



E-Mail-Zugriff am Arbeitsplatz

Die Frage, ob und in welchem Umfang Arbeitgeber auf die E-Mails ihrer Mitarbeitenden zugreifen dürfen, gehört zu den Dauerbrennern des Arbeits- und Datenschutzrechts. Zwischen betrieblicher Kontrolle und Persönlichkeitsschutz besteht ein sensibles Spannungsfeld. Der folgende Beitrag zeigt die rechtlichen Leitlinien auf und formuliert praxisnahe Empfehlungen für Unternehmen.

■ Von RA Dr. iur. Lukas Lezzi, MLaw Alexandra Egger

Rechtsgrundlagen und Grundprinzipien

Im Zentrum stehen zwei Normenkomplexe:

- **Arbeitsrecht** (insbesondere Art. 328 OR: Schutz der Persönlichkeit des Arbeitnehmers): Der Arbeitgeber ist verpflichtet, die Persönlichkeit seiner Mitarbeitenden zu achten und zu schützen. Dazu gehören insbesondere der respektvolle Umgang mit ihrer Privatsphäre sowie der Schutz vor unangemessenen Überwachungs- oder Kontrollmassnahmen.
- **Datenschutzrecht**: E-Mails, die an eine persönliche geschäftliche Adresse des Arbeitnehmers gesendet werden, lassen sich eindeutig einer bestimmten Person zuordnen und gelten daher als Personendaten im Sinne von Art. 5 lit. a DSGVO. Es können aber auch personenbezogene Daten an anonyme Geschäftsadressen geschickt werden. Damit ist jeder Zugriff des Arbeitgebers eine Datenbearbeitung, die einer klar bestimmten Zweckbindung und einer Rechtsgrundlagen bedarf.

Beide Normbereiche verfolgen denselben Grundsatz: Der Arbeitgeber darf – etwa durch den Zugriff auf ein dienstliches E-Mail-Konto – nur insoweit in die Persönlichkeitssphäre der Mitarbeitenden eingreifen, wie dies durch überwiegende betriebliche Interessen gerechtfertigt, verhältnismässig und für die Sicherstellung des Betriebsablaufs notwendig ist. Die Verhältnismässigkeit ist gewahrt, wenn der Eingriff zur Erreichung des verfolgten Ziels geeignet, erforderlich und zumutbar ist. Ein überwiegendes betriebliches Interesse kann insbesondere bei längeren Abwesenheiten ohne wirksame Stellvertretung, bei sicherheitsrelevanten Vorfällen (z.B. Verdacht auf kompromittierte Accounts) oder im Rahmen arbeitsrechtlicher Abklärungen aufgrund konkreter Hinweise auf Pflichtverletzungen bestehen.

Der Arbeitgeber muss zudem transparent über Zweck, Umfang und Modalitäten allfälliger Kontrollen informieren.

Zulässigkeit des Zugriffs auf geschäftliche E-Mails

Bei der Prüfung, wie weit ein Zugriff erlaubt ist, muss unterschieden werden, ob die private Nutzung des E-Mail-Accounts verboten oder erlaubt ist.

a. Private Nutzung verboten

Ein Verbot privater Nutzung ist nur wirksam, wenn es klar und nachweisbar kommuniziert wurde (z.B. durch IT-/E-Mail-Reglement, Personalhandbuch, Schulungen). Die Information hat neben dem Verbot selbst auch dessen Zweck, die zulässigen Kontrollen sowie das Vorgehen bei Abwesenheiten zu erläutern. Weiter sind auch die Konsequenzen bei Verstössen festzulegen.

Trotz Nutzungsverbots bleibt der Persönlichkeitsschutz von Mitarbeitern gemäss Art. 328 OR anwendbar. Eine dauerhafte oder verdachtslose Überwachung ist klar unzulässig. Auch bei ausschliesslich geschäftlicher Nutzung ist der Zugriff auf E-Mail-Inhalte ein schwerer Eingriff und nur bei legitimen Gründen, fehlenden milderen Mitteln wie Team-Mailbox oder automatischer Abwesenheitsnotiz und unter Wahrung der Verhältnismässigkeit erlaubt.

Systematische Inhaltskontrollen sind ausgeschlossen; kurzfristige, anonymisierte Auswertungen, stichprobenartige Kontrollen bei konkretem Anlass sowie technisch notwendige Sicherheitsmassnahmen (Spamfilter, Malware-Scanning, DLP, anonymisierte oder punktuelle Metadaten-Analysen) sind hingegen zulässig.

Interne Prozesse sollen klar festlegen, wer den Zugriff anordnen darf, wie die Verhältnis-

mässigkeit geprüft und dokumentiert wird und wie verhindert wird, dass versehentlich private E-Mails geöffnet werden.

b. Private Nutzung erlaubt oder geduldet

Ist die private Nutzung des geschäftlichen E-Mail-Accounts erlaubt oder wird sie geduldet, gilt das Postfach rechtlich als gemischt genutzt. Dadurch greifen Persönlichkeitsschutz und Fernmeldegeheimnis (Art. 13 BV) besonders stark, sodass ein Arbeitgeber nur in eng begrenzten Ausnahmefällen auf das Postfach zugreifen darf.

Ein Zugriff ist zulässig, wenn

- der Mitarbeitende ausdrücklich zustimmt: Die Zustimmung sollte dokumentiert und für den konkreten Einzelfall eingeholt werden.
- ein Stellvertreter bei Abwesenheiten im Vorfeld klar eingesetzt wurde: In diesem Fall kann die benannte Stellvertretung auf geschäftliche Nachrichten zugreifen. Eine automatische Weiterleitung ist nur in klar definierten Ausnahmefällen und nur bei ausdrücklicher Vereinbarung zulässig. Werden private Nachrichten im Postfach geführt, sollten sie durch Kennzeichnung als «privat» oder mit dem Betreff als solche erkennbar sein. Solche Nachrichten dürfen vom Stellvertreter nicht geöffnet werden. Fehlen solche Anhaltspunkte, ergibt sich der private Charakter erst aus dem Inhalt. Bei Unsicherheit sollte die Arbeitgeberin eine E-Mail nicht lesen, da private Nachrichten einem uneingeschränkten Schutz (Post-/Fernmeldegeheimnis) unterstehen.
- ein erheblichem Missbrauchsverdacht (z.B. strafbare Handlung oder schwere Vertragsverletzung) besteht: Der Eingriff muss auch in diesem Fall verhältnismässig, dokumentiert und möglichst unter Beizug einer neutralen Stelle wie HR oder Compliance erfolgen. Private E-Mails dürfen auch in diesem Fall nicht geöffnet werden.

E-Mail-Zugriff bei Beendigung des Arbeitsverhältnisses

Es ist oft unklar, wie bei der Beendigung eines Arbeitsverhältnisses mit den Serverzugängen und der Sperrung von E-Mail-Accounts korrekt umzugehen ist.

- Bei einem geplanten Austritt übergibt der Arbeitnehmer die laufenden Geschäfte



PRAXISTIPP

Empfehlungen für die Praxis

Unternehmen sollten im Zusammenhang mit dem Zugriff auf die E-Mail-Konten:

- klare interne Reglemente zur E-Mail-Nutzung erstellen und sicherstellen, dass die Mitarbeiter diese kennen
- private Nutzung des E-Mail-Accounts verbieten oder technisch klar trennen: Tools wie z.B. Microsoft 365, Google Workspace können z.B. E-Mails nach Absenderkategorien sortieren oder private Absender automatisch in einen gekennzeichneten Ordner verschieben.
- Abwesenheits- und Zugriffsprozesse definieren
- die Mitarbeitenden über die Zugriffsmöglichkeit bzw. die entsprechende Datenbearbeitung transparent informieren (Art. 19 DSGVO)
- IT-Sicherheits- und Datenschutzbeauftragte einbeziehen, wenn ein Zugriff als nötig erscheint
- die Zugriffe dokumentieren und auf das notwendige Minimum beschränken



und relevanten E-Mails an die zuständige interne Stelle und bestätigt die vollständige Übergabe aller Geschäftsdokumente. Er erhält zudem die Möglichkeit, private E-Mails und persönliche Daten auf ein eigenes Speichermedium zu sichern und anschliessend vom Server zu löschen. Am letzten Arbeitstag werden der E-Mail-Account sowie alle weiteren IT-Zugänge gesichert und gesperrt, bevor sie nach einer angemessenen Frist endgültig gelöscht werden.

- Bei einer fristlosen Kündigung, einer Freistellung oder im Todesfall erfolgt die Sperrung des Accounts sofort, und die vorhandenen Daten werden gesichert. Private E-Mails und andere persönliche Daten werden anschliessend im Vieraugenprinzip ausgesondert, im Todesfall unter Einbezug der Angehörigen. Geht an eine bereits gesperrte E-Mail-Adresse eine Nachricht ein, erhält der Absender automatisch den Hinweis, dass die Adresse nicht mehr gültig ist und welche Ersatzadresse genutzt werden soll; eine Weiterleitung ist in solchen Fällen nicht erforderlich.

Informationspflicht und Transparenz

Das DSGVO und Art. 328 OR verlangen hohe Transparenz beim Umgang mit E-Mail-Daten. Arbeitgeber müssen Mitarbeitende vor jeder möglichen Kontrolle über die wesentlichen Aspekte der Datenbearbeitung informieren. Auch das blosses Öffnen eines geschäftlichen Postfachs stellt eine Datenbearbeitung dar.

Die Information (gemäss Art. 19 DSGVO) muss klar und gut zugänglich sein. Sie soll folgende Punkte beinhalten:

- Es soll klar angegeben werden, welche Stellen im Unternehmen E-Mail-Daten bearbeiten werden (z.B. IT, HR, Stellvertreter). Zudem soll – falls vorhanden – der Datenschutzkontakt genannt werden.
- Der Zweck der Bearbeitung wie z.B. die Sicherstellung der Geschäftskontinuität, die IT-Sicherheit, die Abklärung konkreter Pflichtverletzungen oder die Erfüllung gesetzlicher Vorgaben soll genannt werden. Pauschale Hinweise wie «Kontrollen sind möglich» genügen nicht.
- Der Umfang möglicher Kontrollen soll erläutert werden. Dies umfasst die Aufklärung, welche Datenarten betroffen sind (Meta-, Inhalts-, Logdaten), wer Zugriff haben darf, unter welchen Umständen ein Inhaltszugriff erfolgt (z.B. Abwesenheit, Missbrauchsverdacht) und ob automatisierte Sicherheitssysteme eingesetzt werden.
- Der Mitarbeiter soll über seine Rechte wie z.B. Auskunftsrecht, Berichtigungs-/Löschrecht aufgeklärt werden.
- Es soll dargelegt werden, wie lange E-Mail- und Logdaten gespeichert werden und nach welchen Kriterien sie gelöscht oder anonymisiert werden.

Diese Informationen müssen vor der Datenbearbeitung verfügbar sein. Ein Reglement ist nur wirksam, wenn die Mitarbeitenden es kennen und verstehen.

Ein Zugriff auf E-Mails ist nur rechtmässig, wenn Mitarbeitende im Voraus nachvollziehen konnten, wann und warum ein solcher Zugriff erfolgen darf. Fehlt Transparenz, ist selbst ein an sich zulässiger Zugriff rechtswidrig, da er gegen die Informationspflicht verstösst.

Fazit

Der Zugriff auf E-Mails ist für Unternehmen in gewissen Situationen unverzichtbar, berührt aber immer zentrale Persönlichkeitsrechte der Mitarbeitenden. Das Arbeits- und Datenschutzrecht verlangt einen Ausgleich, der sich an den Grundprinzipien Transparenz, Zweckbindung und Verhältnismässigkeit orientiert. Wer klare Reglemente schafft, Kontrollmechanismen präzise definiert, technische Trennungen vorsieht und Zugriffe rest-

riktiv handhabt, bewegt sich rechtssicher und stärkt gleichzeitig das Vertrauen der Mitarbeitenden.

PRAXISTIPP

Prinzip der Verhältnismässigkeit beim E-Mail-Zugriff



Der Grundsatz der Verhältnismässigkeit ist im Arbeits- und Datenschutzrecht zentral. Ein Zugriff auf ein E-Mail-Konto ist verhältnismässig, wenn die folgenden Bedingungen erfüllt sind:

- **Geeignetheit:** Die Massnahme muss geeignet sein, den verfolgten Zweck zu erreichen, z.B. Zugriff auf ein E-Mail-Konto bei Abwesenheit, um den Betrieb aufrechtzuerhalten.
- **Erforderlichkeit (mildestes Mittel):** Es darf kein milderer, gleich wirksames Mittel zur Verfügung stehen, welches denselben Zweck erfüllt, wie z.B. eine Stellvertretungsregelung, eine Abwesenheitsmeldung oder eine Funktionsmailbox. Erst wenn diese Mittel ausgeschöpft oder untauglich sind, ist ein Zugriff zulässig.
- **Minimierung des Eingriffs:** Der Zugriff ist auf das absolut notwendige Minimum zu beschränken. Dies bedeutet, es dürfen nur relevante Nachrichten geöffnet werden, der Zugriff soll zeitlich begrenzt werden, die Einsicht soll durch den ernannten Stellvertreter geschehen.
- **Zumutbarkeit/Interessenabwägung:** Der Eingriff muss in einem vernünftigen Verhältnis zum verfolgten Zweck stehen. Die Interessen des Unternehmens dürfen die Persönlichkeitsrechte der Mitarbeitenden nicht überwiegen.

AUTOREN



RA Dr. iur. Lukas Lezzi, CIPP/E, CIPM, CAS Forensics, ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz und Finanzmarktrecht.



MLaw Alexandra Egger arbeitet als juristische Mitarbeiterin bei LezziLegal. Sie hat in Luzern studiert. Ihr Schwerpunkt liegt im Bereich Datenschutzrecht.

Das Schweizer Arbeitsrecht im HR



Unternehmen und Personalverantwortliche stellen sich im Arbeitsalltag oft Fragen im Zusammenhang mit dem Arbeitsrecht. Das Handbuch soll als Arbeitshilfe dienen für alle, die im Personalwesen tätig sind und rechtssichere Antworten für ihre alltäglichen Fragen aus der Praxis suchen.

Umfang: 145 Seiten
Als Buch oder E-Book

Bestellung: www.weka.ch/personal/das-schweizer-arbeitsrecht-im-hr.html