

Arbeitgeber ist Diensteanbieter trotz Verbot privater Nutzung

Nach den Teledienstgesetzen wird mit der Einrichtung von personenbezogenen dienstlichen E-Mail-Adressen in Betrieb und Verwaltung jeder **Arbeitgeber zum Teledienstanbieter** i. S. des Gesetzes, da es sich hierbei auch um die technische Ermöglichung des Empfangs von E-Mails mit privatem Inhalt handelt. Nach § 3 Nr. 6 TKG ist »**Diensteanbieter**« jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt. Nach § 3 Nr. 10 TKG ist »**geschäftsmäßiges Erbringen von Telekommunikationsdiensten**« das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht. Im Sinne des Telemediengesetzes TMG bezeichnet der Ausdruck »Diensteanbieter« jede natürliche oder juristische Person, die eigene oder fremde Teledienste zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt, und »Nutzer« jede natürliche Person, die Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen.

E-Mail-Adressen sind weltweit zu recherchieren. Damit kann nach Einrichtung einer solchen personenbezogenen dienstlichen Adresse niemand als Empfänger/in gewollter oder ungewollter private E-Mails ausgeschlossen werden. Nach den Teledienstgesetzen erfordert dies auch eine Einverständniserklärung aller technischen Kommunikationsnutzer/innen bezüglich der hierbei zu erfassenden bzw. erfassten Daten. Ferner greifen hier die gesetzlichen Bestimmungen über das **Post- und Fernmeldegeheimnis** (vgl. § 88 TKG und §§ 202 – 206 StGB). Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von Internetdiensten oder E-Mail erlaubt oder duldet, ist er ihnen gegenüber also Telekommunikations- bzw. Telediensteanbieter. Ein vom Arbeitgeber beauftragter Zugangsanbieter ist zwar diesem gegenüber Telekommunikations- bzw. Telediensteanbieter. Gegenüber den privat nutzenden Beschäftigten sind die Provider aber lediglich Auftragnehmer des dann als Anbieter zu qualifizierenden Arbeitgebers. Selbst das mögliche Untersagen der privaten Nutzung ändert also nichts an dem Status des Telediensteanbieters bei Beibehaltung der personenbezogenen E-Mail-Adressen.

Dem Fernmeldegeheimnis unterliegen der **Inhalt** der Telekommunikation und ihre **näheren Umstände**, insbesondere die Tatsache, ob **jemand** an einem Telekommunikationsvorgang **beteiligt** ist oder war. **Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.** Zur Wahrung des Fernmeldegeheimnisses ist verpflichtet, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt. Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist (vgl. § 88 TKG). Eine vorgesehene Einwilligung der Arbeitnehmer in Speicherung der Nutzungsdaten für konkret beschriebene Zwecke ist zulässig (z. B. transparente Missbrauchskontrolle unter Einbeziehung der Betroffenen, Personalrat, Datenschutzbeauftragter mit Ausschluss einer **darüber hinausgehenden Leistungs- und Verhaltenskontrolle**). Die Speicherung des **Inhalts** privater E-Mails ist unzulässig. Hier gilt das Telekommunikationsgeheimnis uneingeschränkt.

Zur Sicherung des Erhalts und zeitnahen Bearbeitung sind neben den bestehenden persönlichen E-Mail-Adressen vermehrt entsprechend der Dienststellenstruktur nach betrieblichen Organisationseinheiten gezeichnete funktionale E-Mail-Adressen einzurichten, die in Publikationen und Korrespondenz mit dem Hinweis verwandt werden, dass nur an diese Adressen Nachrichten oder Anfragen zu richten sind. Bezüglich der **funktionalen**, aber nicht persönlichen **E-Mail-Adressen** ein Verfahren zur Weiterleitung an die zuständigen bzw. vertreten-

den Kolleginnen oder Kollegen einzurichten, ist in mehrfacher Hinsicht sinnvoll. Hierfür bedarf es auch **keiner Einverständniserklärung** eines Betroffenen.

Die Adresse vorname.name@firma.de ist eine **personenbezogene dienstliche E-Mailadresse** aber **keine funktionale betriebliche E-Mailadresse** wie oftmals behauptet!

Für den Fall der überraschenden Verhinderung mit unterbliebenem Aufruf eines Abwesenheitshinweises und des Vertretungserfordernisses, wäre systemtechnisch ein Abwesenheitsassistent mit Hinweis auf aktuelle Verhinderung der Kenntnisnahme und der Aufforderung, dienstliche Mitteilungen an eine zu benennende E-Mail-Adresse erneut zu senden, vorzusehen.

Zur **Offenlegung dienstlicher E-Mails** gilt grundsätzlich das Verfahren wie bei sonstiger dienstlicher Post: Die dienstliche E-Mail-Nachricht ist nicht das Eigentum der/s jeweiligen Beschäftigten, sondern bleibt trotz personenbezogener dienstlicher E-Mail-Adresse Eigentum der Einrichtung bzw. des Unternehmens und ist für die jeweils bestimmten Zwecke den jeweils berechtigten Zuständigen offen zu legen. Dies rechtfertigt jedoch noch **keinen Zugriff** des Arbeitgebers oder dessen Beauftragten, also weder einer hierarchisch gleichrangigen noch vor- oder nachgeordneten Kollegin bzw. eines Kollegen, auf das E-Mail-Programm der Beschäftigten, wenn dort gleichzeitig private E-Mails einsehbar sind.

Ausnahmen von der Offenlegung dienstlicher E-Mails sind allerdings in der Tätigkeit bezüglich eines **Berufs- oder Amtsgeheimnisses § 203 StGB** wie bei z.B. Rechtsanwälten (mit Rechtschutzaufgaben Beauftragte und deren Hilfsbeschäftigte) Betriebsräte, Sozialpädagogen, Datenschutzbeauftragten u.a. begründet.

Besonderen Schutz und ausdrückliche freiwillige Einwilligungserklärungen zur Datenweitergabe bedürfen z.B. **sensible Daten** nach § 3 Abs. 9 BDSG. Dies sind Angaben über die **rasische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit** oder **Sexualleben**. So muss z. B. in einer Sachbearbeitung nicht jede/r Beschäftigte wissen, worum es da geht, welche Krankheiten, philosophische Überzeugungen oder das Sexualleben eine Rolle spielen. Nicht auszuschließen ist die Kenntnis all derjenigen, die im Rahmen der Arbeitsorganisation damit sachlich befasst sind. Hier darf aber ein ansonsten bestehendes Zugriffsberechtigungskonzept nicht unterlaufen werden.

Das Verfahren einer administrativ geregelten **Passwortweitergabe** oder eingerichtete **Weiterleitung an andere Beschäftigte** ist bei personenbezogenen E-Mail-Adressen datenschutz- und strafrechtlich als rechtswidrig abzulehnen. Es ist schon deshalb nicht geeignet, weil eben ein rechtswidriger Zugriff auf private Daten damit ermöglicht wird.

Der Zugriff auf eine andere als die eigene personenbezogene E-Mail-Adresse (z. B. vorname.name@behörde.de) ist **ohne vorherige freiwillige schriftliche Zustimmungserklärung** der/des Betroffenen datenschutzrechtlich nicht zulässig und kann wegen selbst zu verantwortender Verletzung des Fernmeldegeheimnisses und/oder der Verleitung einer/s Untergebenen zur Verletzung des Fernmeldegeheimnisses als strafbare Handlung geahndet werden (vgl. §§ 206 und 357 StGB).

Ferner muss eine Forderung an eine/n Beschäftigten, **freiwillig eine schriftliche Einverständniserklärung** bezüglich des Zugriffs einer/s anderen Beschäftigten auf die persönliche Firmen E-Mail-Adresse abzugeben, vergleichsweise so abwegig erscheinen wie das Verlangen der Kenntnisgabe privater Post mittels Kopien an Arbeitskolleg/innen oder Vorgesetzte.

Bei Nutzung des **Cc-Verteilers** bietet E-Mail z.B. bei Versand an mehrere Adressaten in verschiedenen Betrieben auch die allgemeine und somit ungewollte Feststellung einer Zugehörigkeit zu einem »sensitiven« **Informationsverteiler** und einer sehr nahe liegenden Mitgliedschaft und Aktivität. So ist z.B. die gewerkschaftliche Mitgliedschaft eine Information, die nur im Rahmen des rechtsgeschäftsähnlichen Schuldverhältnisses und den genannten Erlaubnistatbeständen nach den speziellen Bestimmungen BDSG zu den als besonders schutzwürdig bestimmten Daten einer Gewerkschaftsmitgliedschaft erfasst, verarbeitet oder weitergegeben werden darf.

Als ungesicherte E-Mail mit dem **Empfängerverteiler Cc** ist wegen der vielfältigen Lese- und Protokollier- und Weiterleitungsmöglichkeiten nicht einmal der Empfängerkreis abschließend definiert. Darüber hinaus liegt in der Regel für ein solches Verfahren die gesetzlich geforderte Einverständniserklärung nicht vor. Folglich können hier Ordnungswidrigkeiten nach § 43 BDSG durch die Aufsichtsbehörde festgestellt werden. Ferner sind Schadensersatzansprüche von Betroffenen (z.B. wegen Nichtzustandekommens eines Arbeitsvertrages nach Kenntnisaufnahme aus E-Mail-Verteiler, aber auch andere ohne materielle Folgen) nicht auszuschließen (vgl. §§ 7 und 8 BDSG). Deshalb ist in den Fällen der Offenlegung eines sensitiven Datums eine E-Mail-Nutzung mit der Cc-Empfängerliste als rechtswidrig zu bewerten. Als diesbezüglich rechtlich korrekte Alternative ist hierzu das **Bcc-Adressenfeld** zu nutzen (Bcc = blind carbon copy ~ unsichtbarer Durchschlag, Blindkopie).

Grundsätzlich ist festzustellen, dass **ungesicherte** – also wie bislang allgemein üblich nicht verschlüsselte – E-Mails vielfältige **Angriffsmöglichkeiten** gegen eine vertrauliche Kommunikation bieten:

- Der Weg einer E-Mail im Internet ist nicht vorherzubestimmen.
- Nachrichten können eingesehen, verändert und verfälscht werden.
- Ferner können Kommunikationsprofile erstellt werden.

Der Begriff des **Telediensteanbieters** bezüglich des Begriffs des Unternehmens i. S. v. § 206 StGB ist weit auszulegen. Hierunter ist jede Betätigung im geschäftlichen Verkehr anzusehen, die nicht ausschließlich hoheitlich erfolgt oder auf eine private Tätigkeit beschränkt ist. Stellt eine Dienststelle ihre Telekommunikationseinrichtungen zu Versendung und Empfang elektronischer Post (E-Mail) ihren Mitarbeitern und anderen Nutzergruppen auch für private und wirtschaftliche Zwecke zur Verfügung, so wird sie damit außerhalb ihres hoheitlichen Aufgabengebietes tätig und ist als Unternehmen i. S. v. § 206 StGB anzusehen. Dem Tatbestandsmerkmal »**unbefugt**« kommt in § 206 StGB eine Doppelfunktion zu.

Ein Einverständnis schließt bereits die Tatbestandsmäßigkeit des § 206 StGB aus, im Übrigen handelt es sich um ein allgemeines **Rechtswidrigkeitsmerkmal**. Als Rechtfertigungsgründe für Eingriffe in das Post- und Fernmeldegeheimnis kommen Erlaubnissätze in Betracht, die in einer gesetzlichen Vorschrift, d.h. in einem formellen Gesetz oder einer Rechtsverordnung niedergelegt sind, und die sich ausdrücklich auf Postsendungen, den Postverkehr oder Telekommunikationsvorgänge beziehen. Auch ein Rückgriff auf allgemeine Rechtfertigungsgründe ist möglich, so dass das technische Herausfiltern einer E-Mail gerechtfertigt sein kann, wenn ansonsten Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten können. Im Klageerzwingungsverfahren kann die Staatsanwaltschaft durch eine gerichtliche Entscheidung zur Aufnahme von Ermittlungen aufgefordert werden, wenn sie eine Strafbarkeit aus unzutreffenden rechtlichen Gründen verneint (vgl. OLG Karlsruhe, Beschluss v. 10.1.2005 – 1 Ws 152/04 –, CR 2005, 288).

Zur Frage, ob Unternehmen, die ihren Mitarbeitern auch die private Internetnutzung gestatten oder technisch vorsehen, nach **§ 113a TKG der Pflicht zur Vorratsdatenspeicherung**

unterliegen und die den MitarbeiterInnen zuzuordnenden Verkehrsdaten deshalb für die Dauer von 6 Monaten speichern müssen, gibt es wie immer unterschiedliche Ansichten.

Arbeitgeber werden als TK-Anbieter i.S.d. TKG qualifiziert, sofern sie ihren Arbeitnehmern auch die private Nutzung ihrer Telekommunikationseinrichtungen gestatten und diese technisch ermöglichen. Bereits dies wird von einigen Juristen bestritten, die dies in Frage stellen, weil sich Arbeitgeber und Arbeitnehmer nicht in einem Verhältnis von Anbieter und Nutzer gegenüberstehen sollen, sondern der internetfähige Arbeitsplatz-PC lediglich ein Werkzeug sei, mit dessen Hilfe ArbeitnehmerInnen ihre Pflichten aus dem Arbeitsvertrag erfüllen. Diese Ansicht teile ich nicht, da sie außer Acht lässt, dass der Arbeitgeber jede aktive und passive Kommunikation mittels seiner technischen Ausstattung ermöglicht.

Entscheidend ist aber in jedem Fall, dass § 113a TKG die Erbringung **öffentlich zugänglicher TK-Dienste** verlangt. In der Gesetzesbegründung heißt es hierzu wörtlich: "Daraus folgt zugleich, dass für den nicht öffentlichen Bereich (z. B. unternehmensinterne Netze, Nebenstellenanlagen oder E-Mail- Server von Universitäten ausschließlich für dort immatrikulierte Studierende oder Bedienstete sowie die Telematikinfrastruktur im Gesundheitswesen) eine Speicherungspflicht nicht besteht."

Der betriebliche Zugang zum Internet, der ausschließlich den Unternehmensangehörigen zur Verfügung steht, unterliegt also nicht der Vorratsdatenspeicherung!

Datenschutzrechtliche Hinweise zu einer Betriebsvereinbarung E-Mail Outlook

1. Dienstliche und private e-mails werden systemtechnisch gleich behandelt (Viren, Spam)
2. Anregung privater e-mail-account und Weiterleitung privater e-mails an diesen auch zum Zwecke der Beantwortung
3. Warum soll der firma.de-Absender für private e-mails genutzt werden??? –reicht dafür nicht auch gmx.de, t-online.de u.a.?!?!
4. Weiterleitungen von einer personenbezogenen Firmen-E-mail-Adresse bedürfen auch das Einverständnis der neuen Zielperson
5. Das verlangte Gewähren eines lesenden und/oder schreibenden Zugriffs **auf sein/ihr Postfach und alle anderen Funktionen** von Outlook durch Freigaben an andere Beschäftigte ist nicht mit einer Zweckbestimmung (§28 Abs. 1 Satz 2 BDSG) und der Freiwilligkeit einer Einverständniserklärung vereinbar?
6. Personen nach § 203 StGB und 120 BetrVG sind auszunehmen bzw. deren Daten gesondert zu behandeln.
7. Das Verfahren bei unvorhergesehener Abwesenheit ist konkret zu beschreiben incl. Information der Betroffenen
8. Hinweise zur Nutzung der Adressverzeichnisse AN:, Cc:, Bcc: und nicht lesbare Verteiler und deren Einrichtung
9. Empfehlung ist die verschlüsselte Versendung von personenbezogenen Daten, Listen etc z.B. an Lettershops oder auch an andere Aktive
10. Was sind die Administrationszwecke der Auswertung und welche Zwecke sollen ganz praktisch damit verfolgt werden?
11. Kalenderfunktionen: Privateinträge innerhalb der Bürozeiten oder auch danach und am WE ???, was ist mit länger krank, Kur, Urlaub ??? – hoffentlich nur = abwesend! –Aber auch da mangelt es an der Zweckbestimmung – s. 12.

12. Sind wirklich alle dienstlichen Einträge eine zweckbestimmte Information für andere Arbeitskollegen, die eben nicht in der Rolle „Vorgesetzter“ oder Personalleitung sind? Wie wird hierbei das Amts- oder Berufsgeheimnis § 203 StGB gewahrt?
– Falls nicht, sind DS-Probleme zu erkennen!
Oder Regelung für sog. teilautonome Arbeitsgruppen!
13. Spamfilterung gilt auch für private Mails s.o.
14. arbeitsrechtliches Beweis- und Verwertungsverbot von zu unrecht erhobenen Daten für arbeitsrechtliche Maßnahmen
15. Einverständniserklärung aller betroffenen Beschäftigten zum Umgang mit ihren Kommunikationsdaten bezüglich § 88 TKG zur Vermeidung des Vorwurfes der strafbaren Handlung nach § 206 StGB
16. Beschreibung der zu nutzenden (von wem?) Funktionen von Outlook, Tools und Programmierfunktionen – Qualifikationsbedarf (technisch und rechtlich)

Gez. Norbert Warga



GESELLSCHAFT FÜR DATENSCHUTZ
UND DATENSICHERUNG e.V.