

Vom korrekten Umgang mit Mitarbeiterdaten

Persönlichkeits- und Datenschutz am Arbeitsplatz betrifft alle Arbeitnehmenden. Welche Mitarbeiterdaten darf der Arbeitgeber bearbeiten? Wann ist eine Überwachung der Angestellten zulässig und wer genau hat eigentlich Zugriff auf die Bewerbungsunterlagen? Die wichtigsten Fakten.



Nicolas Facincani, lic. iur. LL.M., ist als Rechtsanwalt in Zürich tätig und berät Unternehmen und Private vorwiegend in wirtschafts- und arbeitsrechtlichen Belangen.
www.citylaw.ch

Reto Sutter, Dr. iur. LL.M., ist Rechtsanwalt und dipl. Steuerexperte. Er berät Unternehmen und Private vorwiegend in wirtschafts- und arbeitsrechtlichen Belangen.
www.umbricht.ch

hrtoday.ch

Weitere Fachbeiträge zum Thema finden Sie auf unserer Website.

Gemäss dem Schweizer Arbeitsrecht hat der Arbeitgeber die Persönlichkeit des Arbeitnehmers zu schützen und zu achten. Er darf nicht in dessen Persönlichkeit eingreifen, sofern solche Eingriffe nicht durch den Arbeitsvertrag gerechtfertigt sind. Zudem muss er solche Eingriffe abwehren.

Arbeitsverhältnisse und deren Anbahnung führen jedoch häufig zu einer langwierigen und umfangreichen Bewirtschaftung der Personendaten von Arbeitnehmenden. Diese beginnt bereits schon mit der Entgegennahme der Bewerbungsunterlagen und findet in der Regel erst lange nach der Beendigung des Arbeitsverhältnisses ihren Abschluss. Die Herrschaft über die persönlichen Daten ist aber ein Grundrecht – auch am Arbeitsplatz.

Datenbearbeitung ohne Fehl und Tadel

Der Arbeitgeber darf Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrages erforderlich sind. Zusätzlich gelten für den Arbeitgeber auch die Bestimmungen des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG). Es wird kein bestehendes Arbeitsverhältnis vorausgesetzt, weshalb die entsprechenden (Sorgfalts-) Pflichten im Umgang mit Personendaten den Arbeitgeber auch gegenüber einem Stellenbewerber treffen.

Neben den arbeitsrechtlichen sind auch die Grundsätze des DSG bei der Bearbeitung von Mitarbeiterdaten zu beachten. Abweichungen davon sind nur ausnahmsweise, unter Berufung auf einen speziellen Rechtfertigungsgrund, erlaubt. Daten dürfen nicht durch illegale Mittel erhoben werden. Ihre Beschaffung muss nach Treu und Glauben erfolgen. Das heisst, die Beschaffung von Personendaten und der Zweck ihrer Bearbeitung müssen für die betroffene Person erkennbar sein.

Der Grundsatz der Verhältnismässigkeit muss ebenfalls eingehalten werden. Demnach dürfen so viele Daten wie nötig, aber nur so wenige wie möglich bearbeitet werden.

Weiter dürfen nur richtige Daten (unrichtige Daten sind zu löschen) und diese nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde (Zweckbindung).

Zutritt für Unbefugte verboten

Schliesslich verlangt das DSG auch, dass Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Dies bedeutet zum Beispiel, dass nur berechtigte Personen auf eine Datenbank Zugriff haben dürfen. Ein maximaler Schutz ist nicht

erforderlich. Die Schutzmassnahmen müssen nur angemessen, das heisst im Hinblick auf die Risiken einer Verletzung des Datenschutzgesetzes geeignet, erforderlich und zumutbar sein. Dabei kommt es auf die Umstände des konkreten Einzelfalls an.

Ob die getroffenen technischen und organisatorischen Massnahmen angemessen sind, muss in ihrer Gesamtheit beurteilt werden. Eine generelle Verschlüsselung besonders schützenswerter Daten ist etwa dann nicht nötig, wenn ein hinreichender Schutz anders erreicht werden kann.

Was geschieht mit den Bewerbungsunterlagen?

Generell gilt: Die Bewerbung, deren Inhalt und die im Zusammenhang damit erhaltenen Daten darf der potenzielle Arbeitgeber nicht bekanntgeben.

Der Zugang zum Bewerbungsdossier ist auf eine «need to know»-Basis zu limitieren, wobei die anvisierte Stelle und Stellung des Bewerbers zu berücksichtigen sind. Das «Streuen» der Daten an verschiedene Mitarbeiter, etwa um die Teameignung eines Bewerbers abzuklären, verstösst in der Regel hiergegen.

Kommt es nicht zu einem Arbeitsverhältnis, muss der Arbeitgeber dem Bewerber dessen eingereichte Unterlagen umgehend zurückgeben. Weitere Unterlagen, Gesprächsnotizen, Fragebögen, Gutachten etc. müssen vernichtet oder dem Bewerber überlassen werden. Braucht der Arbeitgeber Daten noch zur Erfüllung von Pflichten oder Wahrnehmung von Rechten, kann er sie hierzu noch verwenden.

Das Bewerbungsgespräch, namentlich die Befragung durch den Arbeitgeber beziehungsweise durch die Einstellungsverantwortliche, gilt als Datenbeschaffung. Demnach darf der Arbeitgeber nur Informationen nachfragen, mit denen er die Eignung des Bewerbers für die entsprechende Stelle abklären kann. Zusätzlich sind hier die Schranken des Gleichstellungsgesetzes zu beachten; es dürfen grundsätzlich keine Fragen gestellt werden, welche ein Geschlecht diskriminieren (etwa zu Schwangerschaft, Militärdienst oder Ähnlichem). Ob eine Frage zulässig ist, kann nur im Einzelfall und unter Würdigung der gesamten Umstände des potenziellen Arbeitsverhältnisses beantwortet werden. Referenzauskünfte und grafologische Gutachten dürfen nur nach vorgängiger Zustimmung eingeholt werden.

Überwachung mit Vorankündigung

Während des Arbeitsverhältnisses kann der Arbeitgeber Überwachungsmassnahmen treffen. Diese müssen aber generell zur Abklärung der Eignung des Arbeitnehmers für das Arbeitsverhältnis dienen oder zur Durchführung des Arbeitsvertrages erforderlich sein. Zudem müssen sie verhältnismässig und transparent sein.

Verhältnismässigkeit verlangt insbesondere, dass Überwachungsmassnahmen nur soweit gehen, als sie dem vorbestimmten Zweck dienen und dass der Zweck nicht auf anderen Wegen mit mildereren Mitteln erreicht werden kann. Transpa-

renz bedeutet, dass der Arbeitnehmer – mindestens in allgemeiner Form – vorgängig über die Kontrolle informiert wird; hier empfiehlt sich allenfalls ein Überwachungsreglement. Dass Überwachungsmaßnahmen nicht gegen geltendes Recht verstossen dürfen, versteht sich von selbst.

Daneben muss bei Überwachungsmaßnahmen zusätzlich Art. 26 der Verordnung 3 zum Arbeitsgesetz berücksichtigt werden. Demgemäss dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden. Erlaubt ist der Einsatz solcher Systeme grundsätzlich nur aus Sicherheitsgründen und zur Erfassung der Arbeitsleistung und nur sofern Art. 328b OR und das Datenschutzgesetz beachtet werden.

Werden Überwachungsmaßnahmen durch Dritte, etwa wenn der IT-Bereich ausgelagert worden ist, ausgeführt, muss zusätzlich gesondert geprüft werden, ob die Auslagerung der Massnahmen zulässig ist. Ob im speziellen Einzelfall eine Überwachungsmaßnahme zulässig ist, muss anhand des konkreten Falles beurteilt werden.

Der Chef liest, hört und sieht mit

Als Richtmass können die nachfolgenden Grundsätze herangezogen werden:

Unbefugtes Lesen von privaten E-Mails ohne besondere Rechtfertigungsgründe ist verboten, während das Lesen von geschäftlichen E-Mails als im Grundsatz zulässig erachtet wird, sofern die nötige Transparenz gewährleistet ist. In der Regel zielen die Überwachungsmaßnahmen jedoch nicht auf den Inhalt der E-Mails ab. Stattdessen werden Logdaten (Zeitpunkt des Versands oder Empfangs, Adressat und Absender etc.) gesammelt.

Nicht anonymisierte Überwachung von Logdaten von E-Mail- und Internetverhalten (Randdatenerfassung) von Arbeitnehmern darf nicht der Verhaltensüberwachung des Arbeitnehmers



Foto: 123RF

dienen und muss Art. 328b OR und dem DSGVO entsprechen. Sie ist zudem, wie alle Überwachungsmaßnahmen, nur zulässig, wenn der gleiche Zweck nicht mit einem milderen Mittel erreicht werden kann.

Die Installierung von «Compliance Software», welche zum Beispiel versandte E-Mails von Arbeitnehmern nach Versandadresse oder deren Browser-Protokolle nach angerufener Site klassifizieren, oder von «Spyware» ist grundsätzlich unzulässig.

Die Überwachung des Inhalts von Telefongesprächen ist grundsätzlich nur möglich, wenn alle Beteiligten einverstanden sind. Dies ergibt sich neben dem Datenschutzrecht auch bereits aus dem Strafrecht.

Sollen «nur» Randdaten (Dauer, Zeitpunkt, Gebühren, gewählter Anschluss) erfasst werden, ist das unter den oben erwähnten Einschränkungen zulässig. Als Zweck kann hier zum Beispiel dienen, dass Weisungen über den privaten Telefonverkehr kontrolliert werden müssen.

Bei der Videoüberwachung ist im besonderen Masse das Augenmerk auf das Verbot der Ver-

haltensüberwachung zu legen. Sie darf aber namentlich aus Sicherheitsüberlegungen eingesetzt werden.

Denkbar ist auch eine gezielte Überwachung des Arbeitnehmers im Zusammenhang mit einer Straftat, wenn die Massnahme nach Einreichung einer Anzeige richterlich oder gerichtspolizeilich angeordnet wurde. Ansonsten ist der Einsatz einer Videokamera möglich, wenn der Verdacht auf eine Straftat besteht und die Mitarbeiter im Vorfeld über die zeitlich beschränkte Überwachung informiert werden. Ob auf die vorherige Information verzichtet werden kann, muss im Einzelfall geprüft werden.

Fazit

Die Pflicht zum Datenschutz von Mitarbeiterdaten beginnt bereits mit der Bewerbung. Die Bewerbung und deren Inhalt dürfen nur einem auf der Stellung des Bewerbers basierenden Personenkreis bekannt gegeben werden und die Daten müssen vor unbefugtem Zugriff geschützt werden. Das gilt namentlich auch bei elektronischer Erfassung von Bewerbungen.

Überwachungsmaßnahmen im Rahmen von Arbeitsverhältnissen sind unter bestimmten Voraussetzungen möglich, wobei der Persönlichkeitsschutz der Mitarbeiter als Richtschnur gelten kann. Einzelne Massnahmen müssen gesondert unter Berücksichtigung sämtlicher Umstände geprüft werden. Sollen generelle Massnahmen implementiert werden (etwa Logdatenerfassung von E-Mail-Verkehr), empfiehlt es sich, diese mit entsprechenden Verhaltensanweisungen zu kombinieren und die Information der Mitarbeiter gut vorzubereiten.

Transparente und zeitnahe Kommunikation dazu bildet ein Fundament für gegenseitiges Vertrauen. Und gute Arbeit wird in einem Unternehmen vor allem dann geleistet, wenn zwischen Arbeitgeber und Arbeitnehmer ein Vertrauensverhältnis gegeben ist. ■

Nicolas Facincani, Reto Sutter