➜ Zum Thema

Über die Autoren:
Dr. Christoph Ludvik, BSc (WU) ist Rechtsanwalt in der Kanzlei Herbst Kinsky RAe in Wien.
Christoph Hördinger, LLM. (WU), LLB. (WU), war Rechtsanwaltsanwärter ebenda und absolviert aktuell die Gerichtspraxis im OLG Sprengel Wien.
Kontaktadresse: Herbst Kinsky Rechtsanwälte GmbH, Dr.-Karl-Lueger-Platz 5, 1010 Wien.
Tel: +43 (0)1 904 21 80,
E-Mail: christoph.ludvik@herbstkinsky.at,
Internet: www.herbstkinsky.at
Von den Autoren erschienen:
C. Ludvik, Urlaubsverfall bei Arbeitnehmeraustritt, ASoK 2022/1, 2;
C. Ludvik, Der internationale Betrieb – Fragen der grenzüberschreitenden Betriebsverfassung (2021);
C. Ludvik/Zwinger, Nachvertragliche Wettbewerbsbeschränkungen arbeitnehmerähnlicher Personen, in *Brameshuber/Friedrich/Karl,* FS Franz Marhold (2020) 157;
Brameshuber/C. Ludvik, Sozialrechtlicher Missbrauch, in *Kalss/Bergmann,* Handbuch Rechtsformwahl (2020) 189;
Marhold/C. Ludvik, Thoughts about indexing family benefits: Are authorities permitted to apply the Austrian indexation of family benefits? The primacy of EU law and the right/obligation to request a ruling from the Court of Justice of the European Union, EJSS 2020/22/3, 273.
Literatur:
Determann/Hitz, Die private Nutzung von Internet und E-Mail, ASoK 2019, 55; *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[2] (2018);
Körber-Risak/Lurf, Individualarbeitsrechtliche Aspekte unternehmensinterner Untersuchungen, ZAS 2017/35, 191;
Przeszlowska, Internet und E-Mail am Arbeitsplatz, ARD 6392/6/2014.

Pflichtenverletzung bei digitaler Kommunikation im Arbeitsverhältnis

Ausgewählte Praxisszenarien und ihre Konsequenzen

In der Praxis kommt es zunehmend vor, dass Arbeitnehmer berufliche E-Mails an ihre private E-Mail-Adresse weiterleiten oder Anhänge (Daten) auf ihrem eigenen PC oder in der „Cloud" abspeichern. In den meisten Fällen erfolgt dies ohne Hintergedanken und ohne Bewusstsein darüber, dass solche Handlungen jedoch gravierende rechtliche Folgen für den Arbeitnehmer und Arbeitgeber mit sich bringen können. Aus Sicht des Arbeitgebers ist eine private Speicherung meist unerwünscht, weil damit unkontrolliert Daten aus dem Unternehmen abfließen. Besondere Brisanz erlangen diese Speichervorgänge bei der Beendigung von Arbeitsverhältnissen, wo sich diverse rechtliche „Grauzonen" auftun.

Von Christoph Ludvik und Christoph Hördinger

GRAU 2022/5

Inhaltsübersicht:

▶ Arbeitsrecht

A. Allgemein

Digitale Kommunikation im Arbeitsverhältnis betrifft und erzeugt zugleich Unternehmensdaten. Als „Unternehmensdaten" werden für die Zwecke dieses Beitrags alle Daten verstanden, die durch elektronische Datenverarbeitung in einem Unternehmen entstehen. Eine wichtige Quelle von Unternehmensdaten ist der betriebliche E-Mail-Verkehr, seien es die E-Mails selbst oder ihre Anhänge.

Verfügungsberechtigter der Unternehmensdaten ist grundsätzlich der Unternehmer. Dieser darf als Arbeitgeber über die von den Arbeitnehmern generierten Unternehmensdaten im Grundsatz frei verfügen, dh Anhänge und E-Mails lesen, bearbeiten, löschen usw. Handelt es sich hingegen um digitale Kommunikation ohne betrieblichen Bezug, dh solche mit privatem Inhalt, hat der Arbeitgeber keine unbeschränkte Verfü-

gungsbefugnis.[1] Diese Art von Daten kann infolge einer erlaubten oder unerlaubten privaten Nutzung des dienstlichen E-Mail-Accounts entstehen.[2]

In Hinblick auf die Nutzung des betrieblichen E-Mail-Accounts sind mannigfaltige Szenarien vorstellbar, in denen Arbeitnehmer in die Hoheitsgewalt des Arbeitgebers, über betriebliche Daten zu verfügen, eingreifen. Nachfolgend werden beispielhaft **drei gängige Szenarien** dargestellt, auf die im Laufe dieses Beitrages immer wieder Bezug genommen wird:

- Der **Arbeitnehmer A** leitet regelmäßig E-Mails vom betrieblichen Account auf seine private E-Mail-Adresse weiter. Diese Mails beinhalten unter anderem Anhänge mit sensiblen Unternehmensdaten.
- Der **Arbeitnehmer B** speichert betriebliche E-Mails samt sensiblen Anhängen auf seinem privaten PC ab. Bei Beendigung des Arbeitsverhältnisses stellt er die Daten nicht an den Arbeitgeber zurück.
- Der **Arbeitnehmer C** löscht während des bestehenden Dienstverhältnisses und bei Beendigung alte E-Mails am betrieblichen PC. Diese E-Mails enthalten neben privaten Daten des Arbeitnehmers auch Unternehmensdaten.

In allen drei Szenarien handeln die Arbeitnehmer ohne Kenntnis oder Zustimmung des Arbeitgebers.

B. Pflichten der Arbeitnehmer beim Umgang mit Unternehmensdaten

Die Arbeitnehmer unterliegen beim Umgang mit betrieblichen Daten mehreren Pflichten. Diese ergeben sich zum einen aus dem **Arbeitsrecht** und zum anderen aus dem **Datenschutzrecht.** Zusätzlich sind Verpflichtungen aus dem **Wettbewerbsrecht** zu beachten.[3]

1. Arbeitsrechtliche Vorgaben

Unternehmensdaten haben für den Unternehmer (Arbeitgeber) eine besondere Bedeutung, wenn es sich bei diesen um **Betriebs- und Geschäftsgeheimnisse** handelt. Darunter versteht man unternehmensbezogene Tatsachen technischer oder wirtschaftlicher Art, die nur einem bestimmten und begrenzten Personenkreis bekannt sind und die Außenstehenden nur schwer oder gar nicht zugänglich sind.[4] Beispiele für Betriebs- und Geschäftsgeheimnisse sind etwa Kundendaten, Preiskalkulationen und Strategien sowie technische Methoden. Solche Daten finden sich auch häufig im betrieblichen E-Mail-Verkehr wieder, insbesondere wenn die E-Mail-Kommunikation zum unternehmensinternen Austausch von Dateien (in Anhängen) verwendet wird. In allen aufgelisteten Szenarien (Punkt A) besteht daher die Gefahr, dass es zu einer Verletzung der Verschwiegenheitspflicht durch die Arbeitnehmer kommt, weil diese (mit mehr oder weniger Bewusstsein) Tatsachen preisgeben, an deren Geheimhaltung der Arbeitgeber ein rechtliches Interesse hat.

Aus der Treuepflicht des Arbeitnehmers gegenüber seinem Arbeitgeber wird eine **Verschwiegenheitspflicht** in Hinblick auf die Geschäfts- und Betriebsgeheimnisse des Arbeitgebers abgeleitet.[5] Die Verschwiegenheitspflicht des Arbeitnehmers beschränkt sich aber nicht allein auf das Verbot der Weitergabe von Betriebs- und Geschäftsgeheimnissen, vielmehr werden diese Pflichten innerhalb des Arbeitsverhältnisses auch auf sämtliche nicht allgemein bekannten Tatsachen, an deren Geheimhaltung der Arbeitgeber **ein objektives berechtigtes Interesse** hat, erstreckt.[6]

Neben dieser allgemeinen Verschwiegenheitspflicht normieren einige Sondergesetze zudem besondere **berufsbezogene Verschwiegenheitspflichten.**[7] Weitere Grundlagen für Verschwiegenheitsverpflichtungen ergeben sich für Arbeitnehmer aus Geheimhaltungsvereinbarungen, die zB als Klauseln in Arbeitsverträgen oder spezifische Zusatzvereinbarungen ausgestaltet werden. Nicht zuletzt sehen auch manche Kollektivverträge branchenspezifische Verschwiegenheitspflichten der Arbeitnehmer vor.[8]

Praxistipp

Obwohl bereits nach dem Gesetz eine Verschwiegenheitsverpflichtung des Arbeitnehmers besteht, sollte man diese im **Arbeitsvertrag** oder in einer **Zusatzvereinbarung konkretisieren.** Bei der Ausgestaltung ist auf die Formulierung zu achten: Wird die Verschwiegenheit zu detailliert geregelt, kann dies zur Freigabe aller übrigen (nicht erfassten) betrieblichen Informationen führen. Sieht die Geheimnisschutzklausel hingegen zu weitgehende Bindungen des Arbeitnehmers vor, besteht die Gefahr, dass diese für sittenwidrig (iSd § 879 ABGB) und somit unzulässig erklärt wird.[9] Vereinbarungen sollten daher mit **„Maß und Ziel"** getroffen werden.

Wie lange hat sich der Arbeitnehmer an die Verschwiegenheitspflicht zu halten? Da die Treuepflicht des Arbeitnehmers grundsätzlich mit der Beendigung des Arbeitsverhältnisses erlischt, ist der Arbeitnehmer danach nicht mehr an eine Verschwiegenheitspflicht

1) Vgl *Dauser/Plattner,* Umgang mit dem betrieblichen E-Mail-Account ausgeschiedener Mitarbeiter, ARD 6735/6/2021; *Goricnik* in *Grünager/Goricnik,* Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle[3] (2018) Rz 6.18f.
2) Zu diesem Themenkreis s *Ludvik/Hördinger,* Die Privatnutzung betrieblicher E-Mail-Infrastruktur, GRAU 2022, 10 (in diesem Heft).
3) Als Rechtsgrundlage dafür dienen §§ 26a–26j UWG. Siehe hierzu auch *Thiele* in *Wiebe/Kodek,* UWG[2] § 11. Diese werden bei der folgenden Beurteilung ausgeklammert.
4) *Huger,* Schutz von Unternehmensdaten, ARD 6597/4/2018; *Löschnigg,* Arbeitsrecht[13] (2017) Rz 6/062ff.
5) RIS-Justiz RS0079608. Für Betriebsratsmitglieder legt § 115 Abs 4 ArbVG ausdrücklich eine Verschwiegenheitspflicht fest.
6) OGH 19. 9. 2001, 9 ObA 180/01b Arb 12.148; *Petrovic,* Die Vertrauensunwürdigkeit als Entlassungsgrund nach § 27 Abs 1 letzter Satz AngG, ZAS 1984, 49 (53); *Marhold,* Geheimnisschutz und Verschwiegenheitspflichten im Arbeitsrecht, in *Aicher/Funk/Korinek/Krejci/Ruppe,* Geheimnisschutz im Wirtschaftsleben, Schriften zum gesamten Recht der Wirtschaft (1980) 93 (103ff mwN).
7) So sind etwa Rechtsanwälte gem § 9 Abs 2 RAO, Wirtschaftstreuhänder nach § 80 WTBG oder klinische Psychologen und Gesundheitspsychologen gem § 37 PsychologenG 2013 zur standesrechtlichen Verschwiegenheit verpflichtet.
8) ZB § 3 Abs 3 des KollV für Angestellte bei Architekten und Ingenieurkonsulenten oder die KollV für Notariatsangestellte in einzelnen Bundesländern; *Knallnig-Prainsack* in *Reissner/Neumayr,* ZellHB AV-Klauseln[2] Besonderer Teil, 63. Klausel Rz 63.09.
9) *Knallnig-Prainsack* in *Reissner/Neumayr,* ZellHB AV-Klauseln[2] Besonderer Teil, 63. Klausel Rz 63.16.

gebunden.[10] Die Verpflichtung zur Geheimhaltung nach Beendigung des Arbeitsverhältnisses kann jedoch vertraglich vereinbart werden.

Praxistipp

Arbeitgeber sollten jedenfalls **nachvertragliche Verschwiegenheitsverpflichtungen** vereinbaren. Eine solche Geheimhaltungsklausel ist – soweit sie sich tatsächlich auf Betriebs- und Geschäftsgeheimnisse beschränkt – nicht als nachvertragliche Konkurrenzklausel einzustufen und kann somit auch ohne zeitliche Beschränkung abgeschlossen werden.[11]

2. Datenschutzrechtliche Vorgaben

Aus datenschutzrechtlicher Sicht ist relevant, dass neben den Daten des Arbeitnehmers auch die des Arbeitgebers geschützt werden. So sieht etwa die Grundsatzbestimmung § 1 DSG ein **Grundrecht auf Datenschutz** vor. Das Grundrecht auf Datenschutz besitzt eine Drittwirkung und kommt als „Jedermannsrecht" **auch juristischen Personen zu.**[12] Danach hat jedermann, insbesondere in Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit daran „*ein schutzwürdiges Interesse*" besteht.

Soweit der Anwendungsbereich des DSG eröffnet ist, werden danach nicht nur Daten, die das Privat- und Familienleben betreffen, sondern auch solche über den Betrieb bzw das Unternehmen („Wirtschaftsdaten") geschützt.[13] Der Schutz **personenbezogener Daten** kommt Arbeitgebern, die eine juristische Person sind, nicht zu, weil darunter jene Informationen verstanden werden, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.[14]

Im Rahmen eines Arbeitsverhältnisses kommt dem **Datengeheimnis nach § 6 DSG** eine wichtige Rolle zu. Das Datengeheimnis richtet sich an alle Personen, denen berufsmäßig Daten anvertraut wurden oder zugänglich gemacht wurden. Darunter fallen neben (echten) Arbeitnehmern auch Personen, die im Rahmen eines arbeitnehmerähnlichen Dienstverhältnisses beschäftigt sind.[15]

Das Datengeheimnis bewirkt nach § 6 Abs 2 Satz 1 DSG, dass Daten nur auf Grund einer **ausdrücklichen Anordnung** des jeweiligen Arbeitgebers, Verantwortlichen und Auftragsverarbeiters (oder deren Beauftragten) übermittelt werden dürfen. Geschützt werden durch das Datengeheimnis personenbezogene Daten (zB von Arbeitnehmern), die sich aus dem betrieblichen E-Mail-Verkehr ergeben können. Erfasst sind diesbezüglich alle personenbezogenen Daten, gleichgültig, ob sie nun ein „Geheimnis" enthalten oder nicht.[16] In Betracht kommen demnach sämtliche Informationen, die sich aus der konkreten Datenverarbeitung ergeben wie zB Kundenadressen, Geburtsdaten, Namen oder Gesundheitsdaten bei einer Patientendatei.[17] Das Datengeheimnis schützt sohin nicht ausweislich Betriebs- oder Geschäftsgeheimnisse; deren besonderer Schutz ergibt sich aus dem UWG.[18]

Aus der Zusammenschau der Bestimmungen § 1 DSG und § 6 DSG folgt, dass die „Verletzung schutzwürdiger Geheimhaltungsinteressen" nicht so eng interpretiert werden darf, dass davon nur eine Übermittlung oder Preisgabe von Daten des Betroffenen im Sinne eines tatsächlich stattfindenden Informationsflusses erfasst ist. Vom Gesetzgeber wird vielmehr auf die „Verwendung" von Daten abgestellt, mit der nicht nur die Übermittlung von Daten, sondern auch deren Verarbeitung und somit jede Art der Handhabung wie zB das Verknüpfen oder Löschen gemeint ist.

In allen dargestellten Szenarien (Punkt A) kommt es zu einer Verwendung bzw Übermittlung von Unternehmensdaten. Zudem ist regelmäßig davon auszugehen, dass im E-Mail-Verkehr personenbezogene Daten enthalten sind. Die Arbeitnehmer haben – neben spezifischen Vorgaben zu Betriebs- und Geschäftsgeheimnissen – bei ihren Handlungen daher das **Grundrecht auf Datenschutz** nach § 1 DSG sowie das **Datengeheimnis** nach § 6 DSG zu beachten.

Praxistipp

Anders als bei allgemeinen Geheimhaltungsvereinbarungen existieren beim Datengeheimnis besondere Vorgaben. Bei der Gestaltung von Dienstverträgen – sei es bei bestehenden oder bei neu zu begründenden Dienstverhältnissen – ist darauf zu achten, dass Arbeitnehmer **schriftlich**[19] **zur Einhaltung des Datengeheimnisses zu verpflichten sind (Datenschutzklausel).** In diesem Zusammenhang sind die Arbeitnehmer über die Rechtsfolgen eines Verstoßes gegen das Datengeheimnis zu belehren (§ 6 Abs 3 DSG). Bei der Ausgestaltung ist zudem besonderes Augenmerk auf die getrennte und spezifische Formulierung von Regelungen (i) zur Wahrung des Datengeheimnisses (§ 6 DSG) und (ii) zur Wahrung der Betriebs- und Geschäftsgeheimnisse (arbeitsrechtliche Verschwiegenheitspflicht, s Punkt B.1.) zu legen.[20] ➜

10) In manchen Fällen sieht jedoch das Gesetz selbst eine Weitergeltung der Verschwiegenheitspflicht vor, s bspw § 38 BWG, § 19 ABO 2005.

11) *Kietaibl/Rebhahn* in *Neumayr/Reissner,* ZellKomm³ § 1153 ABGB Rz 43f; OGH 27. 4. 1995, 8 ObA 225/95 ARD 4663/5/95. Das bedingt weiters, dass die Verdienstgrenzen des § 37 Abs 3 AngG nicht zur Anwendung gelangen und die Vereinbarung einer Konventionalstrafe das Recht auf Unterlassung nicht ausschließt.

12) Der Schutzbereich der DSGVO erfasst hingegen nur natürliche Personen; *Dopplinger* in *Bresich/Dopplinger/Dörnhöfer/Kunnert/Riedl,* DSG § 1 Rz 3ff.

13) *Grabenwarter/Frank,* B-VG § 1 DSG Rz 3; VfGH 30. 11. 1989, G 245/89 ua VfSlg 12.228/1989.

14) Siehe die Legaldefinition in Art 4 Z 1 DSGVO.

15) *Pollirer/Weiss/Knyrim/Haidinger,* DSG⁴ § 6 RZ 4; *Thiele/Wagner,* Praxiskommentar zum Datenschutzgesetz (DSG) § 6 Rz 25.

16) Das liegt daran, dass das österreichische DSG den Begriff der sogenannten „freien Daten" nicht kennt.

17) *Thiele/Wagner,* Praxiskommentar zum Datenschutzgesetz (DSG) § 6 Rz 6.

18) Siehe dazu §§ 11, 14 UWG und §§ 26a–26j UWG.

19) Daraus folgt nach § 886 ABGB iZm dem Signatur- und Vertrauensdienstegesetz (SVG), dass die Schriftlichkeit nur durch eine eigenhändige Unterschrift *(wet ink signature)* oder qualifizierte elektronische Signatur gewahrt wird.

20) *Heinrich* in *Pachinger,* Datenschutz – Recht und Praxis (2019) Kap 7. Datenschutz im Beschäftigungskontext Rz 15.

3. Pflicht zur Rückstellung betrieblicher Daten bei Beendigung des Arbeitsverhältnisses?

Die bisherige Darstellung zeigt, dass eine Speicherung von Unternehmensdaten auf dem privaten PC oder eine Weiterleitung an die private E-Mail-Adresse eine Verletzung der **Verschwiegenheitspflicht** und des Datengeheimnisses begründen können, weil der Dienstnehmer regelmäßig nicht zu einer solchen Verarbeitung (bzw Verwendung) der Daten berechtigt ist. Neben der Verschwiegenheitspflicht sind die Arbeitnehmer bei Beendigung des Arbeitsverhältnisses zur Rückgabe betrieblicher E-Mails und Unternehmensdaten verpflichtet. Eine solche **Rückgabeverpflichtung** ergibt sich uE bereits schlüssig aus der Bereitstellung des E-Mail-Accounts (als Betriebsmittel) durch den Arbeitgeber und **bedarf sohin keiner gesonderten Anordnung.**[21] Diese Rückstellungspflicht reicht soweit, dass beide Parteien des Arbeitsverhältnisses wechselseitig verwahrte Unterlagen am Ende des Dienstverhältnisses eigenständig zurückzustellen haben. Damit dürfen die Arbeitnehmer nicht nur ohne weiteres nicht davon ausgehen, dass sie die Betriebsmittel und die dazugehörigen Daten nach der Beendigung des Arbeitsverhältnisses für sich behalten dürfen (vgl Arbeitnehmer B), sondern sie haben diese eigenständig zurückzustellen.

Praxistipp

Um eine missbräuchliche Verwendung von Unternehmensdaten zu verhindern und Unklarheiten zu vermeiden, sollten – mittels schriftlicher Vereinbarung (bspw im Arbeitsvertrag) – Arbeitnehmer zur aufforderungslosen **Rückgabe betrieblicher Daten** am Ende des Dienstverhältnisses **vertraglich verpflichtet werden.**

Eine Rückgabeverpflichtung ist nicht auf den betrieblichen E-Mail-Verkehr beschränkt, sondern bezieht sich vielmehr auch auf alle anderen im Zuge des Beschäftigungsverhältnisses erlangten Daten. Aus Sicht des Arbeitgebers kann es daher zweckmäßig sein, eine generelle Verpflichtung zur Rückgabe **sämtlicher betrieblicher Unterlagen, Speichermedien und Dokumente** (spätestens) bei Beendigung des Arbeitsverhältnisses vertraglich vorzusehen. Eine solche Verpflichtung sollte mit dem **Verbot,** dokumentierte Informationen des Arbeitgebers zu vervielfältigen oder in Kopie zurückzubehalten, verbunden werden.

C. Pflichtenverstöße und deren Folgen

1. Wann liegt ein Pflichtenverstoß vor?

Arbeitnehmer, die wie in den drei Szenarien (Punkt A) zum **Träger fremder betrieblicher und geschäftlicher Interessen** wurden, sind aufgrund der Treuepflicht verpflichtet, diese Interessen ihres Arbeitgebers zu wahren und alles zu unterlassen, was diese Interessen zu beeinträchtigen geeignet ist. Sie haben daher auch Stillschweigen über für den Arbeitgeber wichtige Informationen, selbst wenn es sich um keine unmittelbaren Geschäftsgeheimnisse handelt, zu bewahren. Zudem haben die Arbeitnehmer die **Verwendung und Verarbeitung von Unternehmensdaten** nur nach Einwilligung ihres Arbeitgebers vorzunehmen.

Verfügt der Arbeitgeber daher über Daten, an deren Geheimhaltung er ein schutzwürdiges Interesse hat (zB geschäftliche E-Mail-Korrespondenzen), dann ist er auch vor der unzulässigen Löschung dieser Daten geschützt.[22] Daher ist auch die Hinderung des Arbeitgebers, Zugriff auf diese Daten zu erhalten, etwa mittels Löschung durch den Arbeitnehmer, eine **Verletzung des Datengeheimnisses** sowie arbeitsrechtlicher Pflichten (s Arbeitnehmer C).

Liegt keine Einwilligung des Arbeitgebers vor, führt auch die Übermittlung der Daten vom betrieblichen E-Mail-Account zur privaten E-Mail-Adresse (s Arbeitnehmer A) oder die Speicherung auf einem privaten PC (s Arbeitnehmer B) zu einem Verstoß gegen das Datengeheimnis gem § 6 Abs 2 DSG.

Enthalten die E-Mails Informationen, an deren Geheimhaltung der Arbeitgeber ein objektives Interesse hat, stellen die Handlungen der Arbeitnehmer A und B auch einen **Verstoß gegen die allgemeine arbeitsrechtliche Verschwiegenheitspflicht** dar. Diese setzen nämlich Handlungen, durch welche zumindest indirekt eine Weitergabe von Betriebs- und Geschäftsgeheimnissen erfolgt oder deren Schutz nicht entsprechend gewährleistet werden kann. Sind diese Daten einmal aus der Sphäre des Arbeitgebers in die private Sphäre des Arbeitnehmers oder in den Besitz Dritter (zB privater E-Mail-Server) gelangt, können auch (andere) betriebsfremde Personen potentiell auf diese zugreifen.

Praxistipp

Arbeitnehmer sind zB durch Richtlinien regelmäßig auf einen **sorgsamen Umgang** mit betrieblichen Daten hinzuweisen. Zu diesem Zweck können diverse „Negativbeispiele" aufgezeigt werden, um eine Pflichtenverletzung seitens des Arbeitnehmers bereits präventiv zu verhindern. Weiters können für den Fall eines tatsächlichen Pflichtenverstoßes **Konventionalstrafen** im Arbeitsvertrag vorgesehen werden.[23]

21) Der Arbeitgeber hat einen nach 30 Jahren verjährenden Anspruch auf Rückstellung (§ 961 iVm § 1478 ABGB), wenn er dem Arbeitnehmer Betriebsmittel anvertraut, vgl *Krejci* in *Rummel,* ABGB[3] § 1163 ABGB Rz 2 mwN und *Karner* in *Kletečka/Schauer,* ABGB-ON[1.05] § 961 Rz 2 mwN zum Arbeitsvertrag. Derartige Streitigkeiten auf Herausgabe von Gegenständen des Arbeitgebers werden von § 61 Abs 1 Z 4 ASGG adressiert. Zur gegensätzlichen Herausgabepflicht von Arbeitgebern s umgekehrt OGH 6. 10. 2005, 8 ObS 17/05s.

22) *Pilgermair,* Der Dienstgeber als datenschutzrechtlicher Betroffener, RdW 2017/4, 250 (253).

23) Zu beachten ist, dass die Höhe der Konventionalstrafe als pauschalierter Schadenersatz einem zwingenden richterlichen Mäßigungsrecht unterliegt (§ 2e AVRAG); OGH 24. 9. 2018, 8 ObA 49/18s ARD 6626/7/2018.

2. Welche Konsequenzen drohen Arbeitnehmern bei einer Pflichtenverletzung?

a) Entlassung

Die Verletzung der Verschwiegenheitspflicht oder des Datengeheimnisses durch den Arbeitnehmer kann den Arbeitgeber auch zur Entlassung, also der vorzeitigen Auflösung des Arbeitsverhältnisses aus wichtigem Grund, berechtigen. Voraussetzung für die Entlassung ist, dass der Arbeitnehmer einen derart schwerwiegenden Pflichtverstoß begangen hat, dass dem Arbeitgeber die Aufrechterhaltung des Arbeitsverhältnisses nicht einmal für die Dauer der Kündigungsfrist zumutbar ist **(Unzumutbarkeit der Weiterbeschäftigung).**[24)]

Als möglicher Tatbestand kommt für Arbeiter etwa die Erfüllung des Tatbestands **§ 82 lit e GewO 1859** in Frage, der den **Verrat von Betriebs- und Geschäftsgeheimnissen** ausdrücklich als Entlassungsgrund festlegt.[25)] Für Angestellte kann die Verletzung der Verschwiegenheitspflicht und/oder des Datengeheimnisses zur Entlassung wegen **„Vertrauensunwürdigkeit"** gem **§ 27 Z 1 AngG** führen.[26)] Danach ist der Arbeitgeber zur vorzeitigen Auflösung berechtigt, wenn sich der Arbeitnehmer einer Handlung schuldig macht, die ihn des Vertrauens des Arbeitgebers unwürdig erscheinen lässt. Dies setzt **ein Verschulden des Arbeitnehmers,** zumindest in Form von Fahrlässigkeit, voraus; Schädigungsabsicht und der Eintritt eines konkreten Schadens sind hingegen nicht erforderlich. Das bedeutet auch, dass dem Arbeitnehmer das objektive Geheimhaltungsinteresse des Arbeitgebers erkennbar sein musste.[27)]

Soweit der Arbeitnehmer daher Geschäftsgeheimnisse und andere Unternehmensdaten ohne Befugnis in den privaten Bereich verbringt (s Arbeitnehmer A und B), kann sich in einem laschen Umgang mit sensiblen Unternehmensdaten ein Gesetzes- und Vertragsbruch manifestieren, der das Vertrauensverhältnis zum Arbeitgeber nachhaltig zerrüttet.[28)] Die Verletzung der Verschwiegenheitspflicht muss jedoch so schwerwiegend sein, dass beim Arbeitgeber die objektiv gerechtfertigte Befürchtung ausgelöst wird, dass der Angestellte auch zukünftig die erhaltenen Informationen nicht mit der gebotenen Vertraulichkeit behandeln wird.[29)] Dabei spielt es auch eine Rolle, wie die Themen Datenschutz, Umgang mit Daten etc im Unternehmen gehandhabt und den Arbeitnehmern gegenüber kommuniziert werden. Je gewichtiger die Position und je tiefer der Einblick des Arbeitnehmers in das Unternehmen des Arbeitgebers ist, desto geringer sind die Anforderungen an einen zur Entlassung berechtigenden Vertrauensbruch. In diesem Zusammenhang ist auch das empfindliche, vor allem den Arbeitgeber betreffende Strafenregime des DSG bzw der DSGVO zu beachten, das den diese Rechtsmaterie betreffenden Verstößen entsprechendes Gewicht verleiht.

In diesem Sinne urteilte die Rechtsprechung, dass die Mitnahme von Kopien (nur) teilweise der Geheimhaltung unterliegender gemeindeinterner Dokumente durch einen Gemeindeamtsleiter oder die Anfertigung einer privaten Kopie eines Emissionsgutachtens in einem den Vater eines Gemeindebediensteten betreffenden Verwaltungsverfahren den Entlassungsgrund der Vertrauensunwürdigkeit erfüllen.[30)]

In einem anderen Fall sah die Rechtsprechung im bloß externen Abspeichern von Arbeitsunterlagen durch Weiterleitung an die private E-Mail-Adresse jedoch noch keinen Geheimnisverrat, zumal diese nur zum Zweck der Erbringung von Arbeitsleistungen in erlaubter Heimarbeit (Home-Office) verwendet wurden (Arbeitnehmer A).[31)]

Wurde die Verpflichtung zur Geheimhaltung im Arbeitsvertrag oder mittels Zusatzvereinbarung konkretisiert und die Einhaltung dieser Pflicht seitens des Arbeitnehmers missachtet, dann kann dies auch zur Entlassung wegen **beharrlicher Pflichtenverletzung** nach **§ 27 Z 4 Satz 2 AngG** berechtigen. Ob eine vorgehende Er-/Abmahnung des Arbeitnehmers jeweils notwendig ist, ergibt sich aus der Schwere der Verfehlungen.

Allgemein lässt sich die Tendenz eines wachsenden Bewusstseins für Unternehmensdaten und Datenschutzverstöße, auch von den Arbeits- und Sozialgerichten, erkennen, wie die zu diesem Thema aufkommende Rechtsprechung[32)] zeigt.

Praxistipp

Um die Sensibilität für dieses Thema zu schärfen, können die zur Entscheidung berufenen Stellen den jeweiligen Fall im Rahmen eines Gedankenexperiments in die „analoge" Welt transportieren und die Überlegung anstellen, wie viele Seiten an Druckpapier die jeweils aus dem Unternehmen verschafften Daten ausmachen.

Praktische Relevanz erlangt das Thema häufig nach Ausspruch einer Kündigung, etwa weil der Arbeitgeber erst zu diesem Zeitpunkt von einem Pflichtverstoß Kenntnis erlangt (zB bei [Nicht-]Rückgabe von Betriebsmitteln). So ist denkbar, dass der Arbeitgeber erst während der Kündigungsfrist oder eines Arbeitsrechtsprozesses entdeckt (etwa durch Vorlage von Unternehmensdaten vor bzw an das Gericht im Rahmen eines Kündigungsanfechtungsprozesses),[33)] dass der Arbeitnehmer betriebliche E-Mails nicht zurückgegeben, sondern für private Zwecke gespeichert oder nicht auf-

24) Statt vieler: *Löschnigg,* Arbeitsrecht[13] (2017) Rz 8/223.
25) Zu beachten ist, dass zahlreiche Sondergesetze, die einen besonderen Bestandsschutz bestimmter Arbeitnehmergruppen vorsehen, den Verrat von Geschäftsgeheimnissen als Kündigungs- und Entlassungsgrund normieren; s beispielsweise § 122 Abs 1 Z 4 ArbVG und § 12 Abs 2 Z 3 MSchG.
26) *Laimer/Habe/Zojer,* Geheimnisschutz und IP im Arbeitsverhältnis (2020) 7. Kapitel Rz 83.
27) *Grillberger* in *Löschnigg,* Angestelltengesetz II[10] § 27 Rz 52 ff; OGH 19. 9. 2002, 8 ObA 192/02x ASoK 2003, 197.
28) Vgl OLG Linz 24. 6. 2015, 12 Ra 27/15z.
29) OGH 13. 11. 2002, 9 ObA 158/02d ARD 5381/6/2003; 18. 9. 2003, 8 ObA 87/03g ARD 5461/7/2003; RIS-Justiz RS0029511 [T 2].
30) OGH 3. 8. 2006, 8 ObA 84/06w; 25. 8. 2014, 8 ObA 36/14y.
31) OLG Wien 26. 11. 2018, 8 Ra 40/18p ARD 6635/13/2019.
32) OLG Linz 24. 6. 2015, 12 Ra 27/15z; OLG Wien 26. 11. 2018, 8 Ra 40/18p ARD 6635/13/2019.
33) Das kann in der Praxis von Arbeitgebern auch als weiterer Kündigungsgrund angeführt („nachgeschoben") werden.

tragsgemäß gelöscht hat. Der Einwand, solche Unternehmensdaten zur zweckentsprechenden Rechtsverfolgung vorlegen zu müssen, geht fehl, weil vor Gerichten nach § 303 ZPO die Möglichkeit zur Urkundenvorlage durch den Gegner besteht.[34] Ein solcher Fall kann – bei Vorliegen der übrigen Voraussetzungen (s zuvor) – zum Ausspruch einer **Eventualentlassung** für den Fall, dass eine Kündigung erfolgreich angefochten wird (Kündigungsanfechtungsverfahren), berechtigten.[35]

Praxistipp

Eine (Eventual-)Entlassung ist unverzüglich auszusprechen (Unverzüglichkeitsgrundsatz). Allerdings ist dem Arbeitgeber im Vorfeld zuzugestehen, eine den Umständen nach angemessene und zeitnahe Untersuchung vorzunehmen. Im Verdacht stehende Arbeitnehmer sollten während eines solchen Zeitraums vorläufig suspendiert, von IT-Zugängen gesperrt und zur Rückgabe von Betriebsmitteln (Unternehmensdaten) aufgefordert werden. In diesem Prozess stehen spezielle Anbieter unterstützend zur Seite, die potentielle Verstöße gegen den Umgang mit Unternehmensdaten in sog „forensischen Untersuchungen" nachvollziehen, indem zB IT-Protokolle ausgewertet oder wiederhergestellt werden.

b) Kündigung

Neben der Entlassung kann einer der eingangs dargestellten Pflichtverstöße zur Kündigung des Arbeitnehmers führen. Einer möglichen Kündigungsanfechtung kann ein **verhaltensbedingter Kündigungsgrund** gem § 105 Abs 3 Z 2 lit a ArbVG entgegengehalten werden.[36] Derartige Pflichtenverstöße, sollten sie keine Entlassung rechtfertigen, können den Kündigungsgrund nach § 8 Abs 4 lit c BEinstG erfüllen.

c) Schadenersatz und Konventionalstrafe

Verursacht ein Arbeitnehmer durch seine Handlungen einen bezifferbaren Schaden (zB Arbeitnehmer C), kann dieser vom Arbeitgeber als **Schadenersatz (§§ 1293 ff ABGB)** geltend gemacht werden. Das Dienstnehmerhaftungsprivileg des § 2 Abs 1 DHG gereicht dem Arbeitnehmer nicht haftungsmindernd zum Vorteil, wenn der Schaden auf eine private Nutzung des betrieblichen E-Mail-Accounts zurückzuführen ist.[37]

Für den Arbeitgeber besteht die Möglichkeit, eine allenfalls vereinbarte **Konventionalstrafe** geltend zu machen. Der Vorteil einer Konventionalstrafe liegt in erster Linie darin, dass der Berechtigte im konkreten Fall den Schaden bzw dessen Höhe nicht beweisen muss, was in der Praxis häufig zu besonderen Schwierigkeiten führt.

d) Weitere rechtliche Konsequenzen

Neben den eben dargestellten Folgen kann eine Verletzung der Verschwiegenheitspflicht zu **(verwaltungs-)strafrechtlichen Sanktionen** führen. So ist die Verletzung der Verschwiegenheitspflicht durch Betriebsratsmitglieder zugleich auch eine Verwaltungsübertretung, die (nur) auf Anregung des Arbeitgebers zu verfolgen ist **(§ 115 Abs 4 ArbVG).**

Zudem kann eine unbefugte Weitergabe oder Verwendung von Geschäfts- und Betriebsgeheimnissen zu **Wettbewerbszwecken** vom Arbeitgeber nach § 11 UWG iVm § 879 ABGB verfolgt werden (Privatanklagedelikt) und mit einstweiligen Verfügungen (zB auf Unterlassung gerichtet) bekämpft werden (§ 14 UWG).

Überdies ist nach § 123 StGB zu bestrafen, wer ein **Geschäfts- oder Betriebsgeheimnis** mit dem Vorsatz, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, **auskundschaftet.** Daneben kommt bei der „schlichten" Verletzung eines Geschäfts- oder Betriebsgeheimnisses eine Strafbarkeit nach § 122 StGB in Frage. Weiters ist betreffend die Verletzung von Berufsgeheimnissen in Gesundheitsberufen die Bestimmung § 121 StGB einschlägig.[38] Daneben gibt es weitere Bestimmungen, die dem Standesrecht spezifischer Berufe entspringen (zB RAO für Rechtsanwälte).

Bei der vorsätzlichen **Verletzung des Datengeheimnisses** drohen dem Arbeitnehmer gem § 62 Abs 1 Z 2 DSG Verwaltungsstrafen von bis zu € 50.000,– pro Verstoß. Zusätzlich normiert § 63 DSG einen gerichtlichen Straftatbestand. Demnach ist zu bestrafen, wer mit dem Vorsatz, sich oder einen Dritten dadurch unrechtmäßig zu bereichern, oder mit der Absicht, einen anderen dadurch in seinem von § 1 Abs 1 DSG gewährleisteten Anspruch zu schädigen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat.[39]

34) Wenn eine Partei behauptet, dass sich eine für ihre Beweisführung erhebliche Urkunde in den Händen des Gegners befindet, so kann auf ihren Antrag das Gericht dem Gegner die Vorlage der Urkunde durch Beschluss auftragen. In Behördenverfahren, in denen der Amtswegigkeitsgrundsatz gilt, ist es ausreichend, bei der Behörde den Auftrag der Vorlage bestimmter Dokumente durch eine andere Partei anzuregen.

35) Zu beachten sind die damit verbundenen (negativen) Rechtsfolgen für den Arbeitnehmer, wie etwa Ruhen des Arbeitslosengeldes, Verlust einer Kündigungsentschädigung oder mögliche Schadenersatzansprüche des Arbeitgebers. Siehe dazu auch *Lovrek,* Die Eventualkündigung im Arbeitsrecht und ihre prozessualen Folgen, in FS Bauer/Maier/Petrag (2004) 261 (261 f); *Ziehensack,* Die Eventualkündigung, DRdA 2013, 172.

36) Eine Verletzung der Treuepflicht kann auch im Fall der wesentlichen Beeinträchtigung von Arbeitnehmerinteressen eine Kündigung durch den Arbeitgeber rechtfertigen, s *Wolligger* in *Neumayr/Reissner,* ZellKomm³ § 105 ArbVG Rz 206 ff; OGH 9. 7. 1997, 9 ObA 158/97 v ASoK 1998, 190.

37) Vgl *Brodil,* Nutzung und Kontrolle von neuen Medien im Arbeitsrecht, ecolex 2001, 853.

38) *Löschnigg,* Arbeitsrecht¹³ Rz 6/069 mwN.

39) *Stella/Winter* in *Reissner/Neumayr,* ZellHB AV-Klauseln² Besonderer Teil, 63 a.111 f; *Pollirer/Weiss/Knyrim/Haidinger,* DSG⁴ § 6 Rz 12.

➜ Die Grauzone

- **Die unsachgemäße Handhabe von Unternehmensdaten führt in Zeiten der Digitalisierung und der zunehmenden Vermischung des Privat- und Berufslebens (zB Home-Office) zu häufig unbedachten Konsequenzen.**
- **Die Verletzung von Pflichten im Graubereich beruflicher und privater digitaler Kommunikation kann Arbeitgeber zur (Eventual-)Entlassung berechtigen oder als personen-/verhaltensbedingter Kündigungsgrund angeführt werden.**
- **Arbeitgeber können rechtswidrig handelnde Arbeitnehmer zudem nach dem Straf-, Datenschutz-, Wettbewerbs- und Schadenersatzrecht belangen.**

➜ Zum Thema

Über die Autoren:
Dr. Christoph Ludvik, BSc (WU) ist Rechtsanwalt in der Kanzlei Herbst Kinsky RAe in Wien.
Christoph Hördinger, LLM. (WU), LLB. (WU), war Rechtsanwaltsanwärter ebenda und absolviert aktuell die Gerichtspraxis im OLG Sprengel Wien.
Kontaktadresse: Herbst Kinsky Rechtsanwälte GmbH, Dr.-Karl-Lueger-Platz 5, 1010 Wien.
Tel: +43 (0)1 904 21 80,
E-Mail: christoph.ludvik@herbstkinsky.at,
Internet: www.herbstkinsky.at

Von den Autoren erschienen:
C. Ludvik, Urlaubsverfall bei Arbeitnehmeraustritt, ASoK 2022/1, 2.
C. Ludvik, Der internationale Betrieb – Fragen der grenzüberschreitenden Betriebsverfassung (2021).
C. Ludvik/Zwinger, Nachvertragliche Wettbewerbsbeschränkungen arbeitnehmerähnlicher Personen, in *Brameshuber/Friedrich/Karl,* FS Franz Marhold (2020) 157.
Brameshuber/C. Ludvik, Sozialrechtlicher Missbrauch, in *Kalss/Bergmann,* Handbuch Rechtsformwahl (2020) 189.
Marhold/C. Ludvik, Thoughts about indexing family benefits: Are authorities permitted to apply the Austrian indexation of family benefits? The primacy of EU law and the right/obligation to request a ruling from the Court of Justice of the European Union, EJSS 2020/22/3, 273.

Literatur:
Laimer/Habe/Zojer, Geheimnisschutz und IP im Arbeitsverhältnis (2020); *Pachinger* (Hrsg), Datenschutz – Recht und Praxis (2019); *Determann/Hitz,* Die private Nutzung von Internet und E-Mail, ASoK 2019, 55; *Grünanger/Goricnik* (Hrsg), Arbeitnehmer-Datenschutz und Mitarbeiterkontrolle² (2018); *Huger,* Schutz von Unternehmensdaten, ARD 6597/4/2018; *Pilgermair,* Der Dienstgeber als datenschutzrechtlicher Betroffener, RdW 2017/4, 250; *Körber-Risak/Lurf,* Individualarbeitsrechtliche Aspekte unternehmensinterner Untersuchungen, ZAS 2017/35, 191.

Das betriebliche E-Mail-Postfach als rechtliche Grauzone

Kaum eine technische Entwicklung der letzten Jahrzehnte hat den beruflichen Alltag so weitreichend und zugleich auch so nachhaltig verändert wie die Kommunikation via E-Mail. Umso überraschender ist es, dass (arbeits-)rechtliche Aspekte dieser Kommunikation bisher nur vereinzelt geklärt sind. Das betriebliche E-Mail-Postfach ist daher eine rechtliche Grauzone – und zwar in jeder Hinsicht.

Von Miriam Mitschka und Jens Winter

GRAU 2022/6

Inhaltsübersicht:

▶ Arbeitsrecht
▶ Datenschutzrecht

A. Einleitung

Das E-Mail hat die Kommunikation vergünstigt und zugleich für alle spürbar beschleunigt. War das E-Mail zu Beginn seiner Einführung Mitte der 1990er Jahre im Alltag vor allem eine beliebte Kommunikationsform vorwiegend im privaten Bereich, wurde es in diesem Bereich zwischenzeitig von Messenger-Diensten wie WhatsApp, Signal & Co verdrängt. Auch bei älteren Generationen spielt die private Kommunikation via E-Mail heute nur mehr eine verhältnismäßig untergeordnete Rolle. Repräsentative Studien aus dem Jahr 2021 besagen, dass durchschnittlich 26 E-Mails täglich in jedem beruflichen Postfach in Deutschland einlangen. Weltweit wurden bereits 2018 täglich rund 280 Milliarden E-Mails versendet, Tendenz steigend. Auch wenn im beruflichen Kontext neue Technologien, wie zB der Austausch von Daten und Unterlagen über virtuelle Datenräume und dergleichen, Einzug halten, wird das E-Mail als fester Bestandteil der beruflichen Kommunikation auf absehbare Zeit bestehen bleiben. Die Nutzung von E-Mails hat demnach im beruflichen Alltag eine lange Tradition.

Fest steht, dass die Verwendung von E-Mail-Postfächern durch Arbeitnehmer bei Erbringung ihrer Tä-