BESCHÄFTIGTENDATENSCHUTZ

Wichtige Praxishinweise für Ihre Kanzlei zum Beschäftigtendatenschutz, Teil 1

von RAin Heike Mareck, Dortmund

| Datenschutzgesetze zählen nicht zu den Schriftstücken mit hohem Unterhaltungswert. Aber gerade jetzt läuft hier der Countdown: Denn am 25.5.18 wird erstmals die europäische Datenschutz-Grundverordnung (DS-GVO) wirksam. Und die gilt neben dem neuen BDSG auch für (fast) alle Unternehmen. Ein wichtiger Teilbereich ist der Beschäftigtendatenschutz. Wie gut ist Ihre Kanzlei darauf vorbereitet? In dieser Serie erhalten Sie Tipps zur optimalen Umsetzung des Beschäftigtendatenschutzes in Ihrer Kanzlei. |

1. Ausgangslage

DS-GVO und BDSG neu treten am selben Tag in Kraft

Am 25.5.18 wird die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates unmittelbar geltendes Recht in allen EU-Mitgliedstaaten sein. Um ein reibungsloses Zusammenspiel der Verordnung mit dem deutschen Datenschutzrecht sicherzustellen, musste flankierend das bisherige deutsche BDSG überarbeitet werden. Das BDSG n.F. tritt nun ebenfalls am 25.5.18 in Kraft. Insbesondere im Beschäftigtendatenschutz hält die DS-GVO Öffnungsklauseln zugunsten des nationalen Gesetzgebers bereit. Da das BDSG n.F. einige Querverweise auf die DS-GVO enthält, gilt es zukünftig, zwei datenschutzrechtliche Normen im Auge zu behalten.

2. Regelungen zum Beschäftigtendatenschutz in der DS-GVO

Wichtige Norm in der DS-GVO: Art. 88

Die DS-GVO verfügt über keine speziellen Regelungen zum Beschäftigtendatenschutz. Vielmehr verweist sie in Art. 88 darauf, dass die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen spezifischere Vorschriften schaffen können. Art. 88 Abs. 1 DS-GVO nennt Regelungen für die Datenverarbeitung zum Zwecke

- der Einstellung,
- der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten,
- des Management, der Planung und der Organisation der Arbeit,
- der Gleichheit und Diversität am Arbeitsplatz,
- der Gesundheit und Sicherheit am Arbeitsplatz,
- des Schutzes des Eigentums der Arbeitgeber oder der Kunden,
- der Inanspruchnahme individual- oder kollektivrechtlicher Rechte und Leistungen,
- der Beendigung des Beschäftigungsverhältnisses.

Transparenz der Verarbeitung ist zukünftig noch wichtiger

Art. 88 Abs. 2 DS-GVO stellt klar, dass die nationalen Regelungen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person vorsehen. Dies gilt insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmens-

gruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz. Selbstverständlich müssen die nach DS-GVO festgelegten Informationspflichten und die Betroffenenrechte beachtet werden.

3. Regelungen zum Beschäftigtendatenschutz im BDSG n.F.

Kein eigenes Gesetz zum Beschäftigtendatenschutz

Der deutsche Gesetzgeber nahm die DS-GVO nicht zum Anlass, ein eigenes Beschäftigtendatenschutzgesetz zu schaffen. Er integrierte es kurzerhand in das BDSG n.F. So regelt § 26 BDSG n.F. ab dem 25.5.18 den Beschäftigtendatenschutz.

§ 26 Abs. 1 S. 1 BDSG n.F. knüpft hierbei an die personenbedingten Daten an. Diese dürfen von Beschäftigten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden, wenn dies für die Entscheidung

- über die Begründung eines Beschäftigungsverhältnisses,
- nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder
- zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Name, Zeugnisinhalt, Kontodaten, Religion haben eines gemeinsam: ...

Personenbedingte Daten sind nach Art. 4 Nr. 1 DS-GVO danach alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Beispiele im Rahmen des Beschäftigtenverhältnisses werden dabei sein: Name, Adresse, E-Mail-Adresse, Telefonnummer, Geburtsdatum, Kontodaten, Religions- oder Gewerkschaftszugehörigkeit, Zeugnisinhalte etc. Als Beschäftigte gelten dabei nach § 26 Abs. 8 BDSG n.F. auch Leiharbeitnehmer und Bewerber.

4. Die Rechtsgrundlagen

... Es gilt stets das Verbot mit Erlaubnisvorbehalt

Bei der Datenverarbeitung in Europa gilt das sogenannte Verbot mit Erlaubnisvorbehalt. Das bedeutet, dass jede Verarbeitung personenbezogener Daten verboten ist, außer wenn sie per Gesetz (zum Beispiel aus BDSG, Telemediengesetz-TMG, DS-GVO) oder durch eine schriftliche Einwilligung erlaubt wurde.

Nach Art. 6 DS-GVO ist die Verarbeitung nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Einwilligung,
- Zweck der Vertragserfüllung/vorvertragliche Maßnahme,
- Erfüllung einer rechtlichen Pflicht des Verantwortlichen,
- Schutz lebenswichtiger Interessen,
- Aufgaben im Bereich der öffentlichen Sicherheit,
- Wahrung berechtigter Interessen, Erforderlichkeit und Abwägung der Verhältnismäßigkeit.

Ebenso findet § 26 Abs. 1 BDSG n.F. Anwendung. Er regelt, wann Daten erhoben und verarbeitet werden dürfen. Die wichtigsten Bereiche in der Rechtsanwaltskanzlei werden dabei sein:

a) Rechtsgrundlage: § 26 Abs. 1 und 2 BDSG n.F.

Wie auch der alte § 32 Abs. 1 S. 1 BDSG erlaubt § 26 Abs. 1 S. 1 BDSG n.F. das Verarbeiten personenbezogener Daten von Beschäftigten, sofern dies für Zwecke der Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses „erforderlich" ist. Was genau ist nun „erforderlich"? Hierzu finden sich in § 26 BDSG n.F. keine weiteren Angaben. Aber in der Gesetzesbegründung: „Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen zur Herstellung praktischer Konkordanz abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten zu einem schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt." Die vom BAG (20.6.13, 2 AZR 546/12, Abruf-Nr. 196561) vorgenommene Verhältnismäßigkeitsprüfung bleibt daher gültig.

IHR PLUS IM NETZ
ak.iww.de
Abruf-Nr. 196561

Die Verwertung von Daten ist nach § 26 Abs. 1 S. 2 BDSG n.F. zulässig, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

Arbeitgeber müssen in einem solchen Fall einen angemessenen Ausgleich zwischen ihrem Aufklärungsinteresse und den Belangen des von einer Datenverarbeitung betroffenen Arbeitnehmers herstellen.

PRAXISHINWEIS | Die Bundes- und Landes-Datenschutzbeauftragten betonen in ihrem Kurzpapier Nr. 14 „Beschäftigtendatenschutz" vom 10.1.18, dass die Verarbeitung erst erfolgen darf, nachdem die Anhaltspunkte vorliegen. Die vorsorgliche Verarbeitung „auf Vorrat" ist daher unzulässig. Sie dürfen z. B. Daten nicht für den Fall erheben, dass später eine Straftat im Arbeitsverhältnis begangen werden könnte. Zudem müssen sich die Maßnahmen gegen bestimmte verdächtigte Arbeitnehmer richten, nicht gegen größere Gruppen von Beschäftigten.

Vorsorgliche Verarbeitung „auf Vorrat" bleibt unzulässig

b) Die Einwilligung als Rechtsgrundlage

Rechtsgrundlage für eine Verarbeitung personenbezogener Daten im Beschäftigtenverhältnis bleibt die Einwilligung des Arbeitnehmers nach § 26 Abs. 2 BDSD n.F. Hierauf kann nur ausnahmsweise verzichtet werden, wenn wegen besonderer Umstände eine andere Form angemessen ist.

PRAXISHINWEIS | Als Arbeitgeber müssen Sie die Einwilligung grundsätzlich schriftlich einholen, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist (§ 26 Abs. 2 S. 3 BDSG n.F.). Diese Regelung ist abweichend zur DS-GVO! Sie müssen den Beschäftigten zudem über den Zweck der Datenverarbeitung und über sein Widerrufsrecht nach Art. 7 Abs. 2 und 3 DS-GVO aufklären.

Der Arbeitsvertrag und die Einwilligung in Datenverarbeitungen sollten nicht in einem Dokument enthalten sein. Als Arbeitgeber sollten Sie darauf achten, zwei gesonderte Unterschriften einzuholen: Eine für den Arbeitsvertrag und eine für die Abgabe der Einwilligung – günstigenfalls mit einem zeitlichen Abstand.

Zwei gesonderte Unterschriften einholen

5. Besondere Informationen = besondere Einwilligung

Besondere Daten: Religiöse Ansichten, politische Meinung, Gesundheitsdaten

Besondere Kategorien personenbezogener Daten regelt § 26 Abs. 3 BDSG n.F. für Zwecke des Beschäftigtenverhältnisses. Nach Art. 9 DS-GVO sind das solche Daten, aus denen rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit hervorgehen. Darüber hinaus gilt dies für die Verarbeitung von genetischen Daten, biometrischen Daten zur Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung für Zwecke des Beschäftigungsverhältnisses.

Die Verarbeitung dieser Daten ist zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist. Zudem darf kein Grund zu der Annahme bestehen, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Bei Einwilligung gesondert hinweisen

PRAXISHINWEIS | Sofern Sie auf der Grundlage einer Einwilligung auch besondere Kategorien personenbezogener Daten verarbeiten wollen, müssen Sie im Rahmen einer Einwilligung hierauf gesondert hinweisen.

6. Datenschutz im Bewerbungsverfahren

Auch wenn es mühselig ist, schon aus Recruitinggründen sollten Rechtsanwaltskanzleien die Regelungen nach der DS-GVO und dem BDSG n.F. nicht ignorieren. Denn einerseits kann ein Verstoß empfindliche finanzielle Sanktionen nach sich ziehen. Andererseits kann ein Rechtsstreit zum Datenschutz zu einem Reputationsverlust führen – und das wiederum kann das Recruiting spürbar erschweren.

Für das Recruiting sollten Kanzleien folgende Punkte beachten:

CHECKLISTE / Recruiting

Verschlüsseltes E-Mail-Postfach für Bewerbungen

- Generell ist es empfehlenswert, wenn alle Bewerbungen einheitlich über ein verschlüsseltes E-Mail-Postfach, zum Beispiel bewerbung@ra-meier.de, einlaufen. Die Bewerbungen gehen an einem zentralen Ort ein und werden von dort gesteuert, denn Bewerbungen enthalten sensible personenbezogene Daten, die bei ungesichertem elektronischen Versand von Dritten mitgelesen werden können.

- Informieren Sie den Bewerber bei Eingang der Unterlagen über die Art der Datenerhebung (zum Verarbeitungszweck sowie zur Dauer des Aufbewahrungszeitraums) – zum Beispiel mithilfe einer automatischen Eingangsbestätigung. Art. 13 DS-GVO listet die Informationen auf, die darin enthalten sein müssen.

- Ist das Bewerbungsverfahren für die besagte Stelle beendet, müssen die Daten der abgelehnten Bewerber zurückgeschickt, gelöscht oder vernichtet werden. Hier greifen die Grundsätze Zweckbindung, Datenminimierung und Speicherbegrenzung ein, schließlich ist die Nutzung der Daten jetzt überflüssig. Da es jedoch auf der Grundlage des AGG zu Klagen seitens der Bewerber kommen kann, sollten die Kanzleien die Daten aufbewahren, solange sie mit Auseinandersetzungen abgelehnter Bewerber rechnen müssen. Die Daten sollten mindestens vier Monate, aber maximal sechs Monate vorgehalten werden (so auch das Bayerische Landesamt für Datenschutzaufsicht).

Nach beendetem Bewerberverfahren: Unterlagen noch vier Monate behalten

- Länger darf nur mit Zustimmung der jeweiligen Person gespeichert werden. Das heißt, Sie benötigen eine schriftliche Einverständniserklärung des Kandidaten.

Länger nur mit schriftlicher Einwilligung

- Nach Art. 15 DS-GVO haben Bewerber künftig das Recht, von den Unternehmen umfangreiche Auskunft über die gespeicherten Daten zu verlangen. Dokumentieren Sie daher jederzeit die Zweckgebundenheit bei der Speicherung der Daten.

- Dem ArbG ist es erlaubt, im Vorfeld auf frei zugänglichen Plattformen (zum Beispiel Xing, LinkedIn, eigene Website des Bewerbers, Quellen, die die Person in ihrer Bewerbung angegeben hat) Informationen über den Kandidaten einzuholen. Hier ist von einer Einwilligung der Person in die Datenerhebung und -verarbeitung auszugehen. Eine unzulässige Datenerhebung ist es allerdings, auf geschlossene Plattformen (eigener Benutzerzugang erforderlich) zuzugreifen. Zudem fehlt es bei diesen Plattformen (zum Beispiel Facebook, Instagram, Twitter) an einem gezielten Bezug zur beruflichen Tätigkeit.

Xing, Facebook & Co.: Welche Daten dürfen genutzt werden?

- Hinsichtlich des Fragerechts des ArbG gegenüber dem Bewerber gelten nach wie vor die Regelungen aus dem AGG. Relevant ist insofern, dass auch im Bewerbungsgespräch die Grundsätze der Zweckbindung und der Datenminimierung einzuhalten sind. Das heißt: Als Arbeitgeber dürfen Sie nur die Daten für den Zweck verarbeiten, für den sie erhoben worden sind.

- Auch wenn es für kleinere Kanzleien mühselig ist: Nehmen Sie den gesamten Bewerberprozess in einer Verfahrensdokumentation auf.

- Um sicherzustellen, dass alle Kanzlei-Mitarbeiter an einem Strang ziehen, sollten Sie ein Bewusstsein für den Datenschutz im Recruiting-Prozess schaffen. Die hausinternen Prozesse und Regelungen sollten für alle Mitarbeiter, insbesondere bei denjenigen, die mit den Personaldaten arbeiten, Verbindlichkeitscharakter haben. Kanzleien sollten ihre Mitarbeiter regelmäßig schulen und diese Maßnahmen dokumentieren.

Mitarbeiter schulen, damit alle an einem Strang ziehen

PRAXISHINWEIS | Ist der Bewerber der Ansicht, dass Sie als potenzieller Arbeitgeber gegen seinen Bewerberdatenschutz verstoßen, kann er die zuständigen Aufsichtsbehörden einschalten. Wer muss was beweisen? Die Beweislast zum Bewerberdatenschutz liegt bei Ihnen. Kommt es zu einem Rechtsstreit, zum Beispiel vor dem Arbeitsgericht, müssen Sie nachweisen, dass alle erforderlichen Maßnahmen getroffen wurden, um den Schutz der personenbezogenen Daten zu gewährleisten. Sie müssen daher die entsprechenden Sicherheitsvorkehrungen in der Kanzlei einheitlich und lückenlos dokumentieren.

Sicherheitsvorkehrungen ausreichend dokumentieren

↘ WEITERFÜHRENDER HINWEIS

- Rechtzeitig vor dem Start der Datenschutz-Grundverordnung (DS-GVO) am 25.5.18 ist die Sonderausgabe zum Beschäftigtendatenschutz unter aa.iww.de (Downloads) erhältlich

ARCHIV
Sonderausgabe unter aa.iww.de