DataAgenda - das Lösungsportal
zum Datenschutzrecht

Präsentiert von DATAKONTEXT

www.DataAgenda.de

Checkliste Zugriff auf E-Mail-Postfach bei Abwesenheit oder Ausscheiden von Beschäftigten

Der Umgang mit personalisierten E-Mail-Konten länger abwesender oder ausgeschiedener Beschäftigter ist für Unternehmen vor dem Hintergrund der Aufrechterhaltung des Geschäftsbetriebs von grundlegendem Interesse. Im Zentrum steht die Frage, ob und unter welchen Voraussetzungen Arbeitgeber:innen auf betroffene Postfächer zugreifen dürfen.

1 Personalisierte Postfächer versus Funktionsadressen

Um datenschutzrechtlichen Konflikten vorzubeugen, sollten Unternehmen zunächst prüfen, ob die Einrichtung personalisierter E-Mail-Postfächer überhaupt erforderlich ist, oder ob Funktionsadressen (z.B. kundenservice@verantwortlicher.de) ausreichen. Eine unpersönliche E-Mail-Adresse, die für eine bestimmte Aufgabe, Rolle oder ein Team eingerichtet wird, ermöglicht es mehreren Personen gleichzeitig auf das Postfach zuzugreifen und E-Mails einzusehen oder zu bearbeiten. Bei Urlaub oder Krankheit ist die Vertretung sichergestellt, da Nachrichten nicht in einem persönlichen Postfach liegen bleiben. Beim Ausscheiden eines Beschäftigten bleibt die Adresse unverändert bestehen.

2 Privatnutzung untersagt versus Privatnutzung gestattet oder geduldet

Entscheidet das Unternehmen, Beschäftigten eine personalisierte E-Mail-Adresse zur Verfügung zu stellen, ist damit grundsätzlich die Frage verbunden, ob es den Beschäftigten damit die private Nutzung des betrieblichen E-Mail-Postfaches untersagt oder die private Nutzung gestattet oder dies zumindest duldet. Ist die Privatnutzung verboten, hat dies zur Folge, dass der gesamte E-Mail-Verkehr als geschäftliche Korrespondenz einzustufen ist. Andernfalls ist zunächst strittig, ob das Unternehmen zur Einhaltung des Fernmeldegeheimnisses nach § 3 TTDSG verpflichtet ist und damit als „Anbieter von Telekommunikationsdiensten“ gilt. Die Folge wäre, dass für Arbeitgeber nach § 3 Abs. 2 Nr. 1 oder 2 TDDDG das Fernmeldegeheimnis zu beachten wäre, inklusive des strafrechtlichen Verbots nach § 206 Abs. 1 StGB.

Die Tendenz in der rechtlichen Diskussion um die Anwendung des Fernmeldegeheimnisses auf Arbeitgeber entwickelt sich immer mehr in die Richtung, § 3 Abs. 2 TDDDG nicht als einschlägig anzusehen. Die Folge ist, dass „nur“ datenschutzrechtliche Vorgaben der DS-GVO und des BDSG zu beachten sind, jedoch keine Verbote nach § 3 Abs. 1 TDDDG oder nach § 206 StGB.

Vor dem Hintergrund der rechtlichen Diskussion sollten Unternehmen ihren Beschäftigten die private Nutzung des dienstlichen E-Mail-Accounts per se untersagen. Erlaubt das Unternehmen die private Nutzung des E-Mail-Postfachs sollte der Zugriff über eine **Einwilligung** geregelt werden. Die Be-

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

schäftigten haben demnach die Wahl, entweder die dienstlichen Kommunikationsmittel nicht privat zu nutzen oder das Angebot der Erlaubnis der privaten Nutzung durch den Arbeitgeber anzunehmen und gleichzeitig in bestimmte Zugriffsszenarien einzuwilligen. Ein transparenter Umgang mit der Kopplung an die private Nutzung ist dabei unerlässlich.

Unabhängig, ob eine Privatnutzung erlaubt oder verboten ist, sollten vor dem Hintergrund der Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO alle Umstände eines Postfach-Zugriffs jeweils aussagekräftig dokumentiert werden.

3 Grundsätzliche Voraussetzungen für einen Postfach-Zugriff

Unter datenschutzrechtlichen Vorgaben ist der Zugriff auf ein personalisiertes E-Mail-Postfach – unabhängig von einem Verbot oder einer Erlaubnis privater Nutzung - nur zulässig, wenn

- eine **Rechtsgrundlage nach Art. 6 DSGVO** vorliegt (z. B. Wahrung berechtigter Interessen, Einwilligung)
- der Zugriff **erforderlich und verhältnismäßig** ist, z. B. bei Krankheit, Austritt, laufenden Projekten
- Beschäftigte **transparent informiert** wurden (Art. 13 bzw. 14 DS-GVO)
- private Mails **erkannt und ausgespart** werden.

Unternehmen dürfen keinesfalls ohne Anlass Postfächer überwachen und Zugriffe ohne Regelungen mit und Information von Betroffenen durchführen. Zudem ist das Lesen privater Nachrichten verboten.

Unternehmen sollten klare, schriftliche Regelungen zur E-Mail-Nutzung treffen. Diese sollten im Arbeitsvertrag oder in Dienstanweisungen bzw. Richtlinien verankert sein. Existiert ein Betriebsrat, ist eine Betriebsvereinbarung zu dem Thema sinnvoll.

4 Wesentliche Schritte für einen datenschutzkonformen Umgang mit E-Mail-Accounts von Beschäftigten

Präventive Maßnahmen

- Klare Position des Unternehmens zur Privatnutzung (Verbot oder Erlaubnis mit entsprechenden Konsequenzen)
- Festlegung von technischen und/oder organisatorischen Maßnahmen zur Trennung privater und geschäftlicher Mails (z.B. separates privates Mailkonto für Beschäftigte, Verfahren zur Kennzeichnung privater E-Mails, Verschiebung privater Mails in separaten Ordner)
- Schriftliche Regelung zur E-Mail-Nutzung (Arbeitsvertrag, Betriebsvereinbarung, Richtlinie/Dienstanweisung)
- Festlegung von Archivierungs- und Löschregeln für dienstliche Mails
- Löschhinweise für private Mails
- Festlegung archivierungs- und zukunftsrelevante Inhalte grundsätzlich außerhalb des persönlichen E-Mail-Kontos abzulegen
- Information und Schulung der Mitarbeiter zu den im Unternehmen geltenden Regelungen
- Regelmäßige Kontrolle der Einhaltung der Unternehmensregelungen sowie Überprüfung und ggf. Anpassung der Festlegungen

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Technisch-organisatorische Maßnahmen

- Zugriffsprotokolle für E-Mail-Systeme
- Automatische Löschfristen nach betrieblichen und gesetzlichen Vorgaben
- Separate Aufbewahrung aufbewahrungspflichtiger E-Mails in Archivsystemen
- Dokumentation des Umgangs mit E-Mail-Accounts Beschäftigter im Verzeichnis der Verarbeitungstätigkeiten
- Technische Unterstützung des Zugriffs, bspw. durch Suchfunktionen, die nur E-Mails zu bestimmten Themen oder Korrespondenzpartnern anzeigen
- Regelmäßige Überprüfung und ggf. Anpassung der Prozesse

Zugriff während (längerer ungeplanter) Abwesenheit

- Vertretungsreglungen und Abwesenheitsnotiz: Für Abwesenheiten wie z.B. Urlaub, Krankheit oder Elternzeit (schriftlich) Vertretungsreglungen treffen. In einer Abwesenheitsnotiz auf die Vertretung hinweisen, sodass der oder diejenige kontaktiert werden kann.
- Vor Zugriff prüfen, ob ein milderes Mittel zur Zielerreichung besteht, bspw. ob der abwesende Beschäftigte ohne verhältnismäßig hohen Aufwand erreicht werden kann und die Informationen auf diesem Wege bereitgestellt werden können.
- Sofern eine Möglichkeit besteht, mit dem Beschäftigten zu kommunizieren, vorab versuchen eine Einwilligung (z.B**.** telefonisch oder per SMS) einzuholen.
- Wahl des „**mildesten Mittels**“, wenn Beschäftigter nicht erreicht werden kann
  - **Stufe 1:** Einrichtung einer automatischen Abwesenheitsnotiz durch die IT (ohne Mail-Einsicht), die Absender auffordert, sich an eine allgemeine Adresse zu wenden
  - **Stufe 2:** Weiterleitung ausschließlich zukünftig eingehender E-Mails an eine Vertretung
  - **Stufe 3:** Punktueller Zugriff auf bereits empfangene E-Mails, strikt beschränkt auf den relevanten Zeitraum und sachliche Suchbegriffe.
- Prüfung der **Erforderlichkeit und Verhältnismäßigkeit** vor jedem Zugriff auf das E-Mail-Konto des Beschäftigten (verhältnismäßig ist immer nur ein auf den Einzelfall bezogener, zeitlich begrenzter und kontrollierter Zugriff)
- Nur anlassbezogener, dokumentierter Zugriff bei konkretem Bedarf (Fokussierung auf konkrete Projekte, Kunden oder Vorgänge)
- Beschränkung auf geschäftlich notwendige E-Mails; keine Einsichtnahme in private E-Mails (stößt man bei einem Zugriff auf eine private Nachricht, muss der Zugriff auf diese Nachricht gestoppt werden, sobald der private Charakter erkennbar wird)
- **Vier-Augen-Prinzip**: Kein alleiniger Zugriff auf das E-Mail-Konto eines Beschäftigten, sondern z.B. in Abstimmung/im Beisein des Datenschutzbeauftragten, der IT und/oder (wenn vorhanden) auch unter Beisein des Betriebsrates
- **Schriftliches Protokoll**: Festhalten, wann und mit welcher Erforderlichkeit der Zugriff erfolgt ist, welche Personen daran beteiligt waren und welche Dateien angesehen wurden
- Nach Rückkehr des Beschäftigten Information, dass und in welchem Umfang auf sein Postfach zugegriffen wurde
- Passwortänderung: Falls eine Änderung des Passwortes notwendig war, ist das Passwort des Beschäftigten nach erfolgtem Zugriff zurückzusetzen und diesem nach seiner Rückkehr mitzuteilen.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com

Bei bevorstehendem Ausscheiden

- Strukturierte Übergabeplanung mit dem Beschäftigten (**Offboarding-Prozess**)
- Identifikation wichtiger Projekte, Kunden und Korrespondenzpartner
- Archivierung geschäftlicher E-Mails, die die Funktion eines Handels- bzw. Geschäftsbriefes oder eines Buchungsbelegs haben, durch den Beschäftigten selbst
- Weiterleitung relevanter geschäftlicher E-Mails an festgelegte Personen (z.B. Nachfolger, Vorgesetzter) durch den Beschäftigten selbst
- Im Fall privater Nutzung: Sichtung und Löschung privater Dateien durch den Beschäftigten selbst; ggf. Weiterleitung an privaten E-Mail-Account
- Dokumentation der übergebenden Informationen
- Festlegung des Zeitpunkts der Account-Deaktivierung
- Einrichtung einer automatischen Abwesenheitsnotiz (Hinweis auf Inaktivität des Accounts und Bitte um erneute Sendung der E-Mail an eine andere Mailadresse)

Zugriff nach dem Ausscheiden

- Zeitnahe Deaktivierung des Accounts für normale Zugriffe (von einer Weiterverwendung einer personalisierten E-Mail-Adresse ehemaliger Beschäftigter sollte grundsätzlich abgesehen werden)
- Prüfung der **Erforderlichkeit und Verhältnismäßigkeit** vor jedem Zugriff
- Nur anlassbezogener, dokumentierter Zugriff bei konkretem Bedarf (Fokussierung auf konkrete Projekte, Kunden oder Vorgänge)
- Beschränkung auf geschäftlich notwendige E-Mails; keine Einsichtnahme in private E-Mails (stößt man bei einem Zugriff auf eine private Nachricht, muss der Zugriff auf diese Nachricht gestoppt werden, sobald der private Charakter erkennbar wird)
- **Vier-Augen-Prinzip**: Kein alleiniger Zugriff auf das E-Mail-Konto eines Beschäftigten, sondern z.B. in Abstimmung/im Beisein des Datenschutzbeauftragten, der IT und/oder (wenn vorhanden) auch unter Beisein des Betriebsrates
- **Schriftliches Protokoll**: Festhalten, wann und mit welcher Erforderlichkeit der Zugriff erfolgt ist, welche Personen daran beteiligt waren und welche Dateien angesehen wurden
- Information des ehemaligen Beschäftigten über erfolgte Zugriffe

DataAgenda
ist das Lösungsportal zum Datenschutzrecht und fokussiert sich auf die inhaltlichen Entwicklungen in diesem Feld. Das DataAgenda-Experten-Team bietet Videos, News, Whitepaper und Seminartipps rund um den Datenschutz.

DataAgenda plus – powered by GDD
Mit diesem neuen Angebot haben Mitglieder der GDD e.V. exklusiv Zugriff auf folgende Umsetzungshilfen:
- RDV-Archiv
- IT-SICHERHEIT-Archiv
- Aktuelle Arbeitspapiere
- Muster und Checklisten zum Datenschutz
- Webinare zu aktuellen Datenschutz-Themen

Autor

Uwe Bargmann
Freiberuflicher Berater Datenschutzmanagement, Kooperationspartner der DMC Datenschutz Management + Consulting GmbH & Co KG



DATAKONTEXT
ist einer der führenden Fachinformationsdienstleister in den Bereichen Datenschutz und IT-Sicherheit und bietet Kompetenz aus einer Hand: Fachbücher, Fachzeitschriften und Seminare, Zertifizierung und Beratung.

DATAKONTEXT GmbH • Augustinusstraße 11 A • D – 50226 Frechen • Telefon: +49 22 34/989 49 -30 • Fax: +49 22 34/989 49 -32 • E-Mail: info@datakontext.com