SEC.PRO LOG

Ausgabe 1 | Oktober 2019

Inhalt:

BAG: Datenschutzrechtliche Schutzmaßnahmen unabhängig von der Stellung als eigener Verantwortlicher

Alexander Hausner

Entscheidung

Das Bundesarbeitsgericht (BAG) hat entschieden, dass eine Erfüllung betriebsverfassungsrechtlicher Auskunftsansprüche des Betriebsrates durch den Arbeitgeber nur dann zulässig sein kann, wenn der Betriebsrat die Datenschutzbestimmungen der DSGVO und des BDSG einhält (BAG, Beschlüsse v. 9.4.2019 – 1 ABR 51/17 und 7.5.2019 – 1 ABR 53/17).

Hintergrund

Im Verfahren 1 ABR 51/17 begehrte der Betriebsrat (BR) die namentliche Nennung aller Mitarbeiterinnen, die ihre Schwangerschaft dem Arbeitgeber angezeigt hatten. Im Verfahren 1 ABR 53/17 begehrte der BR Einsicht in nicht anonymisierte Bruttolohnlisten.

Der BR stützte seine Auskunftsrechte jeweils auf § 80 Abs. 2 BetrVG, wonach der BR zur Durchführung seiner Aufgaben rechtzeitig und umfassend zu unterrichten ist (Satz 1) und ihm auf Verlangen jederzeit die erforderlichen Unterlagen zur Verfügung zu stellen sind, wobei in die Bruttolohnlisten nur Einblick genommen werden kann (Satz 2).

Die Arbeitgeber lehnten die Offenlegung der gewünschten Informationen u.a. mit dem verfassungsrechtlichen Recht der Arbeitnehmer auf informationelle Selbstbestimmung ab. So hatten insbesondere Mitarbeiterinnen den Arbeitgeber explizit aufgefordert, dem Betriebsrat ihre Schwangerschaft nicht mitzuteilen.

Der entgegenstehende Wille der Beschäftigten konnte den Auskunftsanspruch nicht verhindern, da die Erfüllung des dem Betriebsrat von Gesetzes wegen zugewiesenen Überwachungsaufgabe (§ 80 Abs. 1 BetrVG) nicht von einer vorherigen Einwilligung der Arbeitnehmer abhängig ist und nach der betriebsverfassungsrechtlichen Konzeption nicht zu deren Disposition steht.

Das BAG bestätigte dann, dass eine Offenlegung von personenbezogenen, insbesondere sensiblen (Schwangerschaftsanzeige), Mitarbeiterdaten gegenüber dem Betriebsrat nicht bereits nach § 26 Abs. 6 BDSG gerechtfertigt ist. Zwar blieben nach § 26 Abs. 6 BDSG die Beteiligungsrechte des BR unberührt, allerdings enthält diese Norm, genauso wie ihre Vorgängerregelung § 32 Abs. 3 BDSG a.F., keinen eigenen Erlaubnistatbestand für eine Datenverarbeitung. Insbesondere die Verarbeitung besonderer Kategorien personenbezogener Daten sei nach § 26 Abs. 3 BDSG für Zwecke des Beschäftigungsverhältnisses nur dann zulässig, wenn sie erforderlich sei und kein Grund zur Annahme bestünde, dass das schutzwürdige Interesse des Betroffenen überwiege. Die datenschutzrechtliche Erforderlichkeit folge dabei der betriebsverfassungsrechtlichen Wertung.

Zudem aber sei nach Ansicht des BAG vom Arbeitgeber zu prüfen, ob der Empfänger angemessene Schutzmaßnahmen nach § 26 Abs. 3 Satz 3 i.V.m. § 22 Abs. 2 BDSG vorgesehen habe.

Praxishinweis

Das BAG sieht eine spezifische Schutzpflicht für den BR als Empfänger von Daten, technische sowie organisatorische Maßnahmen zum Datenschutz zu ergreifen, sobald der BR vom Arbeitgeber Auskunft über personenbezogene Daten verlangt.

Nach Art. 4 Nr. 9 DSGVO[1] ist Empfänger, wem gegenüber personenbezogene Daten i.S.d. Art. 4 Nr. 1 offengelegt werden. Offenlegung ist jede Art der Bereitstellung von Daten (Art. 4 Nr. 1). Aus Art. 4 Nr. 9 folgt, dass ein Empfänger jede „andere Stelle“ sein kann, insbesondere nicht zwingend ein Verantwortlicher nach Art. 4 Nr. 7, insbesondere „Dritter“ nach Art. 4 Nr. 10, sein muss. Das BAG musste sich daher nicht zu der nach wie vor umstrittenen Frage positionieren, ob der BR im Verhältnis zum Arbeitgeber selbst Verantwortlicher oder Teil des Verantwortlichen ist.

In beiden Verfahren stand zunächst nur die Berechtigung einer Datenbereitstellung durch die Arbeitgeber als Datenverarbeitungsvorgang in Frage, und nicht der weitere Umgang des Betriebsrates mit den Daten. Die Datenbereitstellung an einen Emp-

[1] Artikel ohne Bezeichnung sind solche der DSGVO.

fänger muss aus der Sicht des verantwortlichen Arbeitgebers zu rechtfertigen sein.

Im Fall besonderer Kategorien personenbezogener Daten i.S.d. Art. 9 konnte das BAG über § 26 Abs. 3 BDSG direkt auf die in § 22 Abs. 2 BDSG angeführten Grundsätze Bezug nehmen. Danach sind angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzunehmen. Hier hätte es jetzt ggf. nahegelegen näher zu erläutern, inwieweit der Arbeitgeber als Schutzmaßnahme die Pflicht hat sicherzustellen, dass der Empfänger der personenbezogenen Daten ein angemessenes Schutzniveau aufbieten kann. Der DSGVO ist diese Betrachtung des Empfängers schließlich nicht fremd. Art. 5 Abs. 1 lit. f) sieht als Grundsatz der Integrität und Vertraulichkeit den Schutz vor unrechtmäßiger Verarbeitung vor. Auch ist beispielsweise eine Übermittlung an einen unsicheren Drittstaat grundsätzlich unzulässig und bedarf Sicherungsmaßnahmen. Der verantwortlichen Stelle ist es also grundsätzlich zumutbar zu prüfen, ob und inwieweit die geplante Offenlegung von personenbezogenen Daten ein Risiko für die betroffene Person darstellt. Das BAG hält sich hier jedoch nicht mit grundsätzlichen Überlegungen auf, sondern geht pragmatischer vor. Da der Arbeitgeber aus betriebsverfassungsrechtlichen Gründen keinen (direkten) Einfluss auf die Schutzmaßnahmen auf Seiten des Betriebsrates habe, müsse der Betriebsrat darlegen, dass er angemessene Schutzmaßnahmen i.S.d. § 22 Abs. 2 BDSG ergriffen hat. Das BAG geht konkret von einer spezifischen Schutzpflicht des Betriebsrates für empfangene Daten aus, unabhängig von seiner Position als Teil des Verantwortlichen oder selbst Verantwortlichem.

Wer Daten erhält, ist nicht nur Empfänger, sondern verarbeitet auch Daten i.S.d. Art. 4 Nr. 2. Als allgemeines Strukturprinzip sieht etwa Art. 5 DSGVO vor, dass personenbezogene Daten auf rechtmäßige Weise verarbeitet werden müssen. Die Strukturprinzipien richten sich an alle Verarbeiter, nicht nur an Verantwortliche i.S.d. Art. 4 Nr. 7. Auch im Verfahren über die Einsicht in Bruttolohnlisten (1 ABR 53/17) führt das BAG schlicht aus, dass die Verpflichtung, personenbezogene Daten vertraulich zu halten, sich allgemein aus den Vorgaben der DSGVO und des BDSG ergäbe.

Die Hürde angemessener Schutzmaßnahmen durch den BR ist allerdings niedrig. Das BAG führt für die Verarbeitung sensibler Daten mögliche, an § 22 BDSG orientierte Maßnahmen auf: Sicherstellen des Verschlusses der Daten, Gewähr begrenzter Zugriffsmöglichkeiten, Beschränkung auf einzelne Gremiumsmitglieder, Datenlöschung nach Beendigung der Überwachungsaufgabe. Bereits ein passwortgeschützter Zugang zur elektronischen Akte und ein plausibles Löschkonzept sowie ein verschließbarer Aktenschrank erfüllen diese Anforderungen.

Wenn der BR solche Maßnahmen allerdings trotz finanzieller und personeller Ermöglichung durch den Arbeitgeber nicht vorhält, wird eine Datenbereitstellung durch den Arbeitgeber verweigert werden. Im Interesse einer ordnungsgemäßen Aufgabenwahrnehmung müssen Betriebsräte also die aktuellen Datenschutzstandards wahren.

Alexander Hausner LL.M.

Rechtsanwalt, Fachanwalt für Arbeitsrecht, Datenschutzbeauftragter (TÜV)

Telefon: +49 40 4223 6660-0
E-Mail: a.hausner@roser-hamburg.de

Datenschutz im Bewerbungs-verfahren

Jessica Stehn-Bäcker

Datenschutz im Bewerbungsverfahren ist für Unternehmen nichts Neues. Bereits seit 2009 ist der Beschäftigtendatenschutz geregelt. Trotz allem herrscht – spätestens seit Einführung der DSGVO im letzten Jahr – Unsicherheit in den Unternehmen, wie die datenschutzrechtlichen Anforderungen im Bewerbungsverfahren umzusetzen sind.

Im Folgenden werden die wichtigsten Maßnahmen aufgeführt, um das Bewerbungsverfahren datenschutzkonform ablaufen zu lassen:

Informationspflicht

Bereits bei der Stellenausschreibung gibt es datenschutzrechtlich etwas zu beachten: die Einhaltung der Informationspflicht. Nach Art. 12 ff. DSGVO ist der Betroffene über den Umgang mit seinen personenbezogenen Daten zu informieren. Denn nur wer weiß, dass über ihn Daten verarbeitet werden und welche Rechte er hierbei hat, kann diese Rechte auch in Anspruch nehmen.

Nachfolgende Angaben sind dabei regelmäßig zu machen:

- Name und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten, sofern benannt
- Zwecke, für die die personenbezogenen Daten erhoben und verarbeitet werden
- Rechtsgrundlage (vgl. unten)
- Dauer der Speicherung (vgl. unten)
- Empfänger oder Kategorien von Empfängern (z.B. Personalabteilung, Fachbereichsleiter oder Betriebsrat)
- Verarbeitungsort/Speicherort
- das Bestehen der Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruch und Datenübertragbarkeit
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde für Datenschutz
- ggf. das Bestehen eines Rechts, die Einwilligung jederzeit für die Zukunft zu widerrufen (vgl. unten, Stichwort: Bewerberpool)

Aber wie kann man dem Bewerber diesen Informationstext ohne Aufwand zur Kenntnis geben?

Hierfür gibt es eine einfache Möglichkeit, nämlich die sogenannte Link-Lösung: Der Text wird auf der unternehmenseigenen Internetseite unter einer eingängigen Adresse (www.musterfirma.de/info-bewerber) veröffentlicht. Nun kann auf den Text in der Stellenausschreibung, in der (ggf. automatisierten) Eingangsbestätigung, im Online-Bewerbungsportal etc. verwiesen werden.

Rechtsgrundlage

Auch wenn häufig und gerne gewählt: Die Bewerber müssen nicht in die Verarbeitung ihrer personenbezogenen Daten einwilligen!

Nach § 26 Abs. 1 BDSG dürfen „personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigtenverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigtenverhältnisses … erforderlich ist.“ Bewerber fallen gemäß § 26 Abs. 8 Satz 2 BDSG unter den Beschäftigtenbegriff.

Die üblichen Tätigkeiten im Bewerbungsverfahren wie beispielsweise das Sichten der Unterlagen, Einladungen zum Vorstellungsgespräch etc. sind durch § 26 Abs. 1 BDSG gerechtfertigt.

In Ausnahmefällen kann es jedoch sinnvoll sein, sich vom Bewerber eine Einwilligung einzuholen. Beispiel hierfür ist die Aufnahme eines interessanten Kandidaten in einen Bewerberpool. Hier greift dann § 26 Abs. 2 BDSG.

Verarbeitungsverzeichnis

Der Verantwortliche ist nach Art. 30 Abs. 1 DSGVO dazu verpflichtet, über seine Verarbeitungstätigkeiten von personenbezogenen Daten ein Verzeichnis zu führen. Auch das Bewerbungsverfahren sollte hier aufgenommen werden.

Löschen von Bewerberdaten

Nach Abschluss des Bewerbungsverfahren sind die personenbezogenen Daten eines abgelehnten Bewerbers zu löschen, es sei denn, er hat in eine längere Speicherung (Stichwort: Bewerberpool) eingewilligt. Unternehmen müssen die Daten jedoch nicht unmittelbar löschen, da die Möglichkeit einer Klage des Bewerbers aufgrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) gegen den potenziellen Arbeitgeber besteht. Als gängige Speicherdauer werden 6 Monate angesehen.

Limitierter Zugriff auf Bewerberdaten

Bewerbungsunterlagen sind im Unternehmen vertraulich zu behandeln und nur Personen zugänglich zu machen, die in die Besetzung der Stelle involviert sind. Dies sind in der Regel Mitarbeiter der Personalabteilung, der unmittelbare Vorgesetzte und die Geschäftsführung des Unternehmens.

Praxistipps

Richten Sie im Unternehmen eine eigene E-Mail-Adresse für Bewerbungen ein (bewerbung@musterfirma.de). Dieses Postfach sollte, sofern vorhanden, von den regelmäßigen Archivierungen ausgenommen werden.

Leiten Sie die Bewerbungen nicht per Mail oder Hardcopy an die Ansprechpartner im Haus weiter. Richten Sie einen Ordner auf dem Server ein, auf den nur die Mitarbeiter Zugriff haben, die in die Besetzung der Stelle involviert sind. Auch dieser Ordner ist aus den Archivierungen auszunehmen. Legen Sie die Bewerbungsunterlagen dort ab und vergeben Sie an die Zugriffsberechtigten lediglich den Lesezugriff. Ein kurzer Hinweis an die zuständigen Mitarbeiter per Mail genügt („Neuer Bewerbungseingang“).

Auf diese Weise stellen Sie sicher, dass der Zugriff auf die Bewerbungsunterlagen beschränkt ist und diese nach 6 Monaten gelöscht werden können.

Jessica Stehn-Bäcker

Magistra Juris, CIPP/E
Senior Consultant Datenschutz, externe Datenschutzbeauftragte

Telefon: +49 40 22861374
E-Mail: js@beredi-datenschutz.de

Datenschutz und IT-Sicherheit – werden Sie Experte

Jutta Köhn

Hintergrund

Stellen Sie sich vor, Sie tippen eine Nachricht auf Ihrem Handy und irgendwo auf der Welt gibt es eine andere Person, die liest alles mit. Sie kann die Fotos und Videos sehen, die Sie auf Ihrem Handy haben und sie kennt alle E-Mail-Adressen, Telefonnummern und möglicherweise sogar die Wohnadressen Ihrer Familie, von Ihren Freunden, von Ihren Bekannten und Geschäftspartnern. Und da Sie viele Ihrer Kontakte jeweils mit einem Foto versehen haben, weiß diese Person also auch, wie Ihre Familie, Freunde etc. aussehen.

Ihre Daten sind nicht in einem großen anonymen Pool gelandet, wie möglicherweise bei Facebook. Nein, es interessiert sich jemand ganz speziell für Sie und Ihr Leben – ähnlich, als ob Sie in einem Big Brother Container leben würden.

Entsetzliche Vorstellung, oder?

Noch viel entsetzlicher ist es aber, dass diese Vorstellung durchaus realistisch ist.

Wie wir aus der Fangemeinde der Big Brother Container und von den anonymen Teilnehmern an Internetplattformen wissen, gibt es Menschen, die nichts lieber tun, als andere beobachten. Am besten bleibt man selbst unerkannt oder wird – noch besser – gar nicht erst bemerkt. Manche gehen auch noch einen Schritt weiter, da bleibt es nicht beim Beobachten, sondern da wird eingegriffen, um das Beobachtete spannender zu gestalten. Was wird passieren, wenn ich im Namen der Person, die ich gerade ausspioniere, eine Nachricht an einen Freund sende mit unerwartetem Inhalt oder wenn ich gar ein kompromittierendes Foto bei Facebook oder auf anderen Kanälen veröffentliche? Solange sich jemand in Sicherheit vor der Entdeckung wiegt, wird die Wahrscheinlichkeit, dass er eine (manipulative oder sogar strafbare) Handlung begeht, größer.

Noch entsetzlicher, oder?

Maßnahmen

Gegen vieles ist eine einzelne Person sowie auch Unternehmen machtlos. Wir können nichts tun, wenn Microsoft oder Apple oder Google (z. B. für Android) in ihrer Software Fehler haben, die einen Daten- oder Geräte-Zugriff durch fremde, unberechtigte Personen ermöglichen. Wir sind für viele Dinge im privaten sowie im Berufsleben auf diese Software angewiesen, da es wenig Alternativen gibt. Software ist überwiegend von Menschenhand entwickelt und somit nicht fehlerfrei. Unsere täglich genutzten Software-Produkte sind meistens sehr komplex, dementsprechend sind viele Personen an der Entwicklung beteiligt und das macht den Prozess und das Endprodukt schwer beherrschbar und auch nicht mehr vollständig testbar. Insofern sind wir als Anwender erst recht nicht mehr in der Lage, die Software kritisch zu prüfen. Wir müssen zu einem guten Teil darauf vertrauen, dass „alles menschenmögliche“ getan wurde, um uns sichere Software bereitzustellen.

Unternehmen, die entsprechende Software einsetzen, können natürlich vieles für die Sicherheit ihrer Daten und ihrer IT tun, da – je nach Unternehmensgröße – IT-Spezialisten beschäftigt werden oder entsprechend kompetente IT-Dienstleister.

Aber auch jeder einzelne von uns, als Mitarbeiter eines Unternehmens, als Selbstständiger sowie als Privatperson kann etwas tun für die Sicherheit seiner eigenen Daten und der Sicherheit der Daten seiner Kontaktpersonen. Wer sich im Voraus etwas Zeit für ein paar Handgriffe nimmt und ein paar Ratschläge beherzigt, wird mit einer höheren Datensicherheit belohnt. So wie Sie sich im Umgang mit anderen Gebrauchsgegenständen (Autos, TV, Musik-Anlagen) durch Lesen der Bedienungsanleitung, Austausch mit anderen Nutzern und der Suche nach speziellen Informationen z. B. in Internet-Foren selbst zum Experten machen, gelingt Ihnen das genauso auch für den Datenschutz mit diesen 12 Tipps:

Praxistipps

1. Lesen Sie vor Nutzung einer Anwendung das „Kleingedruckte“, die Nutzungsbedingungen, damit Sie mögliche Risiken erkennen. Entscheiden Sie dann bewusst, ob Sie die Anwendung unter diesen Bedingungen wirklich nutzen möchten oder müssen.
2. Prüfen Sie die Installationsparameter der Geräte sowie der genutzten Software oder lassen Sie sich diesbezüglich beraten – sind alle Sicherheitsoptionen korrekt und so streng wie

möglich eingestellt? Sind Verschlüsselungen möglich und aktiviert?

3. Kümmern Sie sich zeitnah um Updates. Informieren Sie sich über die damit bereitgestellten Funktionen und über ggf. kritische Sicherheitslücken, die damit geschlossen werden. Installieren Sie zeitnah für Sie relevante Updates.
4. Nutzen Sie keine veralteten Geräte und Anwendungen, die nicht mehr gewartet und supportet werden
5. Verfolgen Sie auch diesbezügliche Nachrichten oder lassen Sie sich mit Informationen versorgen, auch hier gibt es kostenlose Infos von Fach-Portalen.
6. Minimieren Sie Ihre gespeicherten Daten (Reicht ggf. ein Vorname oder Spitzname oder muss es auch der Nachname sein oder umgekehrt? Brauchen Sie wirklich das Foto zum Kontakt? usw.).
7. Wählen Sie die Art der Nachrichtenübermittlung bewusst. (Wenn ich jemandem Kontaktdaten sende, muss das über WhatsApp sein oder geht das auch auf anderem Weg?)
8. Nutzen Sie komplexe Passwörter, auch für das Handy und den privaten PC sowie für Internet-Anwendungen. Speichern Sie Passwörter für Zugänge zu Anwendungen (Banking, Shopping, Kommunikation usw.) nicht auf Ihren Geräten.
9. Schalten Sie Schnittstellen wie WLAN und Bluetooth nach Gebrauch wieder aus.
10. Überlegen Sie sorgsam, ob Sie ein unsicheres WLAN (Hotspot oder Hotel o. ä.) unbedingt nutzen müssen oder ob die Aktivität verschoben werden kann, bis eine sichere Verbindung genutzt werden kann.
11. Seien Sie wachsam, ob sich eines Ihrer Geräte oder Ihre Software plötzlich ungewohnt verhält. Falls das der Fall ist, trennen Sie das Gerät sofort von der Infrastruktur (Kabel abziehen oder Schnittstelle (WLAN, …) ausschalten).
12. Seien Sie auch wachsam Ihren Mitmenschen gegenüber. Wenn Sie eng mit anderen Menschen zusammen sind (Bahn, Flugzeug, an öffentlichen Plätzen), verzichten Sie ggf. auf Arbeiten am Notebook oder auf Telefonate mit vertraulichen Inhalten.

Empfehlung

Werden Sie zu Ihrem eigenen IT-Sicherheits-Experten und Datenschützer und schützen Sie auch die Daten der Personen, mit denen Sie kommunizieren.

Für Unternehmen heißt das: machen Sie Ihre Mitarbeiter zu Experten in Sachen Datenschutz durch Sensibilisierung und Schulungen.

Lesen Sie in den kommenden Ausgaben mehr dazu.

Jutta Köhn

IT- and Business Auditor, CISA

Telefon: +49 40 4223 6660-0
E-Mail: j.koehn@roser-hamburg.de

BEREDI Marketing GmbH
Bereich Datenschutz

Überseeallee 1
20457 Hamburg

www.beredi-datenschutz.de
Telefon: +49 40 22861374
Telefax: +49 40 22861379

Roser Rechtsanwaltsgesellschaft mbH

Roser GmbH Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft

Drehbahn 7
20354 Hamburg

www.roser-group.de
Telefon: +49 40 4223 6660-0
Telefax: +49 40 4223 6660-12