Beschäftigtendatenschutz vor dem Hintergrund der Datenschutzgrundverordnung (DSGVO)

Täglich verarbeiten Personalabteilungen eine Vielzahl von Beschäftigtendaten, von den Personalstamm- inklusive Gehaltsdaten über Daten der Zeiterfassung bis hin zu im Rahmen eines Betrieblichen Eingliederungsmanagements erhobenen Gesundheitsdaten. Die Datenverarbeitung ist dabei nicht auf das laufende Arbeitsverhältnis beschränkt; vielmehr beginnt sie bereits mit der Bewerbung und endet auch mit der Beendigung des Arbeitsverhältnisses nicht. Insbesondere vor dem Hintergrund der hohen Bußgelder, die bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes betragen können, müssen Personalabteilungen sich also spätestens jetzt dringend fragen, wie sich die Datenschutzgrundverordnung (DSGVO), ergänzt um das neue BDSG (BDSG nF), die beide ab dem 25.05.2018 gelten, auf die Verarbeitung personenbezogener Daten der Beschäftigten auswirkt.
Der schon nach dem „alten" Datenschutzrecht maßgebliche Grundsatz, wonach jeglicher Umgang mit personenbezogenen Mitarbeiterdaten grundsätzlich unzulässig ist, es sei denn ein Gesetz, eine Betriebsvereinbarung bzw. ein Tarifvertrag erlauben es oder der Arbeitnehmer hat in die Datenverarbeitung eingewilligt (sog. Verbot mit Erlaubnisvorbehalt), gilt auch unter der DSGVO und dem BDSG nF.

Die zentrale Regelung im Beschäftigtendatenschutz ist § 26 BDSG nF (bislang § 32 BDSG), der bestimmt, dass die Datenverarbeitung zulässig ist, soweit sie zur Entscheidung über die Begründung eines Arbeitsverhältnisses, der Durchführung oder Beendigung eines Arbeitsverhältnisses, der Erfüllung der sich aus einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten sowie der Aufdeckung von Straftaten bei bestehendem Tatverdacht erforderlich ist.

Bewerbungsverfahren

Dementsprechend darf der Arbeitgeber einen Bewerber weiterhin nach Namen, Adresse und E-Mail-Adresse sowie den fachlichen Kenntnissen, der Ausbildung und dem beruflichen Werdegang fragen. Wie bislang ist es auch unter der DSGVO dagegen grundsätzlich nicht zulässig, nach der Schwerbehinderung, der Religions- oder Gewerkschaftszugehörigkeit oder einer Schwangerschaft zu fragen.

Problematisch ist ebenfalls die Erhebung von Daten des Bewerbers über „Google" oder soziale Netzwerke, wie beispielsweise xing oder facebook; denn soweit hier überhaupt berufsbezogene Daten erhoben werden – das Privatleben des Arbeitnehmers ist für den Arbeitgeber weiterhin tabu –, hätte der Arbeitgeber strenge Informationspflichten gemäß Art. 14 DSGVO gegenüber dem Bewerber zu beachten. So müsste er ihm beispielsweise die Kontaktdaten des Verantwortlichen und des Datenschutzbeauftragten ebenso mitteilen wie die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, und die Rechtsgrundlage für die Verarbeitung und die Dauer der Speicherung der Daten. Aus diesem Grund sollte also von dieser Art der Beschaffung von „Zusatzinformationen" über die Bewerber Abstand genommen werden.

Die aufgezählten Mitteilungspflichten gelten aber auch dann bereits in der Bewerbungsphase, wenn die Daten vom Bewerber selbst erhoben werden (Art. 13 DSGVO), soweit er nicht bereits über die Informationen verfügt. Deshalb ist es zukünftig angeraten, den Bewerbern mit der Eingangsbestätigung ihrer Unterlagen die nach Art. 13 DSGVO erforderlichen Informationen, wie insbesondere die Kontaktdaten des Datenschutzbeauftragten und die Speicherdauer mitzuteilen.

Unter der DSGVO wird es vor dem Hintergrund der drohenden empfindlichen Bußgelder noch wichtiger als bisher sein, den Grundsatz der Datensparsamkeit einzuhalten. So muss die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Maß beschränkt werden. Unterlagen abgelehnter Bewerber müssen also innerhalb einer angemessenen Frist gelöscht werden. Sollen die Daten in einen Bewerberpool für zukünftig zu besetzende Stellen aufgenommen werden, muss der Bewerber ausdrücklich zustimmen, wobei auch hier keine unbegrenzte Speicherung erfolgen darf und die konkrete Dauer dem Bewerber vor dessen Zustimmung mitgeteilt werden muss.

Arbeitsverhältnis

Weiterhin zulässig bleibt natürlich die Datenerhebung zur Zeiterfassung und Gehaltsabrechnung. Auch können beispielsweise im Rahmen eines betrieblichen Eingliederungsmanagements gesundheitsbezogene Daten erhoben und – getrennt von der eigentlichen Personalakte und besonders gesichert – aufbewahrt werden. Wichtig ist hier ebenfalls die neue Pflicht zum Hinweis auf die Dauer der Speicherung der Daten.

Zur Datenverarbeitung gehört es aber auch, wenn Mitarbeiterdaten, wie beispielsweise Name, Telefonnummer und E-Mail-Adresse, auf der Homepage des Arbeitgebers veröffentlicht werden sollen, um die Kontaktaufnahme durch Kunden und sonstige Geschäftspartner zu erleichtern. Hier muss zwischen sog. „Funktionsträgern" und „Nichtfunktionsträgern" unterschieden werden. Die Gruppe der Funktionsträger umfasst dabei alle offiziellen Ansprechpartner eines Unternehmens, zum Beispiel Kundenbetreuer, Geschäftsführer oder Niederlassungsleiter. Daten, die zwingend zur Kontaktaufnahme erforderlich sind, also Name, Tätigkeitsbereich, Telefonnummer und E-Mail-Adresse dürfen grundsätzlich auch weiterhin ohne ausdrückliche Einwilligung des Arbeitnehmers veröffentlicht werden. Handelt es sich dagegen um „Nichtfunktionsträger", wie beispielsweise eine reine Schreibkraft, oder sollen weitere Daten des Funktionsträgers veröffentlicht werden, wie Geburtsdatum, beruflicher Werdegang oder eine Fotografie, bedarf es der ausdrücklichen – vorherigen – Einwilligung des Arbeitnehmers.

Die Einwilligung in die Datenverarbeitung, die sich bislang in § 4 a BDSG fand, ist nun in Art. 7 DSGVO und § 26 Abs. (2) BDSG nF geregelt. Sie bedarf grundsätzlich der Schriftform – bei Vorliegen besonderer Umstände soll zwar eine weniger strenge Form möglich sein, was sich jedoch schon aus Beweisgründen nicht anbietet. Weiter erfordert eine wirksame Einwilligungserklärung Freiwilligkeit, weshalb die Einwilligung keinesfalls mehr mit dem Arbeitsvertrag verbunden oder gar in diesem enthalten sein darf; denn diese Koppelung trifft der Anschein der Unfreiwilligkeit. Daneben muss der Zweck der Verarbeitung und Nutzung konkret benannt werden (Bsp.: „Die Fotos werden zum Zweck der Außendarstellung des Unternehmens auf der Webseite www.unternehmen.de und auf den Social Media Kanälen (facebook, twitter, instagram) veröffentlicht."). Auch hat eine Belehrung über ein jederzeitiges Widerrufsrecht zu erfolgen. Abzuwarten bleibt dabei, ob der einzelne Mitarbeiter dieses – wie bislang vom BAG entschieden (Urteil v. 19.02.2015 – 8 AZR 1011/13)– nur bei Vorliegen eines plausiblen Grundes ausüben kann oder ob sich die Rechtsprechung unter der DSGVO und dem BDSG nF ändert. Bereits von den Mitarbeitern eingeholte Einwilligungen sollten ebenfalls insoweit auf ihre Vereinbarkeit mit dem neuen Datenschutzrecht überprüft werden.

Infolge der nun drastisch verschärften Strafen bei Datenschutzverstößen ist es noch dringender angeraten, die Nutzung der Kommunikationsmittel, wie insbesondere E-Mail, zu privaten Zwecken zu untersagen; denn datenschutzrechtliche Probleme bestehen spätestens, wenn der Mitarbeiter kurzfristig erkrankt und der Arbeitgeber oder Kollegen Zugriff auf E-Mails des erkrankten Mitarbeiters benötigen. Ist die Privatnutzung erlaubt, darf der Arbeitgeber in derartigen Fällen nur dann auf das E-Mail-Postfach des erkrankten Mitarbeiters zugreifen, wenn der Mitarbeiter ausdrücklich hierin eingewilligt hat und der Zugriff für betriebliche Zwecke erforderlich ist, so bereits die bisherige Ansicht der Datenschutzaufsichtsbehörden des Bundes und der Länder. Besteht im Unternehmen zur Nutzung firmenbezogener Kommunikationsmittel bereits eine Betriebsvereinbarung, kann diese zwar wirksame datenschutzrechtliche Regelungen enthalten. Ob die getroffenen Vereinbarungen aber auch mit dem neuen Datenschutzrecht vereinbar sind, sollte zwingend vor dem 25.05.2018 geprüft und gegebenenfalls neue Betriebsvereinbarungen abgeschlossen werden.

Was aber kann konkret unternommen werden, wenn der Mitarbeiter beispielsweise in Verdacht steht, Produktionsmittel zu stehlen oder seine Arbeitszeit mit Surfen im Internet zu verbringen?

Nach aktueller Entscheidung des BAG vom 27.07.2017 (Az.: 2 AZR 681/16) dürfen jedenfalls keine sog. „Keylogger" (dt. „Tasten-Protokollierer") eingesetzt werden, ohne dass der konkrete Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung besteht. Derartige anlasslose Überwachungen können sogar einen Schmerzensgeldanspruch des unzulässig überwachten Arbeitnehmers begründen (BAG, Urteil v. 19.10.2015 – 8 AZR 1007/13). Die auf diese Weise erlangten Beweise sind zudem – so das BAG – im Prozess nicht verwertbar.

Soll überprüft werden, ob die Mitarbeiter sich tatsächlich an das ausdrückliche Verbot privater Internetnutzung halten, müssen die Mitarbeiter nach einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte (Urteil v. 05.09.2017 - 61496/08) vor der Überprüfung zudem über die Möglichkeit, die Art und das Ausmaß der Kontrolle unterrichtet werden.

Besteht dagegen aber ein konkreter Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung, war die heimliche Mitarbeiterüberwachung bislang sogar in Form eines Detektiveinsatzes oder einer Videoüberwachung grundsätzlich zulässig, soweit keine weniger einschneidenden Mittel zur Verfügung stehen, den Mitarbeiter zu überführen (vgl. BAG, Urteil v. 29.06.2017 – 2 AZR 597/16). Ob diese Vorgehensweise unter der DSGVO weiterhin zulässig bleibt, ist noch unklar, nachdem die strengen Informationspflichten der Art. 13, 14 DSGVO nach ihrem Wortlaut auch hier gelten. Der Arbeitnehmer müsste also vom Arbeitgeber beispielsweise vor der Erhebung von Bilddaten im Rahmen einer verdeckten Videoüberwachung über diese Maßnahme aufgeklärt werden, wodurch natürlich der Sinn der verdeckten Kontrolle leer liefe. Ein Ausschluss heimlicher Datenverarbeitung würde aber unweigerlich zu einem weitestgehenden Verbot verdeckter Arbeitnehmerkontrollen führen, was – so die bisher vorherrschende Meinung in der Literatur – nicht sein darf. Deshalb soll die Datenerhebung im Rahmen der heimlichen Mitarbeiterüberwachung also weiterhin zulässig bleiben. Aufgrund der drohenden enorm hohen Bußgelder sollten Arbeitgeber jedoch bis zu einer gerichtlichen Klärung der Frage mit dem Einsatz heimlicher Kontrollen zurückhaltend umgehen und diesen zuvor sorgfältig prüfen.

Anzumerken ist ferner, dass die Pflicht zur Datensparsamkeit auch uneingeschränkt im bestehenden Arbeitsverhältnis gilt. Im Rahmen der Löschung von Daten sind dabei die Fristen, innerhalb derer Ansprüche geltend gemacht werden können bzw. die zur Aufbewahrung für die Kontrolle durch Behörden erforderlich sind, zu beachten. So müssen beispielsweise Entgeltunterlagen mit sozialversicherungsrechtlichen Bezügen fünf Jahre, für den Jahresabschluss relevante Unterlagen sogar zehn Jahre aufbewahrt werden. Nicht vergessen werden darf hierbei, dass es auch für bereits erhobene und gespeicherte Daten keine Übergangsregelungen gibt, sodass alle im Sinne der DSGVO und des BDSG nF nicht erforderlichen Daten bis zum 25.05.2018 gelöscht sein müssen.

Ende des Arbeitsverhältnisses

Nach Beendigung des Arbeitsverhältnisses werden bestimmte Daten des ehemaligen Mitarbeiters weiterhin benötigt, um nachvertragliche Ansprüche, wie beispielsweise in Form der betrieblichen Altersversorgung, zu erfüllen. Ausschließlich die zur Erfüllung des Anspruchs erforderlichen Daten – und damit nicht alle in der Personalakte gesammelten Daten – dürfen hierfür gespeichert werden, wobei die Verarbeitung eingeschränkt werden sollte. Werden die Daten dagegen weder zur Abwicklung des Arbeitsverhältnisses noch eines nachvertraglichen Anspruchs benötigt, sind sie mit Ablauf der insoweit zu beachtenden Aufbewahrungsfristen zu löschen.
Arbeitnehmer haben also ein „Recht auf Vergessenwerden" und können die Datenlöschung gemäß Art. 17 DSGVO auch aktiv verlangen.
Für das Löschen elektronischer Daten genügt es dabei nicht, die Daten lediglich in den „Papierkorb" zu schieben und diesen zu leeren; vielmehr müssen die Daten mit Zufallsdaten so überschrieben werden, dass eine Wiederherstellung auch mit Hilfe von speziellen IT-Kenntnissen nicht oder jedenfalls nur schwer möglich ist.

Alle Maßnahmen zur Beachtung des Datenschutzes von der Bewerberphase bis zur Beendigung des Arbeitsverhältnisses sind zudem (datenschutzkonform) zu dokumentieren, da die Einhaltung der datenschutzrechtlichen Vorschriften im Streitfall bewiesen werden muss, eine ebenfalls wesentliche Neuerung, die die DSGVO bereithält.

Fazit

Die neue DSGVO, ergänzt um das BDSG nF, wird für Arbeitgeber einen Einschnitt darstellen. Der bisherige Umgang mit Bewerber- sowie Arbeitnehmerdaten muss grundlegend überdacht und überarbeitet werden, insbesondere in Bezug auf den einzuhaltenden Grundsatz der Datensparsamkeit. Das vollständige Ausmaß der Änderungen und der Herausforderungen ist zum jetzigen Zeitpunkt noch nicht absehbar, vielmehr müssen die Leitlinien, die die Rechtsprechung in den nächsten Jahren entwickeln wird, im Blick behalten werden.

Autorin:
Katharina Haslach
Rechtsanwältin
Telefon: 07121 38361-15
Telefax: 07121 38361-99
E-Mail: haslach@slp-anwaltskanzlei.de