

es in der Praxis zielführend sein, gewisse Daten oder Dokumente aus dem Personaldossier zehn Jahre ab Austritt aus dem Unternehmen aufzubewahren.

### Exkurs: Umgang mit Bewerbungsunterlagen

Auch bei Bewerbungsunterlagen sind die gesetzlichen Vorgaben zu beachten. Unterlagen von abgewiesenen Bewerbenden sind grundsätzlich direkt nach der Ablehnung zu retournieren oder zu vernichten. Das wäre zumindest aus datenschutzrechtlicher Sicht der Fall. Aus dem Gleichstellungsgesetz ergibt sich aber, dass abgelehnte Bewerbende noch drei Monate nach der Ablehnung Ansprüche wegen einer möglichen Diskriminierung geltend machen können. Insofern ist es

empfehlenswert, Bewerbungsunterlagen erst nach Ablauf dieser Frist zu vernichten. Eine Ausnahme besteht, wenn die betroffene Person ausdrücklich in eine längere Aufbewahrung eingewilligt hat. Bei elektronisch eingereichten Unterlagen ist eine Rückgabe nicht möglich, und die Dokumente sind daher zu vernichten.

### Zulässigkeit einer längeren Aufbewahrung

Eine über die gesetzlichen Fristen hinausgehende Aufbewahrung von Personendaten ist nur dann zulässig, wenn die betroffene Person ausdrücklich zugestimmt hat oder die Interessen an der Aufbewahrung nach einer Interessenabwägung überwiegen (z. B. bei einem sich anbahnenden oder be-

stehenden Rechtsstreit). Ohne Einwilligung oder berechtigtes Interesse ist eine weitere Bearbeitung und Aufbewahrung datenschutzrechtlich nicht erlaubt.

### AUTOREN



**Marco S. Meier**, RA, MLaw, CIPP/E, ist Partner bei Binder Rechtsanwälte KLG. Seine Tätigkeitsschwerpunkte liegen im Datenschutz- und IT-Recht sowie in technologiebezogenen Compliance-Fragen.



**Janis Alpstätig**, B.A. HSG in Law and Economics, Substitut bei Binder Legal KLG. Seine Tätigkeitsschwerpunkte liegen in verschiedenen Bereichen des Privat- und Wirtschaftsrechts, insbesondere in den Bereichen Gesellschafts-, Vertrags-, Datenschutz- und Arbeitsrecht.

## Datensicherheit beim Personaldossier

In Zeiten zunehmender Digitalisierung und wachsender regulatorischer Anforderungen ist der sorgfältige Umgang mit Personaldaten wichtiger denn je. Das Personaldossier enthält besonders schützenswerte Daten. Gemäss dem Datenschutzgesetz (DSG) und der Datenschutzverordnung (DSV) gelten klare Vorgaben für die sichere Aufbewahrung, den Zugriff und die Vernichtung dieser Unterlagen. Dieser Artikel beleuchtet die gesetzlichen Anforderungen und gibt praktische Empfehlungen zur rechtskonformen Umsetzung in Unternehmen.

■ Von Lukas Lezzi, Alexandra Egger

### Gesetzlicher Rahmen

Das Personaldossier enthält alle vom Arbeitgeber gespeicherten Informationen über den Arbeitnehmer, z. B. Personalien, Arbeitsverträge, Löhne, Qualifikationen, Absenzen oder Disziplinarverfahren. Die Bearbeitung dieser Daten richtet sich nach dem Datenschutzgesetz (DSG) und der Datenschutzverordnung (DSV). Gemäss DSG dürfen Personendaten nur nach den Grundsätzen der Rechtmässigkeit, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität, Vertraulichkeit und Rechenschaftspflicht bearbeitet werden (Art. 6 DSG).

Besonders schützenswerte Daten (z. B. Gesundheitsdaten oder religiöse Überzeugungen) unterliegen strengeren Anforderungen, etwa an technische und organisatorische Massnahmen (Art. 8 DSG). Besteht ein hohes Risiko für die Persönlichkeit oder Grundrechte, ist zusätzlich eine Datenschutz-Folgenabschätzung (DSFA) erforderlich. Diese umfasst eine Beschreibung der Datenbearbeitung, Risikobewertung und Schutzmassnahmen (Art. 22 DSG).

### Aufbewahrungspflichten Physische Dossiers

Papierbasierte Personaldossiers müssen so aufbewahrt werden, dass unbefugte Dritte keinen Zugang erhalten.

Konkret bedeutet dies:

- Aufbewahrung in abschliessbaren Schränken oder Räumen mit Zutrittsbeschränkung
- Nur berechtigte Personen (z. B. HR-Abteilung, direkte Vorgesetzte mit berechtigtem Interesse) dürfen Zugriff erhalten.
- Schutz vor Feuer, Wasser und anderen Umwelteinflüssen durch geeignete Lagerbedingungen
- keine Ablage an öffentlich zugänglichen Orten, auch nicht temporär (clean desk)

### Elektronische Dossiers

Technische und organisatorische Massnahmen (TOMs) müssen dem



Schutzbedarf angemessen sein. Bei digitalen Personaldossiers gelten zusätzliche Anforderungen an die technischen und organisatorischen Massnahmen gemäss Art. 3 DSV.

#### a. Technische Massnahmen

- Zugriffskontrollen:
  - rollenbasierte Berechtigungskonzepte, die sicherstellen, dass nur autorisierte Personen auf bestimmte Daten zugreifen können, die für die Erfüllung ihrer Aufgaben erforderlich sind
  - Zwei-Faktor-Authentifizierung (2FA)
  - Protokollierung: Alle Zugriffe, Änderungen, Vernichtungen oder Downloads von Personaldaten müssen nachvollziehbar sein und sollten daher automatisch protokolliert werden (Art. 4 Abs. 1 DSV).
- Verschlüsselung: Besonders schützenswerte Personaldaten müssen bei der Übertragung (z. B. TLS/SSL) als auch bei der Speicherung (at rest) verschlüsselt werden.
- Speichermedienschutz
  - Datenträgerkontrolle: keine Speicherung auf mobilen Datenträgern (USB-Sticks, externe Festplatten) ohne Verschlüsselung
  - Serverräume oder Rechenzentren müssen abgeschlossen und gesichert sein.

- Physischen Zugang dürfen nur berechtigte Personen haben.
- Back-ups & Wiederherstellung:
  - regelmässige, sichere Datensicherungen – idealerweise in der Schweiz oder in Ländern mit angemessenem Datenschutzniveau (gemäss EDÖB): Back-ups unterliegen denselben Schutzvorgaben wie Primärdaten.
  - Im Notfall (z. B. technischer Ausfall) muss eine rasche Wiederherstellung der Daten möglich sein (Disaster Recovery).
- Netzwerksicherheit: Firewalls, Intrusion Detection Systems, VPNs müssen auf dem aktuellen Stand installiert und regelmässig überprüft werden.

#### b. Organisatorische Massnahmen:

- Informationssicherheitsstrategien und -prozesse: Es muss ein umfassender, systematischer und realistischer Risikokatalog erarbeitet werden, welcher die Bedrohungen und Schwachstellen von Geschäftsanwendungen und die Massnahmen zur Risikominderung beschreibt.
- Meldepflicht von Datenschutzverletzungen: Es muss klar geregelt werden, wer eine Datenschutzverletzung bewertet und entscheidet, ob eine Meldung an den EDÖB

(Art. 24 DSGVO: «sofern ein hohes Risiko besteht») oder andere Behörden erfolgen muss, bzw. diese vornimmt.

### Verantwortlichkeiten und Datenschutzprinzipien

Der Arbeitgeber ist im Sinne des DSGVO Verantwortlicher für die Datenbearbeitung und somit verpflichtet, die Einhaltung der Datenschutzvorschriften zu gewährleisten. Dazu gehören:

- Rechtmässigkeit: Die Datenbearbeitung muss nach Treu und Glauben und verhältnismässig erfolgen (Art. 6 DSGVO).
- Datenminimierung: Es dürfen nur diejenigen Daten erhoben und bearbeitet werden, die für den Zweck erforderlich und sachlich gerechtfertigt sind (Art. 6 Abs. 2 DSGVO).
- Zweckbindung: Personendaten dürfen nur für den klar bestimmten und rechtmässigen Zweck bearbeitet werden, der bei der Erhebung angegeben wurde – z. B. Personaladministration, Lohnabrechnung, Sozialversicherung (Art. 6 Abs. 3 DSGVO).
- Richtigkeit: Die Personendaten müssen sachlich richtig und aktuell sein. Unrichtige oder veraltete Daten sind zu berichtigen oder zu löschen (Art. 6 Abs. 5 DSGVO).
- Rechenschaftspflicht: Der Arbeitgeber muss z. B. durch Dokumentationen, Verzeichnisse von Bearbeitungstätigkeiten, Datenschutzrichtlinien nachweisen können, dass er die Datenschutzpflichten einhält.

### Praktische Umsetzung: Datenschutzkonzept

Ein wirksames Datenschutzkonzept soll sämtliche Aspekte der Personaldatenbearbeitung regeln, von der Erhebung über die Aufbewahrung bis hin zur Löschung. Wichtige Bestandteile sind:

- interne Richtlinien betreffend Aktenführung: standardisierte Ablagestrukturen, Verantwortlichkeiten, Versionskontrollen
- regelmässige Schulungen für HR, Vorgesetzte und IT zur Sensibilisierung auf Datenschutzthemen

## HINWEISE



Das Datenschutzkonzept der Unternehmung soll folgende Punkte beinhalten:

- interne Richtlinien
  - wie die Datenschutzgrundsätze eingehalten werden
  - wie die Aktenführung erfolgen soll
- regelmässige Schulungen für HR, Vorgesetzte und IT zur Sensibilisierung für Datenschutzthemen
- Vertraulichkeitserklärungen für Mitarbeitende mit Zugang zu Personaldossiers
- Datenschutzerklärung für die Transparenz gegenüber den betroffenen Personen
- Dokumentation, welche technischen und organisatorischen Massnahmen (TOMs) getroffen werden zum Schutz der Personendaten
- Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSGVO)
- Meldemechanismen für Datenschutzverletzungen und definierte Prozesse bei Sicherheitsvorfällen
- Evaluation und Auditierung der eingesetzten technischen Systeme auf Sicherheitslücken

- Vertraulichkeitserklärungen für Mitarbeitende mit Zugang zu Personaldossiers
- Datenschutzerklärung: klar und transparent, leicht zugängliche Information der Mitarbeiter, wie ihre Personendaten erhoben, bearbeitet und geschützt werden und was ihre Rechte sind (Art. 13 DSGVO)
- Auftragsbearbeitungsvertrag: Besonders bei der Auslagerung von Personaldaten an Drittdienstleister (z.B. Cloud-Anbieter oder Lohnbuchhalter) ist sicherzustellen, dass der Auftragnehmer die gesetzlichen Vorgaben ebenfalls einhält (Art. 9 DSGVO).
- Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSGVO): Übersicht aller Datenbearbeitungen im Unternehmen, welche den Zweck der Bearbeitung, die Kategorien von bearbeiteten Personendaten, die Kategorien von betroffenen Personen, die Empfänger sowie die Aufbewahrungsdauer und technische und organisatorische Massnahmen (TOM) dokumentiert

- Meldemechanismen für Datenschutzverletzungen und definierte Prozesse bei Sicherheitsvorfällen: interne Meldung, Erstbeurteilung durch Datenschutzbeauftragte, Meldung beim EDÖB bei hohem Risiko für die betroffenen Personen
- Evaluation und Auditierung der eingesetzten technischen Systeme auf Sicherheitslücken: z.B. Penetration Testing, Schwachstellenscanning, Prüfung von Zugriffsberechtigungen, Überprüfung von Back-up- und Recovery-Verfahren

## Löschung und Archivierung

Sobald der Zweck der Datenbearbeitung erfüllt ist – etwa nach Beendigung des Arbeitsverhältnisses –, sind die Daten zu löschen, sofern keine gesetzliche Aufbewahrungspflicht besteht. Die Löschung muss sicher und nachvollziehbar erfolgen:

- Papierdokumente: Vernichtung durch Schredder nach DIN 66399 nach der für die entsprechenden Personendaten geeigneten Sicherheitsstufe (z.B. für Personaldaten Sicherheitsstufe 4 oder 5)
- digitale Daten: sicheres Überschreiben oder physische Zerstörung der Datenträger
- Archivierung: Falls eine gesetzliche oder vertragliche Aufbewahrungspflicht besteht (z.B. zehn Jahre für Lohnabrechnungen), sind diese getrennt vom aktiven Dossier aufzubewahren.

## Straf- und Haftungsrisiken bei Verstössen

Unzulässige Bearbeitung besonders schützenswerter Daten kann zu:

- zivilrechtlicher Haftung wegen Persönlichkeitsverletzung (Art. 28 ZGB i.V.m. Art. 31 DSGVO),
- verwaltungsrechtlichen Massnahmen durch den EDÖB,
- strafrechtlichen Sanktionen (z.B. bei Verletzung der Datensicherheit) führen.

## Fazit

Die sichere Aufbewahrung von Personaldossiers ist in jeder Unternehmung

## HINWEISE



Bei digitalen Personaldossiers gelten zusätzliche Anforderungen an die technischen und organisatorischen Massnahmen (Art. 8 DSGVO):

Technische Massnahmen:

- Zugriffskontrollen: Rollenbasierte Berechtigungskonzepte, Zwei-Faktor-Authentifizierung (2FA), Protokollierung von Zugriff, Änderungen oder Vernichtung von Daten
- Verschlüsselung: Besonders schützenswerte Personendaten müssen bei der Übertragung (z.B. TLS/SSL) als auch bei der Speicherung (at rest) verschlüsselt werden.
- Back-ups & Wiederherstellung: regelmässige, sichere Datensicherungen und schnelle Wiederherstellung der Verfügbarkeit der Daten im Falle eines physischen oder technischen Zwischenfalls (Disaster Recovery)
- Netzwerksicherheit: Firewalls, Intrusion Detection Systems, VPNs müssen auf dem aktuellen Stand installiert und regelmässig überprüft werden.

von zentraler Bedeutung. Die Arbeitgeber sind verpflichtet, geeignete technische und organisatorische Massnahmen zu ergreifen, um die Datensicherheit zu gewährleisten. Wer die gesetzlichen Vorgaben kennt und umsetzt, schützt nicht nur die Rechte der Mitarbeitenden, sondern auch das Unternehmen vor rechtlichen und Reputationsrisiken. Ein systematisches Datenschutzmanagement, unterstützt durch klare Prozesse, internen Richtlinien und regelmässige Schulung, bildet dabei die Grundlage für eine rechtskonforme und vertrauenswürdige Personaldatenbearbeitung.

## AUTOREN



**Lukas Lezzi** ist selbstständiger Rechtsanwalt in Zürich (LezziLegal). Seine Tätigkeitsschwerpunkte liegen im Bereich Datenschutz- und Finanzmarktrecht.



**Alexandra Egger** arbeitet als Juristin bei LezziLegal. Sie arbeitet hauptsächlich im Bereich des Datenschutzrechts.