Minenfeld DSGVO im Personalbereich

In kaum einem anderen Unternehmensbereich sind so viele – und teils sensible – personenbezogene Daten involviert.

Gastbeitrag

••• *Von Markus Knasmüller*

Grundsätzlich ist die Datenschutzgrundverordnung (DSGVO) eine sehr sinnvolle Verordnung der EU, um Datenkraken wie Google oder Facebook in den Griff zu bekommen, was wohl auch die hohen Strafandrohungen von teilweise über 20 Mio. € erklärt. Die Strafen, die aber jetzt *alle* treffen können, werden von einem strengen Regelwerk begleitet, das viele Fragen offenlässt. Eine vollständige Umsetzung, die *alles* berücksichtigt, erscheint kaum möglich.

Checkliste zur DSGVO

Eine praxisorientierte Vorgehensweise ist sinnvoll; folgende Checkliste kann dafür herangezogen werden:

- Auch wenn ein Datenschutzbeauftragter für die meisten Unternehmen nicht nötig ist, so ist doch sinnvollerweise eine für den Datenschutz verantwortliche Person zu bestimmen. Diese benötigt die Unterstützung des *gesamten* Unternehmens und vor allem die des Top-Managements, das mit gutem Beispiel vorangehen sollte.
- Ein Verzeichnis der Verarbeitungstätigkeiten ist zu führen. Dies ist vielfach ohnehin verpflichtend, aber jedenfalls sinnvoll. Darin sollten – vereinfacht gesagt – die Programme angeführt werden, mit denen personenbezogene Daten verarbeitet werden; hier sind auch die Softwareanbieter gefragt.
- Dieses Verzeichnis muss nicht nur bei etwaigen Kontrollen der Datenschutzbehörde vorgelegt werden. Es dient vor allem dazu, *selbst* die Übersicht zu bewahren. Wo sind bessere Datensicherheitsmaßnahmen zu setzen, in welchen Systemen muss nachgesehen werden, wenn jemand Auskunft begehrt, welche Löschfristen sind wo festzulegen …

> *So wird etwa die private Facebookseite eines Bewerbers nicht berücksichtigt werden dürfen, das Xing- oder LinkedIn-Profil (…) schon.*

- Werden bei der Verarbeitung von Daten *andere* Unternehmen, sogenannte Auftragsverarbeiter, eingebunden? Beispiele dafür könnten Newsletter-Agenturen, Steuerberater oder auch IT-Dienstleister (z.B. Cloudanbieter) sein. Mit diesen müssen die Vertragsverhältnisse wahrscheinlich überarbeitet werden, um die DSGVO-Vorschriften zu erfüllen.
- Aber auch andere Verträge und insbesondere die AGBs sind wahrscheinlich zu überarbeiten.
- Alle Mitarbeiter sollten eine Verschwiegenheitserklärung unterzeichnen und sind entsprechend zu schulen.
- Werden Daten in das EU-Ausland übertragen? Derartige Datenflüsse sind nur unter gewissen Umständen zulässig und müssten genauer betrachtet werden.
- Im Internet sollte eine Informationsseite angeboten werden, die offenlegt, welche Datenkategorien über welche Personen gespeichert werden. Auf diese kann bei der Erhebung von Daten, etwa bei Online-Shops, verwiesen werden.

Fallstricke im HR-Bereich

Der HR-Bereich ist von der DSGVO-Umsetzung natürlich stark betroffen. Erst einmal sind hier unzweifelhaft jede Menge personenbezogener Daten involviert – und zweitens sind hier auch noch Daten besonderer Kategorie, häufig auch *sensible Daten* genannt, anzutreffen.

Bei Letzteren handelt es sich vor allem um Gesundheitsdaten (etwa Krankenstanddaten oder die SV-Nummer) und diese sind der DSGVO nach besonders zu schützen. Etwa kann als Rechtsgrund für deren Speicherung niemals das berechtigte Interesse angegeben werden. Es müsste sich wohl vielmehr aufgrund des Arbeitsrechts ergeben. Deshalb wäre es etwa sinnvoll, Bewerber nicht nach deren SV-Nummer zu fragen, bevor es zu einer Einstellung kommt.

Vorsicht bei Bewerbungen

Wie bereits angesprochen, spielt das Thema DSGVO auch im Bereich der Bewerbungen eine große Rolle. So wird etwa die private Facebookseite eines Bewerbers *nicht* berücksichtigt werden dürfen, das Xing- oder LinkedIn-Profil – die eher beruflichen Hintergrund haben –, schon. Bewerbungen sollten zudem sechs Monate nach einer etwaigen Absage gelöscht werden. Ausnahme: Dem Bewerber wird mitgeteilt, dass die Daten beispielsweise aus Gründen der Evidenz noch für drei Jahre aufbewahrt werden – und: Es erfolgt kein Widerspruch.

Falls ein Widerspruch erfolgt, wären die Daten aber zu löschen. Hier muss aufgepasst werden, weil anschließend eigentlich auch etwaige *interne* Mails über die Bewerbung zu löschen wären. Sinnvoll ist daher sicherlich die Verwendung eines Bewerbermanagementsystems, das derartige Punkte berücksichtigt.

© Matthias Witzany/BMD

Markus Knasmüller Abteilungsleiter für Softwareentwicklung, Prokurist bei BMD-Systemhaus, gerichtl. zert. Sachverständiger, u.a. für Datenschutz.

Das Thema Einwilligung des Betroffenen ist gerade im HR-Bereich ein interessanter Punkt. Denn: Eine Einwilligung, personenbezogene Daten verarbeiten zu dürfen, ist nur dann gültig, wenn diese Einwilligung *ausdrücklich* und *freiwillig* erfolgt. Gerade Letzteres ist aber zu bezweifeln, wenn ein klares Ungleichgewicht zwischen dem Betroffenen und Verantwortlichen vorliegt. Daher wäre eine etwaige im Dienstvertrag gegebene Einwilligung jedenfalls nichtig. Es ist daher sehr wichtig, gut zu überlegen, welche personenbezogenen Daten gespeichert