## Up to Data:

# Austritt eines Mitarbeiters - was tun, wenn einer geht?

Namen, Adressen, Kontonummern, AU-Bescheinigungen oder Abmahnungen – als Arbeitgeber haben Sie jede Menge personenbezogene Daten von Ihren Mitarbeitern gespeichert. Datenschutzrechtlich ist das im laufenden Arbeitsverhältnis unproblematisch. Das sieht schnell anders aus, wenn Mitarbeiter Ihren Betrieb verlassen.

Aber meist sind die Prozesse zur Einstellung bzw. bei Austritt eines Mitarbeiters nicht klar definiert. So kann schnell eine unübersichtliche Lage hinsichtlich Rechte des Betroffenen, ausgegebener Arbeitsmittel entstehen oder Know-How und Geschäftsgeheimnisse gehen verloren. Schlimmstenfalls kann eine solche Situation in einer meldepflichtigen „Datenschutzpanne“ enden. Mit einigen einfachen betrieblichen Handlungsanweisungen werden diese Risiken jedoch erheblich minimiert. Aus Sicht des Datenschutzes ist es deshalb wichtig, die Datenschutzkontrolle bei Verfahren rund um den Austritt eines Mitarbeiters sehr genau zu nehmen und hier auch aktuelle Entwicklungen zu berücksichtigen. Prüfen Sie daher diese Verarbeitungstätigkeit nicht nur regelmäßig, sondern bringen Sie sie auch fortlaufend auf einen aktuellen Stand.

## Übersichtsliste Austritt eines Mitarbeiters

Wenn ein Mitarbeiter aus dem Unternehmen austritt, gibt es eine Vielzahl von anfallenden Tätigkeiten, welche beachtet werden müssen. So müssen Zugriffsberechtigungen und Zugangsrechte entzogen, Bilder des Mitarbeiters von der Internetseite oder auch Social Media Präsenzen entfernt, sowie Hardware entzogen werden.

Es empfiehlt sich daher als ersten Schritt eine Bestandsaufnahme der ausgegebenen Endgeräte, Zutritts- und Zugriffsrechte anzufertigen. Dies geschieht bestenfalls bereits bei Eintritt des Mitarbeiters ins Unternehmen. Anschließend sollte diese während des Beschäftigungsverhältnisses regelmäßig aktualisiert werden. Die Hardware mit Inventarnummern zu versehen, kann dabei auch zweckdienlich sein.

Folgende Maßnahmen dienen dabei als Anhaltspunkte dafür, was wichtig für ein Unternehmen beim Austritt eines Mitarbeiters sein könnte:

- Entzug der Zugriffsrechte auf Hardware, Software und Laufwerke
- Rückgabe des betrieblich überlassenen Smartphones
- Rückgabe von Hardware (Laptop, Tablet, USB-Stick, externe Festplatten o.ä.)
- Entzug von Zugangs-/Zutrittsrechten (Rückgabe von Schlüsseln oder Tokens)

- Rückgabe des Geschäftswagens
- Rückgabe von Werkzeugen

Im Falle eines Austrittes eines Mitarbeiters sollte es jeden Mitarbeiter klar sein, wie er vorzugehen hat. Es empfiehlt sich eine Prozessbeschreibung zu erstellen, um sowohl allgemeine als auch abteilungsbezogene Prozesse zu erkennen, damit diese in angemessener Zeit abgearbeitet werden können. Außerdem empfiehlt es sich für diesen Prozess auch ein Verzeichnis der Verarbeitungstätigkeit gemäß Artikel 30 Abs. 1 DSGVO zu erstellen.

## Bei der praktischen Umsetzung gibt es folgendes zu beachten:

Auch wenn ein Mitarbeiter innerhalb des Unternehmens die Abteilung wechselt, sollten durch die IT dann evtl. unnötige Zugriffsrechte bzw. Benutzerkonten für IT-Systeme entfernt werden.

Scheidet ein Mitarbeiter aus dem Unternehmen aus, darf es auf keinen Fall möglich sein, dass mit veralteten Passwörtern noch ein Zugang zu den IT-Systemen des früheren Arbeitgebers möglich ist und sie dann z. B. via Fernzugriff einsetzt werden können.

Ebenso darf es nicht passieren, dass sich Ex-Kollegen evtl. Hintertüren anlegen, wie z. B. neue oder zusätzliche Benutzerzugänge, welche aktiv und nutzbar bleiben.

**betriebliche E-Mail-Adresse**

Bereits im Vorfeld sollte eine Privatnutzung der betrieblichen E-Mail-Adresse ausgeschlossen sein. Damit auch nach Austritt des Mitarbeiters u. U. ein Zugriff des Unternehmens auf betriebliche Mails erfolgen kann. Außerdem ist es ratsam, dass der Mitarbeiter einen Abwesenheitsassistenten einrichtet und gleich auf den neuen Ansprechpartner hinweist.

In jedem Fall sollte ausgeschlossen werden, dass betriebliche E-Mails automatisch an private E-Mail-Adressen weitergeleitet werden können.

**personalisierte E-Mail-Adresse nicht weiterverwenden**

In Stellenausschreibungen wird heutzutage meist eine E-Mail-Adresse angegeben. Das sollte auf keinen Fall eine personalisierte E-Mail-Adresse von einem ehemaligen Mitarbeiter sein. Hier empfiehlt es sich generell mit einer Funktionsmail-Adresse zu arbeiten.

**Mitarbeiterfotos im Netz vollständig löschen**

Viele Betriebe verwenden Fotos von ihren Mitarbeitern in Flyern oder auf der Website. Liegt Ihnen für die Verwendung des Bildes eine Einwilligung vor, gilt diese bis zum Widerruf und endet nicht

automatisch mit dem Ende des Beschäftigungsverhältnisses. Doch diese Bilder sollten Sie als Arbeitgeber zeitnah löschen, sobald ein Mitarbeiter sein Einverständnis widerruft.

Sollte der ehemalige Mitarbeiter noch als Ansprechpartner für Kunden in Flyern oder auf der Homepage aufgeführt sein, ist dies nach dem Ende des Beschäftigungsverhältnisses von der Einwilligung nicht mehr gedeckt.

Deshalb kann es sinnvoll sein, die Bilder zeitnah zu löschen, bevor es der ehemalige Mitarbeiter verlangt. Die Löschung gilt in jedem Fall für individuelle personalisierte Porträtaufnahmen. Bei Gruppenbildern muss dies differenziert betrachtet werden. Alle Fotos des Mitarbeiters sollten dabei entfernt werden, z. B. auch in weitergehend verlinkten Medien.

**Ehemalige Mitarbeiter aus der Chat-Gruppe löschen**

Besteht im Unternehmen eine Chat-Gruppe zur Kommunikation im Team, dann sollte der Mitarbeiter auch hier umgehend nach Austritt aus dem Unternehmen aus der Gruppe entfernt werden.

## Beachten Sie auch die neuen Technologien

Zu den neuen Technologien gehören z. B. mobile Endgeräte, mobile Apps, Cloud-Services, BYOD1 und Social Media, auch diese sollten bei Austritt eines Mitarbeiters nicht unbeachtet bleiben.

**Cloud Computing[2]:**

- Sorgen Sie dafür, dass die IT die Zugänge für betriebliche Cloud-Services deaktiviert und nach der Datensicherung die Cloud-Daten gelöscht werden, wie dies auch für lokale und Netzwerk-basierte Dienste der Fall ist.
- Waren bei mobilen Mitarbeitern Cloud-Speicherdienste für den Austausch von Daten im Einsatz, müssen auch diese gesichert, geleert und deaktiviert werden.
- Wurde von dem Unternehmen die Verwendung eines privaten Cloud-Dienstes geduldet, müssen auch hier die betrieblichen Daten entfernt werden.

[1] BYOD „Bring your own device“: Bezeichnung dafür private mobile Endgeräte (Laptops, Tablets) zu integrieren.
[2] Nutzung von IT-Ressourcen über das Internet

**Soziale Netzwerke:**

- Genau wie bei Netzwerk- und Cloud-Diensten muss die IT die betrieblichen Zugänge der ausscheidenden Mitarbeiter deaktivieren und nach der Sicherung entfernen.
- Durfte der Mitarbeiter seine (privaten) Zugangsdaten zu sozialen Netzwerken auch für betriebliche Logins nutzen (Social Sign-in), muss diese Berechtigung entfernt werden.

**Mobile Endgeräte / mobile Apps / BYOD:**

- Manchmal überlassen Unternehmen ihren ehemaligen Mitarbeiter das nicht mehr ganz aktuelle Smartphone. Darauf aber könnten sich noch betriebliche Daten befinden. Diese Daten müssen gesichert und anschließend auf dem Gerät sicher gelöscht werden.
- War es dem Kollegen erlaubt, ein privates Gerät zu nutzen oder wurde das vielleicht geduldet, können sich darauf ebenfalls betriebliche Daten befinden. Die IT muss die Daten sichern und anschließend lokal löschen.
- Es kann zudem sein, dass sich betriebliche Apps mit Zugang zu betrieblichen Netzwerken oder Clouds auf den privaten Endgeräten befinden. Typisches Beispiel ist eine E-Mail-App für den betrieblichen Mail-Dienst. Diese Apps müssen entfernt werden, wenn der Beschäftigte das Unternehmen verlässt.

## Welche Aufbewahrungsfristen gelten für die Personalakte müssen eingehalten werden?

Auf Grundlage der DSGVO dürfen personenbezogene Daten nur so lange gespeichert werden, solange ein berechtigtes Interesse besteht. Hier sollte nach dem Prinzip der Datensparsamkeit und Datenminimierung gehandelt werden. Aufbewahrungsfristen können sich aus Anforderungen aus dem HGB oder aus der Abgabenordnung (AO) ergeben.

Nach dem Ausscheiden eines Mitarbeiters sollten Sie nicht alle Daten umgehend aus der Personalakte löschen. Folgende Daten müssen oder sollten aufbewahrt werden.

- So sind etwa 3 Jahre Speicherfrist für solche Daten notwendig, die für mögliche Schadensersatzansprüche bei arbeitsrechtlichen Auseinandersetzungen bedeutsam sind.
- Steuerrelevante Gehaltsunterlagen müssen Sie wegen der gesetzlichen Aufbewahrungsfrist bis zu 10 Jahre aufbewahren.
- Unterlagen, die Sie für Rechtsstreitigkeiten brauchen, dürfen Sie ebenfalls speichern. Haben Sie dem Mitarbeiter gekündigt, sollten Sie Abmahnungen und AU-Bescheinigungen aufbewahren, sofern diese für den Kündigungsgrund von Bedeutung sind. Sollten Sie mit der Krankenkasse um Lohnfortzahlung streiten, dann sollten Sie die AU-Bescheinigungen aufbewahren.

- Und bei Daten zu betrieblichen Altersversorgungszusagen können es im Extremfall sogar bis zu 30 Jahre sein.
- Eine dauerhafte Speicherung von Personaldaten mit Hinweis auf das Vorbeschäftigungsverbot des Teilzeit- und Befristungsgesetzes ist jedoch nicht zulässig.

## Facts zu Weihnachten:

- Deutschlands meistverkaufter Weihnachtsbaum ist die Nordmanntanne. Sie stammt allerdings ursprünglich aus dem Kaukasus, nicht – wie der Name vermuten lässt – aus Skandinavien. Die Kiefernart ist nämlich nicht nach Wikingern benannt worden, sondern nach dem Biologen Alexander von Nordmann. Der war aber immerhin Finne.
- In den Wochen vor Weihnachten werden jedes Jahr rund 28 Millionen Nadelbäume verkauft und meistens im Wohnzimmer aufgestellt.
- Früher hing man den Weihnachtsbaum aus Platzgründen sogar an der Decke auf.
- Der deutsche Durchschnittsweihnachtsbaum kommt auf eine Höhe von 1,64 m. Bei dieser Größe hat ein Tannenbaum übrigens mehr als 300.000 Nadeln. Wie viele davon nach Silvester noch dran sind, ist eine andere Sache.

In diesem Sinne wünschen wir Ihnen ein frohes und besinnliches Weihnachtsfest mit viel Erfolg, Glück und Gesundheit für das neue Jahr.

*Ihr Team der RKM Data*