutzer“ gem § 87 Abs 3 Z 3 TKG sein, weil dieser Begriff die Nutzung eines „öffentlichen“ Telekommunikationsdienstes voraussetzt. Gerade das ist ja beim Arbeitgeber als Internetprovider – mangels Öffentlichkeit - nicht der Fall!

[7] Vgl zum Begriff der „Gewerblichkeit“ die Hinweise bei *Thiele*, wbl 2002, 523.

[8] Ein weiteres Argument gegen das Vorliegen der Öffentlichkeit beim Arbeitgeber ist § 62 TKG, der für Anbieter öffentlicher Telekommunikationsdienste einen Kontrahierungszwang vorschreibt sowie zahlreiche andere Bestimmungen des TKG, die an das Vorliegen eines öffentlichen Telekommunikationsdienstes anknüpfen.

Aus datenschutzrechtlicher Sicht ist daher Folgendes zu unterscheiden:

- Prinzipiell gelten für **externe ISP** die Sonderbestimmungen des TKG, subsidiär dazu nach § 87 Abs 1 leg cit das Datenschutzgesetz[9] soweit das TKG nicht anderes bestimmt.
- Handelt es sich beim ISP jedoch um den **Arbeitgeber**, so sind die sonderdatenschutzrechtlichen Bestimmungen des TKG nicht anzuwenden, sehr wohl aber das DSG.

3. Externer Internetserviceprovider

Die Pflichten eines externen ISPs beim Empfangen der e-Mail vom Absender sind also zunächst nach dem TKG zu beurteilen:

Dieses Gesetz unterscheidet in seinen Bestimmungen über das Fernmeldegeheimnis (§ 88 TKG) und den Datenschutz (§§ 91 ff TKG) zwischen **Stammdaten, Vermittlungsdaten** und **Inhaltsdaten**. Als allgemeines Prinzip gilt, dass diese Daten nur für Zwecke der Besorgung eines Telekommunikationsdienstes ermittelt, verarbeitet oder übermittelt werden dürfen. Sonstige Übermittlungen dürfen nur auf Grund einer vorherigen schriftlichen Zustimmung des Betroffenen erfolgen, die ausdrücklich als Antwort auf ein Ersuchen des Betreibers gegeben wurde. Das TKG fordert idZ damit strengere Voraussetzungen für eine Zustimmung als das DSG.

Den Betreiber trifft weiters eine besondere **Informationspflicht**: Er ist verpflichtet, den Teilnehmer darüber zu informieren, welche personenbezogenen Daten er ermitteln und verarbeiten wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Diese Information hat in geeigneter Form, insb im Rahmen allgemeiner Geschäftsbedingungen und spätestens bei Beginn der Rechtsbeziehungen zu erfolgen.

a) Stammdaten

Bei den Stammdaten handelt es sich um alle personenbezogenen Daten, die **für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen** zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind. Konkret sind dies Familienname und Vorname, akademischer Grad, Adresse, Teilnehmernummer und Bonität.

Diese Daten dürfen von Betreibern nur für den Abschluss bzw die Beendigung von Verträgen, für die Entgeltverrechnung und die Erstellung von Teilnehmerverzeichnissen ermittelt und verarbeitet werden. Sie sind spätestens nach Beendigung der Rechtsbeziehungen mit dem Teilnehmer vom Betreiber zu löschen. Ausnahmen sind nur so weit zulässig, als diese Daten noch benötigt werden, um Entgelte zu verrechnen oder einzubringen, Beschwerden zu bearbeiten oder sonstige gesetzliche Verpflichtungen zu erfüllen.

---

[9] Und zwar wegen der Übergangsbestimmung des § 61 Abs 7 DSG in Verfassungsrang sinngemäß die Bestimmungen des DSG 2000. Der VwGH hat in seinem Erk vom 9.7.2002, 2000/01/0423 klar gestellt, dass mit dieser Übergangsbestimmung nicht die bestehenden Verweise auf das DSG 1978 „konserviert“ werden (entgegen der Auffassung von *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (Juridica Verlag, 2000) Anm zu § 61 Abs 7, 304).

b) Vermittlungsdaten

Vermittlungsdaten sind alle personenbezogenen Daten, die sich auf Teilnehmer und Benutzer beziehen und **für den Aufbau einer Verbindung oder für die Verrechnung von Entgelten erforderlich** sind. Konkret sind dies: Aktive und passive Teilnehmernummern, die Anschrift des Teilnehmers, die Art des Endgerätes, Gebührencode, Gesamtzahl der für den Abrechnungszeitraum zu berechnenden Einheiten, Art, Datum, Zeitpunkt und Dauer der Verbindung, übermittelte Datenmenge, andere Zahlungsinformationen, wie Vorauszahlung, Ratenzahlung, Sperren des Anschlusses oder Mahnungen.

Diese Daten dürfen grundsätzlich nicht gespeichert werden und sind vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren. Nur für Verrechnungszwecke dürfen die Daten solange gespeichert werden, bis die Rechnung nicht mehr beanstandet bzw der Zahlungsanspruch nicht mehr geltend gemacht werden kann.

Dem Betreiber ist es außer in den gesetzlich besonders geregelten Fällen untersagt, einen Teilnehmeranschluss über die Zwecke der Verrechnung hinaus nach den von diesem Anschluss aus angerufenen Teilnehmernummern auszuwerten. Mit Zustimmung des Teilnehmers darf der Betreiber die Daten zur Vermarktung für Zwecke der eigenen Telekommunikationsdienste verwenden.

c) Inhaltsdaten

Inhaltsdaten, also **die Inhalte der übertragenen Nachricht**, genießen einen besonderen Schutz. Sie dürfen grundsätzlich nicht gespeichert werden. Nur ausnahmsweise, nämlich sofern die Speicherung einen wesentlichen Bestandteil des Telekommunikationsdienstes darstellt, ist diese zulässig. Dies ist etwa bei e-Mail-Diensten der Fall. Die Daten sind aber jedenfalls **unmittelbar nach der Erbringung des Dienstes zu löschen**.

Der Betreiber hat durch technische und organisatorische Vorkehrungen sicherzustellen, dass Inhaltsdaten nicht oder nur in dem aus technischen Gründen erforderlichen Mindestausmaß gespeichert werden.

d) Pflichten des externen Internetserviceproviders

Der externe ISP ist als Betreiber eines öffentlichen Telekommunikations-dienstes verpflichtet, die genannten Bestimmungen des TKG betreffend Vermittlungsdaten und Inhaltdaten einhalten. Der Inhalt der e-Mails ist unmittelbar nach der Weiterleitung zu löschen. Das gleiche gilt für Vermittlungsdaten, außer deren Speicherung ist für Verrechnungszwecke notwendig.

4. Arbeitgeber als Internetserviceprovider

Bei der zweiten Konstellation, nämlich wenn der Arbeitgeber selbst die Funktion des ISPs übernimmt, ist insb die Beurteilung der Versendung von **privaten e-Mails** aus der Sicht des Datenschutzrechts von Interesse.[10] Der

[10] Die arbeitsrechtliche Literatur zur Frage der Zulässigkeit der Privatnutzung des WWW kommt jüngst zum Egebnis, dass diese vom Arbeitgeber nicht generell verboten werden

Arbeitgeber ist in diesem Fall – wie oben dargelegt[11] - kein Betreiber iSd des TKG, weshalb die datenschutzrechtlichen Sonderregelungen des TKG nicht anzuwenden sind. Er ist allerdings verpflichtet, die Bestimmungen des DSG einhalten. Es ist also die Zulässigkeit der Datenverwendung nach allgemeinem Datenschutzrecht zu prüfen.

a) Auftraggebereigenschaft des Arbeitgebers

Die Pflichten nach dem DSG treffen den datenschutzrechtlichen **Auftraggeber**. Es ist daher als erstes zu prüfen, ob der Arbeitgeber, der den Internetzugang für seine Arbeitnehmer selbst zur Verfügung stellt, die Auftraggebereigenschaft nach dem DSG erfüllt.

Nach § 4 Z 4 DSG sind Auftraggeber natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft oder die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen **die Entscheidung getroffen haben, Daten** für einen bestimmten Zweck **zu verarbeiten** und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Datenschutzrechtlicher Auftraggeber ist damit auch derjenige, der einem anderen Daten zur Herstellung eines Werkes überlässt, selbst wenn der (zivilrechtliche) Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten, außer es wurde ihm dies untersagt. Im Fall der Untersagung gilt der (zivilrechtliche) Auftragnehmer als (datenschutzrechtlicher) Auftraggeber. Das Gleiche gilt auch für Fälle, in denen der (zivilrechtliche) Auftragnehmer die Vornahme der Datenverarbeitung auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gem § 6 Abs 4 DSG **eigenverantwortlich** zu treffen hat; dieser ist dann (datenschutzrechtlicher) Auftraggeber.

Bei der Versendung von privaten e-Mails am Arbeitsplatz fällt die Entscheidung, Daten für einen bestimmten Zweck zu verarbeiten durch den Arbeitnehmer, er zieht für die Verarbeitung einen anderen heran, nämlich den Arbeitgeber. Es muss also weiter untersucht werden, ob der Arbeitgeber, der nun zum (zivilrechtlichen) „Auftragnehmer“ iSd § 4 Z 4 DSG geworden ist, die Entscheidung über die Art und Weise der Verwendung der Daten (nämlich die Speicherung und Versendung der e-Mail) **auf Grund von Rechtsvorschriften**, Standesregeln oder Verhaltensregeln eigenverantwortlich zu treffen hat. Nur wenn dies bejaht werden kann, wird der Arbeitgeber zum datenschutzrechtlichen Auftraggeber.

Um das zu beurteilen, muss die gesamte Rechtsordnung nach Rechtsvorschriften und Standesregeln durchforstet werden, aus der eine „Eigenverantwortung“ abgeleitet werden kann. Verhaltensregeln nach § 6 Abs 4 DSG wurden – soweit ersichtlich – bislang von keiner Berufsgruppe erlassen. [12]

Im konkreten Fall kann auf die Argumentation bei der Frage, ob der Arbeitgeber den Begriff Betreiber nach dem TKG erfüllt, zurückgegriffen

---

kann. Sinnvollerweise sollte eine Betriebsvereinbarung über die konkreten Nutzungsbedingungen abgeschlossen werden. Vgl *Laimer/Mayr*, ecolex 2003, 113.

[11] S II.2.

[12] Vgl die Kritik an dieser komplizierten Regelung bei *Jahnel*, Datenschutzrecht, in *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht[2] (Springer Verlag, 2002), 241 (247), *Dohr/Pollierer/Weiss*, DSG[2] (Manz Verlag, 2002) § 4 Anm 5 und *Duschanek*, Neuerungen und offene Fragen im Datenschutzgesetz 2000, ZfV 2000/1303, 526 (527).

werden. Wie oben[13] ausgeführt wurde, ist der Arbeitgeber zwar nicht Betreiber iSd § 87 Abs 3 Z 1 TKG, aber dennoch **Anbieter eines gewerblichen Telekommunikationsdienstes**. Auf diesen sind zwar nicht die Sonderdatenschutzbestimmungen des TKG anwendbar, sehr wohl aber die sonstigen Bestimmungen des TKG, soweit sie nicht auf „öffentliche" Telekommunikationsdienste Bezug nehmen. Zu denken ist etwa an §5 Abs 1 TKG, wonach die Errichtung und der Betrieb von Infrastruktureinrichtungen und Netzen zu Zwecken der Telekommunikation bewilligungsfrei ist. Anzumerken ist, dass das TKG neben dem speziellen Begriff des „Betreibers" in § 87 Abs 3 Z 1 TKG einen allgemeinen Begriff des „Betreibens" in § 3 Z 1 leg cit kennt. Danach bedeutet „Betreiben" das Ausüben der rechtlichen und tatsächlichen Kontrolle über die Gesamtheit der Funktionen, die zur Erbringung des jeweiligen Telekommunikationsdienstes notwendig sind.

Diese rechtlichen und tatsächlichen Kontrolle des Arbeitgebers bietet zumindest gute Argumente für eine **Eigenverantwortung** des Arbeitnehmers iSd § 4 Z 4 DSG, aus der seine Eigenschaft als datenschutzrechtlicher Auftraggeber folgt. Der hohe Argumentationsaufwand für dieses - auf den ersten Blick - nahe liegende Ergebnis führt die Problematik der Definition des Auftraggebers im DSG deutlich vor Augen.[14]

b) Die Zulässigkeit der Datenverwendung

Die Datenverwendung durch den Arbeitgeber besteht im konkreten Fall zunächst im Speichern der Nachricht am Mailserver, was nach der Terminologie des DSG eine **Verarbeitung** darstellt, und schließlich im Weiterleiten (nach der Terminologie des DSG eine Übermittlung) der e-Mail an den Zielserver.

Im Verhältnis Arbeitnehmer – Arbeitgeber als ISP ist zunächst die Zulässigkeit der Verarbeitung zu prüfen. Nach § 7 Abs 1 DSG dürfen die Daten nur verarbeitet werden, wenn eine entsprechende rechtliche Befugnis des Auftraggebers (hier: des Arbeitgebers als ISP) besteht und keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden.

Die **rechtliche Befugnis** des Arbeitgebers als ISP zur Speicherung der e-Mail lässt sich aus seinem Eigentum an der Computeranlage ableiten. In einem nächsten Schritt ist zu fragen, ob es sich bei e-Mails um sensible oder nicht sensible Daten handelt.

Nach § 4 Z 2 DSG sind „sensible Daten" Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihre Sexualleben. Da sich diese Informationen gegebenenfalls uU schon aus der e-Mail-Adresse des Empfängers, jedenfalls aber aus dem Inhalt der Nachricht ableiten lassen, handelt es sich bei e-Mails um **potenziell sensible Daten**.[15] Zur Beurteilung, ob schutzwürdige Geheimhaltungsinteressen der

[13] Punkt II.2.
[14] Das Ziel, damit für mehr Transparenz und eine Erleichterung der Rechtsverfolgung durch den Betroffenen zu sorgen (vgl die RV zu § 4 Z 4,5 DSG), wurde jedenfalls nicht erreicht.
[15] Ebenso: *Gruber*, in: *Österreichische Juristenkommission*, Grundrechte 167 (172).

Betroffenen verletzt sind, ist daher die strengere Bestimmung des § 9 DSG heranzuziehen.[16]

Nach § 9 Z 4 DSG sind dann schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten nicht verletzt, wenn der Betroffene seine **Zustimmung** zur Verwendung der Daten ausdrücklich erteilt hat. Dies ist anzunehmen, wenn er seine private e-Mail auf den Mailserver seines Arbeitgebers als ISP übermittelt.

5. Bestimmungen für beide Konstellationen

Unabhängig von der Anwendbarkeit des TKG gelten für beide Konstellationen im Verhältnis Absender – ISP die sonstigen Bestimmungen des DSG. Zu denken ist insb daran, dass der Absender der e-Mail als Betroffener **alle weitern Rechte nach dem DSG** gegenüber dem datenschutzrechtlichen Auftraggeber in Anspruch nehmen kann, wie insb das Recht auf Auskunft über die gespeicherten Daten, das Recht auf Richtigstellung und das Recht auf Löschung.

Sollte sich der ISP im **Ausland** befinden, so liegt eine Datenübermittlung ins Ausland vor. Diese ist genehmigungsfrei, entweder weil es sich um eine Übermittlung in ein EU-Mitgliedsland handelt (§ 12 Abs 1 DSG) oder weil der Betroffene – durch das Versenden der e-Mail - ohne jeden Zweifel seine Zustimmung zur Übermittlung seiner Daten ins Ausland gegeben hat (§ 12 Abs 3 Z 5 DSG).

III. Mailserver – Zielserver

Im Verhältnis zwischen den beiden ISP des Absenders (SMTP-Server) und des Empfängers (POP-Server) liegt eine **Übermittlung** von Daten vor, die nach § 7 Abs 2 DSG zu beurteilen ist:

- Die Daten stammen, wie eben festgestellt, aus einer zulässigen Datenanwendung am Mailserver.
- Die rechtliche Befugnis des Empfänger (Zielserver) steht im Hinblick auf den konkreten Zweck der Übermittlung einer e-Mail außer Zweifel.
- Durch Zweck und Inhalt der Übermittlung werden die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt. Vgl dazu die Begründung unter Punkt II.4.b).

Nach erfolgter Übermittlung der e-Mail stellt sich die Frage, was mit den Daten am Mail-Server zu geschehen hat. Dabei ist wieder zu unterscheiden:

---

[16] Die Versendung von e-Mails ist einer jener Fälle, in denen nicht von vornherein feststeht, ob „sensible“ oder „nicht-sensible“ Daten verwendet werden. Dies ergibt sich immer erst aus dem konkreten Fall. Das DSG 2000 stellt, wie sich aus seiner Entstehungsgeschichte ableiten lässt, bei dieser Unterscheidung primär auf jene Datenverarbeitungen ab, bei denen schon aus dem verwendeten Datenkategorien klar hervorgeht, ob darin sensible oder nicht-sensible Daten gespeichert werden sollen. Der Schutzzweck des Datenschutzrechts spricht jedoch dafür, im Zweifel die strengere datenschutzrechtliche Bestimmung – hier also § 9 DSG und nicht § 8 DSG – anzuwenden (vgl *Gruber*, in: *Österreichische Juristenkommission*, Grundrechte 172, FN 27).

1. Externer Internetprovider

Befindet sich der Mailserver bei einem Betreiber eines öffentlichen Telekommunikationsdienstes in Österreich, so ist dieser verpflichtet, die oben[17] genannten Bestimmungen des TKG einzuhalten. Er muss also den Inhalt der e-Mail unmittelbar nach der Weiterleitung löschen. Die Vermittlungsdaten sind ebenfalls sofort nach Weiterleitung der e-Mail zu löschen. Sie dürfen nur dann gespeichert werden, wenn dies für Verrechnungszwecke erforderlich ist, was bei e-Mails regelmäßig nicht der Fall sein wird.

2. Arbeitgeber als Internetprovider

Für den Arbeitgeber als ISP hingegen gelten die allgemeinen Bestimmungen des DSG. Nach den Grundsätzen für die Verwendung von Daten nach § 6 Abs 1 DSG dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden (Z 2 leg cit) bzw nur solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist (Z 5 leg cit). Nach § 27 DSG hat jeder Auftraggeber Daten aus eigenem zu löschen, sobald ihm die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist.

Die Regelungen des DSG sind flexibler als die strikte Löschungsverpflichtung nach dem TKG und schließen eine Kontrolle durch den Arbeitgeber nicht von vornherein aus.

Die Frage, ob der Arbeitgeber die Nutzung des Internet durch Arbeitnehmer überwachen darf, wurde bislang fast ausschließlich aus der Sicht des Arbeitsrechts diskutiert. Das Datenschutzrecht wurde zwar auch angesprochen, jedoch blieb es bislang meist bei einer Darstellung der allgemeinen Prinzipien.[18]

Bei einer **Kontrolle des e-Mail-Verkehrs** am Server durch den Arbeitgeber handelt es sich in der Terminologie des DSG um ein „Verarbeiten von Daten“ nach § 4 Z 9 leg cit, konkret kommen aus der dort angeführten Liste vor allem Ermitteln und Abfragen in Frage.

Da sich die Art und Weise der Protokollierung am Mail-Server einstellen lässt, stellt sich die Frage, welche Daten der Arbeitgeber zulässigerweise speichern darf, um das Ausmaß der Internetnutzung zu kontrollieren. § 7 Abs 3 DSG führt als weitere Voraussetzung der Zulässigkeit einer Datenverwendung an, dass die Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und **mit den gelindesten zur Verfügung stehenden Mitteln** erfolgen dürfen. Daraus folgt, dass der Arbeitgeber auf seinem Mail-Server nach

---

[17] Vgl II.3.

[18] *Thiele*, Internet am Arbeitsplatz, ecolex 2001, 613 (614); *Dellisch*, Private E-Mail und Internetnutzung am Arbeitsplatz; ASoK 2001, 316. Bisher hat sich – soweit ersichtlich – lediglich *Gruber*, in: *Österreichische Juristenkommission*, Grundrechte näher mit dem Arbeitsrecht und dem Datenschutzrecht hinsichtlich der Protokollierung durch den Arbeitgeber auseinandergesetzt. ME ist aber die Art der Fragestellung etwas zu modifizieren: Es ist zu fragen, welche Daten durch den Arbeitgeber zulässiger Weise protokolliert werden dürfen. *Gruber* hingegen untersucht die datenschutzrechtliche Zulässigkeit der tatsächlich vorgenommenen Protokollierungen.

Übermittlung der e-Mail nur so viel protokollieren darf, als für die Erreichung der Kontrollzwecke unbedingt erforderlich ist.

Damit ist die Zulässigkeit der Protokollierung von der konkreten arbeitsrechtlichen Situation am Arbeitsplatz abhängig. In Frage kommen ein Nutzungsverbot, das Vorliegen einer Einzel- oder Betriebsvereinbarung über das Ausmaß der Privatnutzung, die Erlaubnis einer unbeschränkten Privatnutzung und das Fehlen einer Vereinbarung.

a) Vereinbarung über eingeschränkte Privatnutzung

Wenn eine Vereinbarung (im Arbeitsvertrag oder in Form einer Betriebsvereinbarung) über die **eingeschränkte Zulässigkeit der Privatnutzung** von e-Mail vorliegt, ist zur Überwachung dieser Vereinbarung eine umfassende Protokollierung des e-Mail-Verkehrs auf dem Mailserver notwendig. Nur durch Aufzeichnung von e-Mail-Adresse des Absenders und des Empfängers kann zwischen dienstlichen und privaten Mails unterschieden werden. Der Inhalt der Nachricht ist für diese Kontrollzwecke nicht notwendig und muss daher gelöscht werden.

Datenschutzrechtlich ist die Protokollierung und allfällige Auswertung dieser Daten nach § 9 DSG zu beurteilen, weil es sich dabei - wie bereits begründet[19] - um potenziell sensible Daten handelt. Die Datenverwendung ist erlaubt, wenn der Arbeitnehmer seine **Zustimmung** ausdrücklich erteilt hat (§ 9 Z 6 DSG). Als weiterer Grund für die Zulässigkeit kommt § 9 Z 11 DSG in Betracht, wonach die Verwendung erforderlich sein muss, um den Rechten und Pflichten des Arbeitgebers auf dem Gebiet des Arbeits- oder Dienstrecht Rechnung zu tragen und sie nach besonderen Rechtsvorschriften zulässig ist. Hier stellt sich die Frage, ob eine Betriebsvereinbarung zB nach § 96 Abs 1 Z 3 ArbVG[20] bzw – falls es keinen Betriebsrat gibt – eine Zustimmung nach § 10 AVRAG eine derartige „Rechtsvorschrift“ darstellt.[21] Wenn man diese Frage – mE nach mit guten Gründen - verneint, bleibt nur die ausdrückliche Zustimmung als Grundlage der Zulässigkeit der Protokollierung.

IdZ ist noch darauf hinzuweisen, dass der Arbeitgeber nach § 14 Abs 2 Z 7 DSG verpflichtet ist, seine **Kontrollzugriffe** auf die Protokolldateien wiederum zu **protokollieren**, damit seine Abfragen und Übermittlungen im Hinblick auf ihre Zulässigkeit nachvollzogen werden können.

b) Fehlende Vereinbarung, Nutzungsverbot

Besteht keine Vereinbarung hinsichtlich der Privatnutzung von e-mail, so wird angenommen, dass diese im „ortsüblichen“ Ausmaß zulässig ist und zwar abhängig von den konkreten Umständen des Einzelfalls während oder außerhalb der Arbeitszeit.[22] Auch in diesem Fall ist zur Kontrolle, ob dieses Ausmaß nicht überschritten wird, eine **umfassende Protokollierung** des e-

---

[19] Siehe Punkt II.4.b).
[20] Vgl dazu von *Posch*, xxx in diesem Band.
[21] So offenbar *Gruber*, in: *Österreichische Juristenkommission*, Grundrechte, 173, während *Drobesch/Grosinger*, DSG, Anm zu § 9 Z 11, 146 meinen, dass eher eine „gesetzliche Vorschrift“ wie in § 9 Z 3 DSG notwendig ist
[22] *Laimer/Mayr*, ecolex 2003, 113 (114); ebenso *Posch*, xxxx.

Mail-Verkehrs nötig, die datenschutzrechtlich ebenso zu beurteilen ist, wie bei Vorliegen einer Vereinbarung über eine eingeschränkte Privatnutzung.

c) Keine Einschränkung der Privatnutzung

Gibt es hingegen keine Einschränkung der privaten e-Mail-Nutzung am Arbeitsplatz, so ist auch **keine Protokollierung** der beim e-Mail-Versand anfallenden Daten **nötig**. Die Daten am Mailserver sind daher zu löschen.

d) Informationspflicht

In allen Fällen, in denen eine zulässige Protokollierung erfolgt, ist der Arbeitgeber als datenschutzrechtlicher Auftraggeber nach § 24 DSG verpflichtet, den Arbeitnehmer **über den Zweck der Speicherung zu informieren**. Die Informationspflicht über Name und Adresse des Arbeitgebers entfällt im konkreten Fall, weil diese Informationen bereits vorliegen. Die Ausnahmetatbestände des § 24 Abs 3 DSG kommen bei der Protokollierung der e-Mail-Adressen von Absender und Empfänger nicht in Betracht.

3. Zielserver im Ausland

Erfolgt eine Übermittlung an einen Zielserver im Ausland, ist diese aus den unter II.5. genannten Gründen zulässig.

IV. Zielserver – Empfänger

Im Verhältnis zwischen dem ISP des Empfängers (Zielserver) und dem Empfänger der e-Mail kommt es zu einer **Übermittlung** von Daten, die datenschutzrechtlich wie unter Punkt III. zu beurteilen sind. Auch hier liegt der wesentliche Unterschied darin, ob ein externer ISP oder der Arbeitgeber selbst den e-Mail-Verkehr abwickelt.

V. Zusammenfassung

Bei der datenschutzrechtlichen Beurteilung des Versendens von e-Mails ist zunächst zu unterscheiden, ob der e-Mail-Dienst durch einen externen ISP oder durch den Arbeitgeber selbst geleistet wird. Im ersten Fall gelten die Sonderdatenschutzbestimmungen des TKG neben dem DSG, im zweiten Fall ausschließlich das DSG.

Ein externer ISP hat nach Übermittlung der Daten sowohl den Inhalt der e-Mail als auch die Vermittlungsdaten unverzüglich zu löschen. Der Arbeitgeber als ISP hingegen muss zwar die Nachricht selbst ebenfalls löschen, darf aber die e-Mail-Adressen von Absender und Empfänger zu Zwecken der Kontrolle des Umfangs der e-Mail-Nutzung speichern und abfragen, außer wenn die Privatnutzung von e-Mail ohne jede Einschränkung erlaubt ist. Da es sich dabei um potenziell sensible Daten handelt, ist dazu jedoch die ausdrückliche Zustimmung des Arbeitnehmers erforderlich.