



Michael Wilmsen

Rechtsanwalt

UNTERNEHMERKANZLEI

RECHT & STEUERN

Erich-Zeigner-Allee 69-73 . 04229 Leipzig

Tel. 0341 / 4774728 . Fax 0341 / 4772547 . E-Mail: kanzlei@ra-wilmsen.net

www.unternehmerkanzlei.net

24.04.2018 1/2

Beschäftigtendatenschutz

- Teil 2 -

Am 25.05.2018 wird erstmals in Europa ein einheitlicher Datenschutz eingeführt. Dann startete die EU-Datenschutz-Grundverordnung (DS-GVO). Deren Vorgaben zum Beschäftigtendatenschutz hat Deutschland im neuen § 26 BDSG konkretisiert:

III. Beschäftigtendatenschutz bei der Anbahnung

Nach § 26 BDSG gelten auch Bewerber als Beschäftigte. Damit sind deren Daten genauso schutzbedürftig wie die der beschäftigten Arbeitnehmer.

Personenbezogene Daten dürfen nur insoweit verarbeitet werden, als dies für die Entscheidung über die Einstellung eines Bewerbers oder zur Durchführung, Ausübung oder Beendigung eines Arbeitsverhältnisses erforderlich ist.

1. Bewerbungsunterlagen enthalten personenbezogene Daten. Der Arbeitgeber sollte den Kreis derer, die die Bewerbungsdaten erhalten, möglichst klein halten. Das heißt maximal der Personalleiter und der direkte Fachvorgesetzte der Stelle sollten involviert werden bzw. bei kleineren Unternehmen der Geschäftsführer/Inhaber selbst. Die Bewerbung intern beliebig weiterzuleiten, ist keine gute Idee. Die Gefahr, die Grundsätze der Vertraulichkeit und der Speicherbegrenzung zu verletzen, ist dabei sehr hoch.

Ist das Bewerbungsverfahren für die besagte Stelle beendet, müssen die Daten der abgelehnten Bewerber zurückgeschickt, gelöscht oder vernichtet werden. Hier greifen die Grundsätze Zweckbindung, Datenminderung und Speicherbegrenzung ein, schließlich ist die Nutzung der Daten jetzt überflüssig.

Die Bewerbungsunterlagen dürfen und sollten aber noch mindestens vier Monate, längstens 6 Monate gespeichert werden, um Schadensersatzansprüchen von abgelehnten Bewerbern nach dem AGG wegen angeblicher Diskriminierung entgegentreten zu können-

Von den Daten der Person, die den Job erhält dürfen nur die Daten gespeichert werden, die für die konkrete Beschäftigung erforderlich sind. Nicht erforderlich sind Anschreiben, Schul- oder Ausbildungszeugnisse, Allgemeine Praktikumsbescheinigungen, Zeugnisse. Diese Unterlagen sind zurückzugeben bzw. datenschutzgerecht zu löschen/vernichten.

2. Auch im Bewerbungsgespräch gilt es die Grundsätze der Zweckbindung und Datenminimierung einzuhalten. Alle Antworten des Bewerbers auf die Fragen des Arbeitgebers stellen personenbezogene Daten dar.

Auch hier sollten Sie die Aufzeichnungen aus AGG-Zwecken 4 bis 6 Monate aufbewahren, dann aber vernichten.

IV. Beschäftigtendatenschutz bei Beendigung des Arbeitsverhältnisses

Der Arbeitgeber darf nur die Daten für den Zweck (Arbeitsverhältnis) verarbeiten, für den sie erhoben worden sind (Zweckbindung). Und er darf sie nur solange speichern, wie sie notwendig sind (Speicherbegrenzung). Das heißt, scheidet der Arbeitnehmer aus, sind auch seine Daten zu löschen, denn der Zweck der Speicherung entfällt.

Dies gilt jedoch nicht für nach anderen Gesetzen aufbewahrungspflichtige Daten.

Nach arbeitsrechtlichen Schutzgesetzen, sozialversicherungs- und steuerrechtlichen Vorschriften ergeben sich unterschiedlich lange (teilweise bis zu 10 Jahre) Aufbewahrungsfristen.

Eng verknüpft mit der Löschung von Mitarbeiterdaten nach Beendigung des Beschäftigungsverhältnisses ist der rechtskonforme Umgang mit dem E-Mail-Account des ehemaligen Arbeitnehmers. Dazu ausführlich unter V. Spezialthemen.

Wenn der ehemalige Mitarbeiter verlangt, dass seine Daten und sein Foto im Mitarbeiterprofil der Unternehmenshomepage gelöscht werden sollen, hat der Arbeitgeber dem zu entsprechen.

Ausnahmen von der sofortigen Löschungspflicht auf Verlangen kann es im Einzelfall geben, für ausschließlich Veranschaulichungszwecken dienende Bilder ohne Individualitätsbezug des einzelnen Arbeitnehmers oder für Gruppenfotos, auf denen der Arbeitnehmer zu erkennen ist.

demnächst:

Teil 3:

V. Spezialthemen

1. Datenschutz bei der Meldung der Arbeitsunfähigkeit
2. Datenschutz bei Video- und Audioüberwachung
3. Datenschutz bei privater Email-Nutzung im Unternehmen