

Loschelder Praxistipp

Der Zugriff auf die Mailbox ausgeschiedener Mitarbeiter

Wenn ein Mitarbeiter das Unternehmen verlässt, bleibt seine dienstliche Mailbox oft voller wichtiger Informationen – etwa zu Kunden, Projekten oder internen Abläufen. Für den Arbeitgeber kann es erforderlich sein, auf dieses Postfach zuzugreifen, um einen reibungslosen Betriebsablauf sicherzustellen. Technisch ist ein solcher Zugriff meist problemlos möglich. Die rechtliche Zulässigkeit ist jedoch nicht immer gegeben.

Grundlagen

Die dienstliche Mailbox stellt ein Arbeitsmittel dar und steht im Eigentum des Arbeitgebers. Dieser kann im Rahmen seines Weisungsrechts nach § 106 GewO den zulässigen Umgang mit dem Postfach festlegen. Es handelt sich hier um eine Konkretisierung der Art und Weise der Arbeitsleistung. Regeln für den Umgang können in internen Richtlinien, wie zum Beispiel einem „Best Practice“, festgehalten werden.

Bei dem Zugriff auf das dienstliche Postfach sollte zwischen zwei Kategorien von Datensätzen unterschieden werden, auf die unabhängig voneinander zugegriffen werden kann. Die Metadaten (oder auch Logfiles) geben Aufschluss über Kommunikationsabläufe, ohne den eigentlichen Inhalt der Nachrichten offenzulegen. Hieraus lassen sich die IP- und E-Mail-Adressen von Absender und Adressaten, die Menge der verschickten Daten, Zeitpunkt und Anzahl der Verbindungen und ggf. sogar die Betreffzeilen ablesen. Die Inhaltsdaten stellen den eigentlichen Inhalt der Nachricht dar. Enthalten sind der Mailtext und Anhänge der Mail. Beide Datensätze enthalten Informationen, die sich auf identifizierbare oder identifizierte Personen beziehen und stellen somit personenbezogene Daten i.S.d. Art. 4 Nr. 1 DSGVO dar.

Zulässigkeit der Datenverarbeitung

Jeder Zugriff auf E-Mail-Metadaten, ebenso wie auf den Inhalt der Kommunikation selbst, erfordert gem. Art. 5 Abs. 1 a), Art. 6 Abs. 1 DSGVO eine datenschutzrechtliche Rechtfertigung (sog. Verbot mit

Erlaubnisvorbehalt). Zudem müssen die Prinzipien des Art. 5 Abs. 1 DSGVO beachtet werden.

Die Datenverarbeitung ist grundsätzlich zulässig, wenn der Betroffene in die Verarbeitung seiner Daten einwilligt (§ 26 Abs. 2 BDSG, Art. 6 Abs. 1 lit. a DSGVO). Von der Bearbeitung betroffen i.S.d. Art. 4 Nr. 1 DSGVO ist jedoch nicht nur der ausgeschiedene Beschäftigte. Auch die Kommunikationspartner sind Betroffene i.S.d. DSGVO. Hierbei kann es sich um unternehmensexterne Dritte handeln, aber auch andere Mitarbeiter. Gegenüber jeder dieser Personen bedarf es beim Zugriff auf die Mailbox eine Rechtfertigung. Die vorherige Einholung einer Genehmigung sämtlicher Kommunikationspartner dürfte in der Praxis regelmäßig unmöglich oder zumindest unverhältnismäßig aufwendig sein.

Entscheidend ist daher die Möglichkeit einer Rechtfertigung nach den übrigen Rechtfertigungstatbeständen des Art. 6 Abs. 1 DSGVO. Sind die Daten erforderlich, damit der Arbeitgeber eine gesetzliche Pflicht erfüllen kann, kann die Verarbeitung auf Art. 6 Abs. 1 lit. c DSGVO gestützt werden. Insbesondere kommt jedoch Art. 6 Abs. 1 lit. f DSGVO in Betracht. Hiernach ist jede Verarbeitung zulässig, die zur Wahrung der berechtigten Interessen des Arbeitgebers oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte oder Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Hiernach kommt prinzipiell für jeden Datenverarbeitungsvorgang der ein ausreichend gewichtiges Interesse verfolgt, eine Rechtfertigung in Betracht. Über die Zulässigkeit der Datenverarbeitung entscheidet eine Interessenabwägung im Einzelfall.

Wird das Postfach rein dienstlich genutzt, ist der Zugang zu diesem grundsätzlich zulässig, solange der Arbeitgeber durch den Zugriff einen legitimen Zweck verfolgt. Ein solcher Zweck kann grundsätzlich in allen zur Durchführung und Organisation des Betriebs gebotenen Anlässen liegen. Wer mit geschäftlichen E-Mail-Adressen korrespondiert, muss damit rechnen, dass seine Mails weitere Verarbeitung erfahren. Den dienstlichen Interessen des Arbeitgebers wird daher grundsätzlich Vorrang eingeräumt. Ein direkter Zugriff auf das Postfach ist jedoch dann nicht erforderlich und damit nicht zulässig, wenn die benötigten Daten durch ein milderes Mittel erlangt werden können.

War die private Nutzung nicht gestattet, dürfte den Interessen des Arbeitgebers ebenfalls grundsätzlich ein Vorrang eingeräumt werden. Mitarbeiter dürfen nicht damit rechnen, dass ihre Kommunikation vertraulich bleibt, wenn sie entgegen den Anweisungen ihres Arbeitgebers die dienstliche Mailbox zur privaten Kommunikation nutzen. Der Zugriff ist dann regelmäßig zulässig, obwohl private Kommunikation betroffen ist.

Anders verhält es sich, wenn der Arbeitgeber die Privatnutzung der dienstlichen Mailbox gestattet oder duldet. Auch hier soll dem Arbeitgeber grundsätzlich das Recht zustehen, dienstliche Mails einzusehen. Kann bei einem Zugriff jedoch nicht ausgeschlossen werden, auch private Kommunikation auszulesen, kann der Zugriff ausnahmsweise unzulässig sein. Wird die Möglichkeit und der Umfang des Zugriffs jedoch vorher klar kommuniziert, kann sich dies im Rahmen der erforderlichen Interessenabwägung positiv für den Arbeitgeber auswirken und einen Verstoß gegen Art. 5 Abs. 1 lit. a DSGVO verhindern. Gleiches gilt in Bezug auf die Datenmenge. Der Arbeitgeber sollte nach Art. 5 Abs. 1 lit. c DSGVO die verarbeiteten Daten auf das Mindestmaß reduzieren.

Praxishinweis

In der Praxis kann im Vorfeld regelmäßig nicht mit Sicherheit bestimmt werden, ob eine dienstliche Mailbox – verbotenerweise – auch privat genutzt wurde. Für Arbeitgeber empfiehlt sich daher, bereits im Vorfeld klare Maßnahmen zu treffen und ein abgestuftes Zugriffsverfahren vorzusehen. Auf diese Weise werden die Interessen und Rechte der Beschäftigten und ihrer Kommunikationspartner gewahrt, während sich der Arbeitgeber rechtlich absichert und das Risiko möglicher Verstöße gegen Datenschutz- oder Kommunikationschutzvorschriften minimiert:

Zu Beginn des Arbeitsverhältnisses: individual- und kollektivvertragliche Regelungen

Im Vorfeld empfiehlt es sich, den Umgang mit der dienstlichen Mailbox verbindlich zu regeln. Der Arbeitgeber sollte die private Nutzung ausdrücklich untersagen, um einen rechtssicheren Zugriff auf das Postfach nach dem Ausscheiden des Arbeitnehmers zu gewährleisten. Darüber hinaus sollten Beschäftigte verpflichtet werden, vor ihrem Ausscheiden alle relevanten dienstlichen E-Mails auf einem gesonderten Speicherplatz abzulegen. Wird die private Nutzung der dienstlichen Mailbox ausnahmsweise gestattet, empfiehlt es sich, den

Arbeitnehmer zusätzlich anzuweisen, dienstliche und private Kommunikation klar voneinander zu trennen. Dies kann entweder durch die Löschung privater Nachrichten oder durch deren separate Speicherung erfolgen. Um eine gewisse Transparenz sicherzustellen, sollten die Beschäftigten zudem bereits zu Beginn ihres Beschäftigungsverhältnisses über die Möglichkeit und die Umstände eines möglichen Zugriffs auf ihre Mailbox nach ihrem Ausscheiden hingewiesen werden.

Achtung: Werden Beschäftigte angewiesen, schon während der Laufzeit ihres Anstellungsverhältnisses E-Mails oder sonstige Daten auf einem für den Arbeitgeber regelmäßig zugänglichen Weg abzuspeichern, eignet sich dies zur Überwachung der Beschäftigten. In diesen Fällen kann ein Mitbestimmungsrecht des Betriebsrats bestehen (§ 87 Abs. 1 Nr. 6 BetrVG).

Kurz vor Ausscheiden: Zustimmung oder Anweisung des Beschäftigten

Ist ein Ausscheiden und das Erfordernis des Zugriffs absehbar, empfiehlt es sich, mit den Beschäftigten das Gespräch zu suchen. Es sollte über mögliche Sichtsmaßnahmen bzgl. der dienstlichen Mailbox aufgeklärt werden. Der Beschäftigte sollte in diesem Gespräch angewiesen werden, entsprechende Sortierungsmaßnahmen bzgl. des relevanten Mailverkehrs vorzunehmen. Im besten Fall sollte zusätzlich die Genehmigung eingeholt werden, auf die Mailbox zugreifen zu können.

Zugriff auf das Postfach

Kann die private Kommunikation ausgesondert werden, ist ein Zugriff auf die Mailbox regelmäßig zulässig. Auch wenn keine Sortierungsmaßnahmen erfolgt sind, ist der Zugriff nicht vollständig ausgeschlossen. Der Arbeitgeber kann zunächst auf die LogFiles zugreifen und eine Sortierung eigenständig anhand der Betreffzeilen oder der Adressdaten vornehmen. Ein Zugriff auf Logfiles stellt zwar einen Eingriff dar, ist aber im Vergleich zum Zugriff auf den vollständigen Nachrichteninhalt weniger intensiv und einfacher zu begründen. Ein gestufter Zugriff kann dann erforderlich sein, wenn der Beschäftigte sich geweigert hat, eine Vorsortierung vorzunehmen oder aufgrund eines fristlosen Ausscheidens keine Möglichkeit zur Vorsortierung bestand. Um den datenschutzrechtlichen Grundsatz der Datenminimierung zu wahren, sollte der Zugriff auf Logfiles technisch möglichst gefiltert erfolgen. Die auszulesenden Datensätze

sind auf den betreffenden Arbeitnehmer sowie – soweit möglich – auf bestimmte Zeiträume und Kommunikationspartner zu begrenzen.

Besteht Gefahr im Verzug, kann im Zweifel unmittelbar auf den Inhalt der Nachrichten zugegriffen werden. Gefahr im Verzug liegt beispielsweise vor, wenn ohne die Informationen aus dem Postfach gesetzliche Pflichten nicht erfüllt werden können oder Schwierigkeiten mit Geschäftspartnern drohen.



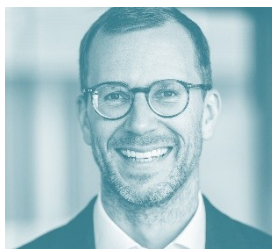
Unser Team Arbeitsrecht



Dr. Detlef Grimm
+49 221 650 65-129
detlef.grimm@loschelder.de



Dr. Martin Brock
+49 221 650 65-233
martin.brock@loschelder.de



Dr. Sebastian Pelzer
+49 221 650 65-263
sebastian.pelzer@loschelder.de



Arne Gehrke, LL.M.
+49 221 650 65-263
arne.gehrke@loschelder.de



Dr. Stefan Freh
+49 221 650 65-129
stefan.freh@loschelder.de



Farzan Daneshian, LL.M.
+49 221 65065-263
farzan.daneshian@loschelder.de



Dr. Sebastian Krülls, LL.M.
+49 221 65065-129
sebastian.kruells@loschelder.de



Dr. Baris Güzel
+49 221 65065-129
baris.guezel@loschelder.de



Dr. Moritz Waltermann
+49 221 65065-129
moritz.waltermann@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE

Partnerschaftsgesellschaft mbB

Konrad-Adenauer-Ufer 11

50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110

info@loschelder.de

www.loschelder.de