

Merkblatt: Richtiger Umgang mit Personaldaten

1. Ausgangslage

Ob Leistungsbeurteilung, Gesundheitsdaten, Weiterbildung – im Personalbereich werden zahlreiche Daten bearbeitet. Dies ist zur Durchführung des Arbeitsverhältnisses erforderlich. Der Arbeitgeber ist dabei allerdings dazu verpflichtet, die Privatsphäre – eines der kostbarsten Güter der Mitarbeitenden – zu schützen. Was sind Personaldaten?

Personaldaten stellen eine Unterkategorie der Personendaten im Sinne von § 3 Absatz 3 des Gesetzes über die Information und den Datenschutz¹ dar. Als Personaldaten, Personalakten und Personaldossier gelten alle Dokumente zu einem bestimmten Arbeitsverhältnis, die vom Arbeitgeber aufbewahrt werden, unerheblich, ob in elektronischer oder in Papierform. Das sind beispielsweise Personalien, Arbeitsverträge und Arztzeugnisse.

Personaldaten sind somit Informationen, Unterlagen und Daten, die einer Person klar zugeordnet werden können (z. B. durch Angabe ihres Namens, ihrer Personal- oder Registernummer). Hierbei ist von vertraulichen Daten auszugehen. Zu finden sind diese Informationen beispielsweise im Personalinformations- und Lohnsystem SAP, im elektronischen Personaldossier, in der digitalen Applikation SAP SuccessFactors sowie im e-Recruiting Prozess.

2. Was fällt unter das Bearbeiten von Personaldaten?

Jeder Umgang mit Personaldaten gilt als Bearbeiten im Sinne des Datenschutzgesetzes. Darunter fallen unter anderem das Beschaffen, Aufbewahren, Lesen, Verändern, Bekanntgeben, Archivieren, Löschen und Vernichten. Ein öffentliches Organ darf Personaldaten bearbeiten, wenn eine gesetzliche Grundlage besteht oder, wenn dies zur Erfüllung einer gesetzlichen Aufgabe erforderlich ist. § 10 Absatz 1 des Personalgesetzes² erlaubt das Bearbeiten von Personendaten zur Beurteilung der Eignung, der Leistung und des Verhaltens der Mitarbeitenden während des Arbeitsverhältnisses. Wichtig ist dabei, dass das Bearbeiten auf ein Minimum beschränkt wird (Grundsatz: so wenig wie möglich, so viel wie nötig).

Alle vertraulichen Daten müssen sowohl technisch (z. B. mittels Verschlüsselung und Schutz vor Zutritt zu Räumlichkeiten) wie auch organisatorisch (mittels Richtlinien, Clean Desk Policy etc.) gegen die Einsicht für Unbefugte geschützt werden. Zudem dürfen keine vertraulichen Daten ausserhalb der dafür vorgesehenen Bereiche abgespeichert werden (z. B. auf einem lokalen Laufwerk oder ausserhalb der Applikation).

Werden elektronische Zugriffsrechte eingerichtet, damit bei der Erfüllung einer gesetzlichen Aufgabe der Zugriff auf die relevanten Daten für die dafür vorgesehenen Personen gewährleistet ist, erfordert u. a. der Datenschutz von allen Mitarbeitenden, welche über die Zugriffsrechte verfügen, einen sorgfältigen Umgang.

3. Wer kann Personaldaten einsehen?

Personaldaten sind strengstens vertraulich zu behandeln. Einsicht dürfen nur Personen erhalten, die sich dafür auf eine gesetzliche Grundlage stützen oder dies zur Erfüllung einer gesetzlichen Aufgabe benötigen. Im Rahmen des Arbeitsverhältnisses sind dies beispielsweise die zuständigen Vorgesetzten, das Personalamt, die HR-Beratung und unter Umständen der technische Support. Die Details sind in der Verordnung über den Umgang mit Personaldaten³ geregelt.

¹ Gesetz über die Information und den Datenschutz vom 10. Februar 2011 (Informations- und Datenschutzgesetz, IDG; [SGS 162](#))

² Gesetz über die Arbeitsverhältnisse der Mitarbeiterinnen und Mitarbeiter des Kantons vom 25. September 1997 (Personalgesetz; [SGS 150](#))

³ Verordnung über den Umgang mit Personaldaten vom 16. April 2013 ([SGS 150.21](#))

Jede Mitarbeiterin, jeder Mitarbeiter kann grundsätzlich Einsicht in ihre bzw. seine eigenen Personaldaten bei der zuständigen HR-Beratung nehmen. In Ausnahmefällen können rechtliche Gründe gegen eine Einsicht sprechen.

4. Dürfen Personaldaten bekanntgegeben werden?

Bekanntgeben ist jedes Zugänglichmachen von Informationen wie Einsicht gewähren, Weitergeben oder Veröffentlichen. Auch hier gilt, dass Personaldaten nur bekanntgegeben werden dürfen, wenn diesbezüglich eine gesetzliche Grundlage besteht oder diese Personaldaten zur Erfüllung einer gesetzlichen Aufgabe benötigt werden.

Sind die oben genannten Voraussetzungen nicht erfüllt, darf die Weitergabe an Dritte wie beispielsweise ein neuer Arbeitgeber, Bank- oder Kreditinstitute oder die Vermieterschaft nur mit schriftlicher Zustimmung der bzw. des Mitarbeitenden erfolgen.

5. Was ist nicht erlaubt?

Nicht erlaubt sind das Führen von sogenannten «Schattendossiers» oder «graue Dossiers», zumal die Mitarbeitenden Anspruch auf Zugang zu den eigenen Personaldaten haben. Aus diesem Grund ist es nicht möglich, einzelne Teile des Dossiers abzuspalten oder parallel noch ein weiteres Personaldossier zu führen. Persönliche Notizen der vorgesetzten Personen (beispielsweise Gedächtnisstützen für das MAG etc.) sind hingegen nicht als Schattendossier zu werten und müssen somit nicht offengelegt werden.

Zur Beurteilung der Eignung, der Leistung und des Verhaltens der Mitarbeitenden für das Arbeitsverhältnis dürfen keine Überwachungs- und Kontrollsysteme eingesetzt werden, die der Überwachung des Verhaltens der Mitarbeitenden dienen. Darunter fallen alle technischen Einrichtungen, durch die einzelne oder mehrere Tätigkeiten oder Verhaltensweisen der Mitarbeitenden erfasst werden wie beispielsweise

- die Videoüberwachung am Arbeitsplatz;
- das Aufzeichnen von Telefongesprächen;
- das Anbringen und Auswerten von Ortungssystemen an Dienstfahrzeugen zur Lokalisation (GPS-System);
- die Auswertung der Ortungsdaten von geschäftlichen Mobilgeräten;
- das Aufzeichnen und Auswerten von Daten aus Schliesssystemen, Türzugängen, Lift-Benutzung o.ä.;
- der Einsatz von Spionageprogrammen;
- die Auswertung der Anrufliste und des Internetbrowserverlaufs.
- der Einsatz von Programmen zur Standortverfolgung oder zur Kontaktnachverfolgung

Zulässige Kontroll- und Überwachungsmassnahmen sind abschliessend in den §§ 22 ff. des Benutzungsreglements Informatikmittel⁴ enthalten. Demnach darf die Zentrale Informatik ausnahmsweise den Internetbrowserverlauf einer oder eines Mitarbeitenden überprüfen, wenn ein Verdacht auf Verstoß gegen das Benutzungsreglement Informatikmittel besteht. Dies darf aber nicht rückwirkend geschehen, sondern nur nach Ankündigung.

Im Rahmen eines Bewerbungsprozesses ist es nur bedingt zulässig, Informationen über Stellenbewerbende im Internet zu suchen. Denn Personendaten von Stellenbewerbenden und Mitarbeitenden dürfen vom Arbeitgeber nur bearbeitet werden, soweit sie für die Beurteilung der Eignung, der Leistung und des Verhaltens für das Arbeitsverhältnis notwendig und geeignet sind. Unter anderem dürfen private soziale Netzwerke wie Facebook, Instagram, TikTok oder X (ehemals Twitter) vom Arbeitgeber nicht nach Informationen über Stellenbewerbende durchsucht werden. Die dort geteilten Beiträge geben Einblick in die Privatsphäre und richten sich meist an einen beschränkten Benutzerkreis. Weisen Stellenbewerbende im Bewerbungsdossier oder -gespräch hingegen ausdrücklich auf ihr Profil in einem sozialen Netzwerk hin, darf dieses vom Arbeitgeber ausnahms-

⁴ Benutzungsreglement Informatikmittel vom 16. Dezember 2014 ([SGS 140.551](#))

weise konsultiert werden. Dasselbe gilt für persönliche Webseiten, Blogs und Ähnliches. Im Gegensatz zu den privaten sozialen Netzwerken dürfen Personendaten aus sozialen Netzwerken mit vorwiegend beruflichem Charakter (z. B. LinkedIn oder Xing) von Arbeitgebenden beschafft und verwendet werden. Diese Profile enthalten grundsätzlich berufsbezogene Informationen, welche die Betroffenen potenziellen Arbeitgebenden bewusst zur Kenntnis bringen wollen.

Nicht erlaubt ist weiter die Einholung von Referenzauskünften ohne das explizite Einverständnis der bzw. des Bewerbenden. Aus der Bewerbung muss klar und unmissverständlich hervorgehen, dass Bewerbende vorbehaltlos die Einwilligung zum Einholen von Auskünften erteilen. Diese Voraussetzung ist mit der blossen Erwähnung von allfälligen Referenzpersonen nicht implizit gegeben. Auch die Erteilung einer Referenzauskunft an einen potentiellen Arbeitgeber über aktuelle oder ehemalige Mitarbeitende setzt deren vorgängiges Einverständnis voraus.

Gesetzeswidrige oder missbräuchliche Zugriffe auf Personaldaten können personalrechtliche Konsequenzen nach sich ziehen.