Personaldossier und Datenschutz

Auf Schritt und Tritt beobachtet – das Smartphone ist der Spion im Hosensack. Auch im Rahmen des Arbeitsverhältnisses werden viele Daten generiert. Einige davon landen im Personaldossier – wie ein korrekter Umgang damit aussehen sollte, wird nachstehend erläutert.

Von Ursula Uttinger

Bewerbungsphase

Noch bevor man eine Stelle antritt, werden Daten bearbeitet – und selbst nach dem Austritt aus einem Unternehmen verbleiben viele Daten im Personaldossier, zu viele? Ein Personaldossier kann, je nach Unternehmen, eine richtiggehende Lebensgeschichte erzählen über eine Person. Denn nach wie vor werden Daten gesammelt und viel zu selten vernichtet und definitiv gelöscht. Die Angst, etwas im entscheidenden Moment nicht mehr zur Hand zu haben, ist oft gross. Dabei gibt es gesetzliche Vorgaben, was erlaubt ist.

Bevor ein Dossier angelegt werden kann, bewerben sich Menschen. Bereits hier stellen sich erste datenschutzrechtliche Fragen, insbesondere da kaum mehr Bewerbungen in Papier erfolgen und sich folglich auch die Frage stellt, auf welchen Servern die Daten liegen. Bei einem elektronischen Erfassungstool sollten die Bewerbenden informiert werden, was mit den Daten passiert. Je nachdem, ob die Daten durch ein automatisiertes Tool oder von einem Menschen bearbeitet werden, ergeben sich andere Folgen – insbesondere mit Blick auf die Revision des schweizerischen Datenschutzgesetzes.

Bei einer automatisierten Datenbearbeitung mit Folgen für betroffene Personen, indem diese beispielsweise nicht zu einem Bewerbungsgespräch eingeladen werden, müssen diese informiert werden; sie haben dann auch das Recht, eine Bearbeitung durch Menschen zu verlangen. Ob diese zu einem anderen Ergebnis kommen oder dann einfach den Entscheid des Tools bestätigen werden, ist abzuwarten. Vor allem lässt sich bei einer Absage für eine Stelle kaum nachweisen, ob die angegebenen Gründe stimmen oder einen Vorwand darstellen.

Sobald Daten elektronisch einverlangt werden, gilt es sicherzustellen, dass diese nicht auf Servern in einem Land ohne gleichwertigen Datenschutz landen. Eine neue Tendenz besteht darin, dass man sich per WhatsApp bewerben kann.[1] WhatsApp ist nicht für einen hohen Datenschutz bekannt. Doch solange eine Alternative zur Verfügung steht, entscheiden die Bewerbenden selbst, wie hoch sie den Datenschutz gewichten. Es ist nicht Aufgabe eines Unternehmens, sich paternalistisch zu verhalten und einen solchen Kanal zu verbieten.

Grundsätzlich sollte auch für eine Bewerbung ein jederzeitiger Widerruf möglich sein; wird eine Person nicht angestellt, gilt es, die Daten nach Absage definitiv zu vernichten. Dies ergibt auch Sinn, um keinen Datenfriedhof zu generieren.

Je nach Funktion kann sich eine Personensicherheitsüberprüfung aufdrängen. Bevorzugt wird eine solche durch ein spezialisiertes Unternehmen mit Einwilligung der betroffenen Person gemacht. Der Vorteil: Das spezialisierte Unternehmen gibt nur die für eine Funktion relevanten Daten weiter. Grundsätzlich Zurückhaltung ist bezüglich eines Strafregisterauszugs geboten:[2] Heute werden Strafregisterauszüge inflationär einverlangt. Ein Argument lässt sich leicht finden; bei einer kritischeren Prüfung desselben sind diese Argumente oft nicht stichhaltig.

Daten dürfen grundsätzlich nur im Rahmen von Art. 328b OR[3] erhoben werden, also wenn diese Daten im Zusammenhang mit der Eignung für eine Funktion tatsächlich notwendig sind. Dies ist kritisch zu hinterfragen.

Anstellung

Bei der Anstellung wandern die Bewerbungsunterlagen in das Personaldossier. In einem ersten Schritt ist dies korrekt; doch nach Beendigung der Probezeit sollten alle Unterlagen, die nicht zwingend notwendig sind – wiederum im Sinne von Art. 328b OR – zurückgegeben beziehungsweise vernichtet werden. Muss nachgewiesen werden, dass eine Person eine bestimmte Ausbildung absolviert hat, dann darf dieser Nachweis selbstverständlich aufbewahrt werden.

Wird im Zusammenhang mit der Anstellung ein Assessment oder ein Test gemacht, hat die betroffene Person Anrecht auf eine Kopie dieser Unterlagen. Doch auch diese Unterlagen sind spätestens nach zwei Jahren zu vernichten; die Aussagen sind zu einem Zeitpunkt korrekt, verlieren jedoch mit der Zeit an Gültigkeit/Richtigkeit.[4]

Im Verlaufe der Anstellung sammeln sich sehr viele Informationen; regelmässig sollte das Personaldossier «ausgemistet» werden[5] im Sinne der Verhältnismässigkeit von Art. 4 Abs. 2 DSG[6] bzw. von Art. 6 Abs. 4[7] nDSG.

Bei Mitarbeiterbeurteilungen sollte ebenfalls im Sinne der Verhältnismässigkeit die Aufbewahrungsfrist definiert werden; auch wenn immer weniger Mitarbeitende ein Leben lang beim selben Arbeitgeber bleiben, sollten die Mitarbeiterbeurteilungen nach spätestens fünf Jahren vernichtet werden.[8] Auch hier gilt: Bei wiederholt ungenügenden Leistungen sollte direkt gehandelt werden; seien es Unterstützungsmassnahmen, Versetzung oder Beendigung des Arbeitsverhältnisses. Nach Jahren auf eine alte, ungenügende Mitarbeiterbeurteilung zurückzukommen, ist nicht sinnvoll. Auch wenn gerade in Unternehmen mit Vorgaben, bevor eine Kündigung ausgesprochen werden darf, gerne alles aufbewahrt wird, um später auf eine schlechte Beurteilung zurückkommen zu können.

Bei Arztzeugnissen, die indirekt Gesundheitsdaten darstellen, dürfte dies allgemein anerkannt sein; bei schriftlichen Verwarnungen ist die Aufbewahrungsdauer idealerweise in der Verwarnung selbst festgehalten. Es ist zu vermeiden, dass nach Jahren auf ein nicht konformes Verhalten verwiesen wird. Es kann nicht Jahre später darauf bezugnehmend gekündigt werden. Darum sollten solche Unterlagen zeitnah vernichtet werden.

Wird im Zusammenhang mit einer gesundheitlichen Einschränkung ein Case Management durchgeführt, sind solche CM-Unterlagen zwingend separat vom Personaldossier aufzubewahren. Auch sind solche Daten zeitnah, nach Abschluss des Case Managements, zu vernichten. Die Stadt Zürich hat den Umgang mit Case-Management-Unterlagen klar geregelt in der Personalverordnung u.a. in Art. 55bis Personalrechtverordnung inkl. einer Aufbewahrungsfrist von zwei Jahren nach Fallabschluss.[9]

Bei allen Unterlagen im Personaldossier sollte beachtet werden, dass betroffene Personen via Auskunftsrecht das Anrecht auf eine Kopie haben. Entsprechend sollten allfällige Notizen sorgfältig formuliert werden; ein Schattendossier zu führen, ist nicht rechtmässig.

Lohndaten sowie allfällige Bonuszahlungen sind zehn Jahre aufzubewahren. Dabei handelt es sich um Daten, die geschäftsbuchrelevant sind im Sinne von Art. 2 GeBüV,[10] und diese müssen gemäss Art. 958f OR während zehn Jahren aufbewahrt werden.

Im Sinne der Verhältnismässigkeit ist nicht nur die Aufbewahrungsdauer, sondern auch die Anzahl der zugriffsberechtigten Personen zu prüfen. Zu Lohndaten, obwohl gemäss Definition des Datenschutzgesetzes nicht besonders schützenswert, wird regelmässig nur einem sehr eingeschränkten Kreis Zugriffsrechte gegeben. Bei Personaldossiers – gemäss heutiger Gesetzgebung ein Persönlichkeitsprofil, das analog zu besonders schützenswerten Daten zu bearbeiten ist – werden die Zugriffsrechte oft weniger strikt gehandhabt. Insbesondere besteht immer wieder der Wunsch der Linie, auch über mehrere Stufen hinweg Zugriff zu haben; hier ist die Verhältnismässigkeit kritisch zu hinterfragen. Braucht es den Zugriff wirklich?

Nach Beendigung

Endet das Arbeitsverhältnis, muss über die gesamte Anstellungsdauer ein Arbeitszeugnis erstellt werden. Dazu ist es notwendig, dass man eine Übersicht hat, was die betroffene Person geleistet hat. Idealerweise existieren bei langjährigen Arbeitsverhältnissen verschiedene Zwischenzeugnisse, die auch aufbewahrt worden sind und als Grundlage für das Schlusszeugnis dienen können.

Solche Zwischenzeugnisse sollten vor Erstellung des Schlusszeugnisses nicht vernichtet – jedoch nach Erstellung des Schlusszeugnisses, sofern es nicht zu einer arbeitsrechtlichen Auseinandersetzung kommt, vernichtet werden. Mit dem Austritt sollte nun spätestens das Personaldossier durchkämmt werden, welche Daten weiterhin aufzubewahren sind.

Grundsätzlich können Forderungen aus dem Arbeitsvertrag während fünf Jahren geltend gemacht werden (Art. 128 Ziff. 3 OR) – das bezieht sich beispielsweise auf Forderungen bezüglich Ferien,[11] Überstunden oder auch Ersatz von Spesen und Auslagen;[12] bei Arbeitszeugnissen besteht jedoch eine Verjährungsfrist von zehn Jahren, wie auch das Bundesgericht in einem Urteil vom 28. Dezember 2020 festgehalten hat.[13]

Am besten wird das Personaldossier aufgeteilt in zwei Teile: Ein Teil ist nach fünf Jahren definitiv zu vernichten, der andere Teil nach zehn Jahren. In der heutigen Zeit, in der viele Daten elektronisch aufbewahrt werden, sollte es einfacher sein, eine Löschung fast auf den Tag genau zu definieren/programmieren.

Exkurs elektronisches Personaldossier

Elektronische Personaldossiers haben viele Vorteile: Mitarbeitende haben jederzeit Zugriff auf das eigene Dossier, ein Dossier kann einfach aktuell gehalten werden, und Mitarbeitende selbst können Inhalte korrigieren. Die Zugriffsberechtigungen können durch klare Rollen vergeben werden – sofern die Rollen aktuell sind, ist damit sichergestellt, dass die Verhältnismässigkeit eingehalten wird. Zusätzlich sollte eine Nachvollziehbarkeit der Zugriffe gesichert sein. Doch wie bei allen Systemen muss ein Augenmerk auf die Datensicherheit gerichtet werden. Das schwächste Glied ist meist der Mensch und nicht die Technik, sofern das System/Programm eine datenschutzfreundliche Voreinstellung hat und über eine datenschutzfreundliche Technik verfügt (vgl. Art. 7 nDSG). Bevor ein System eingeführt wird, muss dieses zwingend auf die Datenschutzvereinbarkeit geprüft werden.

Fazit/Zusammenfassung

Beim Personaldossier ist darauf zu achten, dass nicht zu viele Daten gesammelt und aufbewahrt werden. Sofern die Unterlagen nicht in einem elektronischen Personaldossier mit zum Voraus bestimmter Aufbewahrungsdauer liegen, ist das Dossier periodisch, mindestens alle zwei Jahre, zu durchforsten und nicht mehr benötigte Daten zu vernichten. Im Rahmen der Revision des Datenschutzgesetzes müssen im Verzeichnis der Bearbeitungstätigkeiten die Aufbewahrungsdauer oder die Kriterien für diese festgelegt sein (Art. 12 Abs. 2 lit. e nDSG), dabei ist auch der Grundsatz der schnellstmöglichen Vernichtung zu berücksichtigen (Art. 6 Abs. 4 nDSG).

FUSSNOTEN

1 https://www.20min.ch/story/bei-diesem-spital-kannst-du-dich-per-whatsapp-bewerben-400622820622 – Abruf am 14. November 2021.
2 EDÖB: Leitfaden über die Bearbeitung von Personendaten im Arbeitsbereich, S. 8.
3 Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind. Im Übrigen gelten die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz.
4 Vgl. Auch www.edoeb.admin.ch/edoeb/de/home/dokumentation/taetigkeitsberichte/aeltere-berichte/9--taetigkeitsbericht-2001-2002/aufbewahrung-des-personaldossiers.html.
5 EDÖB, Leitfaden, S. 12.
6 Ihre Bearbeitung (Peraonendaten) hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
7 Sie (Personendaten) werden vernichtet oder anonymisiert, sobald sie zum Zweck der Bearbeitung nicht mehr erforderlich sind.
8 Vgl. auch Art. 23 Abs. 3 Verordnung über den Schutz von Personendaten des Bundes.
9 Verordnung über das Arbeitsverhältnis des städtischen Personals und Ausführungsbestimmungen – 177.100/177.101 Stadt Zürich.
10 SR 221.431 Verordnung über die Führung und Aufbewahrung der Geschäftsbücher (GeBüV).
11 BGE 136 III 94.
12 ZH: JAR 1990, S. 130: 5 Jahre; VD: JAR 2010, S. 650 ff.: 10 Jahre; neuerer Entscheid VS wieder 5 Jahre (www.arbeitsrecht-aktuell.ch/de/2020/02/11/verjaehrung-von-spesen-und-auslagen/ Abruf 21. November 2021; kein BGE).
13 BGer 4A_295/2020 vom 28. Dezember 2020.

AUTORIN

Ursula Uttinger ist Juristin und beschäftigt sich seit über 25 Jahren insbesondere mit dem Thema Datenschutz. Sie hat mehrere Jahre als Datenschutzbeauftragte gearbeitet, hat als leitende Auditorin Datenschutz-Audits durchgeführt und Datenschutzmanagementsysteme eingeführt. Aktuell ist sie Dozentin für Datenschutz an der Hochschule Luzern, arbeitet als Leiterin Legal & Compliance in einem Spital und publiziert regelmässig zu Datenschutzthemen.