Umgang mit Personaldaten leicht gemacht

Personalprozesse datenschutzkonform gestalten

Der Umgang mit Personaldaten erfordert von jedem Unternehmen große Sorgfalt: Nicht nur Datenschutzbeauftragter und Betriebsrat prüfen kritisch, ob und wie das Unternehmen die Persönlichkeitsrechte seiner Arbeitnehmer schützt, sondern inzwischen sind auch die Arbeitnehmer sensibilisiert. Daneben ist der unzulässige Umgang mit Personaldaten den Medien immer eine Schlagzeile wert. Damit es nicht so weit kommt, hier ein kurze Anleitung, wie Unternehmen Personalprozesse datenschutzkonform gestalten können.

Das Bundesdatenschutzgesetz (BDSG) definiert den Begriff des Beschäftigten weit: Sowohl der Bewerber als auch der Praktikant, der Heimarbeiter oder der Rentner gelten als „Beschäftigte" im Sinne des BDSG. Daher muss nicht nur der Umgang mit den Daten der bereits angestellten Arbeitnehmer datenschutzkonform ausgestaltet werden, sondern es müssen auch die Prozesse vor und nach deren Anstellung den datenschutzrechtlichen Anforderungen entsprechen.

Datenschutzrechtliche Grundlagen

Auch im Rahmen der Erhebung etc. von Beschäftigtendaten sind die Grundprinzipen des BDSG anzuwenden: Der Grundsatz der Datensparsamkeit und -vermeidung gilt ebenso wie die Zweckbindung und der Grundsatz der Direkterhebung. Zudem erlaubt das BDSG den Umgang mit Daten, wenn entweder eine Rechtsgrundlage oder eine Einwilligung des Betroffenen vorliegt.

Rechtsgrundlagen: § 32 BDSG ...

Den Umgang mit Beschäftigtendaten regelt § 32 BDSG:

- § 32 Abs. 1 BDSG erlaubt u.a. die Erhebung etc. von Daten, sofern dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist.
- § 32 Abs. 2 BDSG regelt, inwieweit Beschäftigtendaten für Zwecke der Aufklärung von Straftaten genutzt werden dürfen.

... und § 28 BDSG

Weiterhin ist inzwischen überwiegend anerkannt, dass § 28 BDSG, der – kurz gesagt – den Umgang mit Daten für eigene Zwecke des Unternehmens regelt, neben § 32 BDSG Anwendung finden kann. Das gilt allerdings nur, sofern der Arbeitgeber die Daten für Zwecke außerhalb des Beschäftigtenverhältnisses nutzen möchte. Das ist beispielsweise der Fall, wenn er Terrorlistenscreenings durchführt, zu denen er gesetzlich verpflichtet ist (siehe Datenschutz PRAXIS 02/2015, S. 5f.).

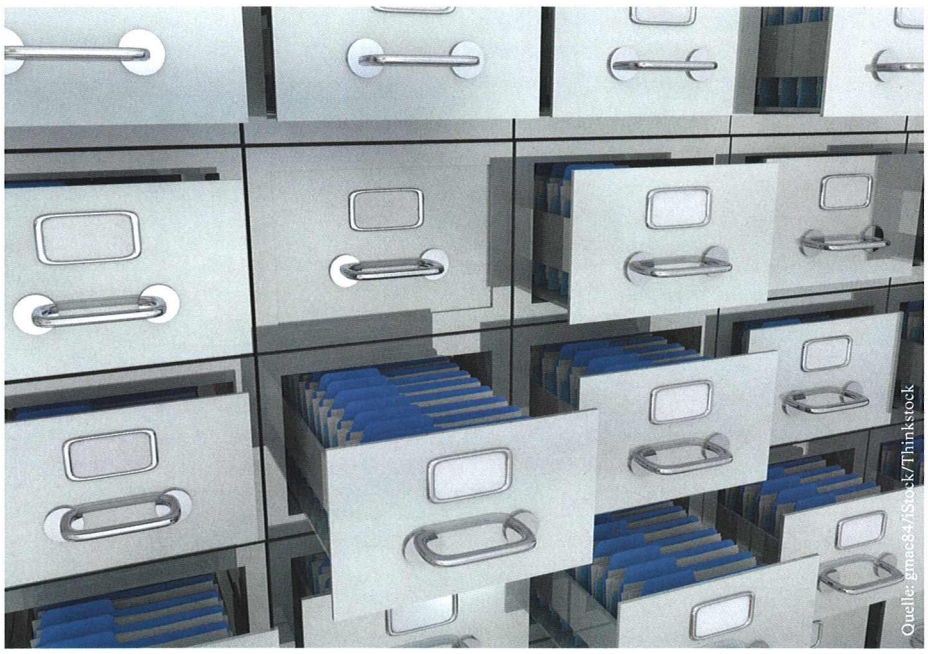
Betriebsvereinbarung?

Der Umgang mit Beschäftigtendaten lässt sich alternativ in einer Betriebsvereinbarung regeln. Ob und inwieweit die Betriebsvereinbarung das Datenschutzniveau des BDSG unterschreiten kann, ist umstritten. Während die Arbeitsgerichte dies bejahen, stehen die Datenschutzaufsichtsbehörden naturgemäß entsprechenden Praktiken kritisch gegenüber. Empfehlenswert ist es in jedem Fall, den Bogen nicht zu überspannen.

Einwilligung?

Gleiches gilt für die Einholung von Einwilligungen:

- Eine wirksame Einwilligung nach § 4a BDSG setzt immer voraus, dass sie freiwillig erteilt wird.
- Ein Bewerber oder auch ein Arbeitnehmer befindet sich in der Regel in einem Abhängigkeitsverhältnis vom (künftigen) Arbeitgeber. Es kann daher bezweifelt werden, ob der Beschäftigte freiwillig einwilligt.
- Nur dann, wenn wirklich die Wahl besteht, ob er die Einwilligung erteilen will oder nicht, und er sie jederzeit widerrufen kann, wird sie



Quelle: gmac84/iStock/Thinkstock

Unter die Personaldaten fallen auch Daten von Bewerbern und Rentnern

als wirksame Einwilligung im Sinne des BDSG gelten.

In der Praxis empfiehlt sich daher zur Minimierung von Risiken ein Verzicht auf die Einwilligung.

Datenschutz in den drei Phasen eines Arbeitsverhältnisses

Die Personalabteilung muss ihre Prozesse an den oben dargestellten Grundlagen ausrichten. Dabei stellen sich in den verschiedenen Phasen des Arbeitsverhältnisses die unterschiedlichsten Anforderungen. Die Hauptphasen stellen wir im Einzelnen nachfolgend vor:

- Phase 1: Die Einstellung
- Phase 2: Während der Beschäftigung
- Phase 3: Das Ausscheiden

Phase 1: Die Einstellung

Für Bewerber gilt nichts anderes als für Mitarbeiter: Es muss eine Rechtsgrundlage vorliegen, die die Erhebung ihrer Daten erlaubt. Auf Einwilligungen sollte aus obigen Gründen grundsätzlich verzichtet werden.

Risiko: Erhebung

Die Erhebung und anschließende Nutzung der Daten ist in der Regel dann erlaubt, wenn die Kenntnis der Daten für die jeweilige Tätigkeit erforderlich ist und dem Bewerbungsprozess dient.

Beispiele:

- Die Erhebung von Kontaktdaten oder Qualifikationen ist zulässig.
- Rückfragen nach einer Vorstrafe sind nur dann erlaubt, wenn dies für die Tätigkeit relevant ist.
- In einem Online-Bewerbertool werden Hobbys als Pflichtfeld abgefragt. Die Abfrage ist nicht erforderlich für die Tätigkeit.
- Internet-Recherchen sind nur zulässig, wenn sie sich auf öffentlich zugängliche Quellen beschränken, d.h. Quellen, die ohne vorherige Registrierung genutzt werden können oder die gezielt beruflichen Zwecken dienen (z.B. Xing oder LinkedIn).

Gibt der Bewerber freiwillig Daten preis, die für die künftige Tätigkeit nicht erforderlich sind, lässt sich daraus ableiten, dass er mit deren Verwendung einverstanden ist.

- Die Personalabteilung sollte bei Erstellung des Jobprofils festlegen, welche Informationen sie vom Bewerber benötigt. Dazu könnte der Datenschutzbeauftragte ein Formblatt zur Verfügung stellen, das z.B. die erlaubten Datenkategorien auflistet.
- Sofern die Daten über ein Online-Bewerbungstool erhoben werden, ist rechtlich zu prüfen, welche Daten der Bewerber zwingend angeben muss. Nur sie dürfen Pflichtfelder sein.
- Ein Merkblatt sollte die Kriterien für die Internet-Recherche festlegen.

Risiko: Weitergabe von Bewerberdaten

Risiken ergeben sich in der Praxis immer wieder bei der Weitergabe von Bewerberdaten: Sie sollte nur an die unmittelbar mit der Bewerbung befassten Personen erfolgen. Es ist sicherzustellen, dass z.B. per E-Mail versandte Unterlagen verschlüsselt werden und nur Berechtigte auf die elektronisch gespeicherten Unterlagen Zugriff haben.

Beispiel:

- Daten werden ohne Information des Bewerbers an andere Unternehmen der Konzerngruppe übermittelt. Dabei hatte sich der Bewerber lediglich auf eine Hausmeisterstelle bei dem deutschen Unternehmen beworben.

Risiko: Aufbewahrung

Es sollte zudem ein Archivierungskonzept umgesetzt werden mit Regelungen zur Löschung der Daten.

Beispiel:

- Der Bewerber wird abgelehnt. Seine Bewerbung sollte spätestens nach Ablauf der Fristen nach § 15 Allgemeines Gleichbehandlungsgesetz (AGG) gelöscht werden. Hier käme höchstens eine Speicherung des Namens in Betracht, alternativ muss die (freiwillige) Einwilligung zur längeren Speicherung eingeholt werden. Widerruft der Bewerber sie, sind die Daten zu löschen.

Phase 2: Während der Beschäftigung

In der Regel ergibt sich die Zulässigkeit des Umgangs mit Mitarbeiterdaten aus § 32 BDSG: Danach dürfen – soweit erforderlich – Beschäftigtendaten für Zwecke der Durchführung des Arbeitsverhältnisses erhoben, verarbeitet und genutzt werden.

Risiko: Erforderlichkeit

Hier liegt der Teufel im Detail: Im Einzelfall stellt sich die Frage, welche Nutzungen tatsächlich „erforderlich" sind. Während der eine es als vertretbar ansieht, dass zumindest der Geburtstag der Mitarbeiter für Zwecke der Förderung der Gemeinschaft im Unternehmen ausgetauscht wird, halten die Datenschutzaufsichtsbehörden dies aufgrund mangelnder Erforderlichkeit für bedenklich.

Hier empfiehlt es sich für den Datenschutzbeauftragten, die Mitarbeiter der Personalabteilung z.B. durch Schulungen zu sensibilisieren und in praxisbezogenen Handlungsanweisungen kritische Themen aufzugreifen. Diese Handlungsanweisungen sollten im Idealfall die im Unternehmen geltende Datenschutzrichtlinie bereichsspezifisch ergänzen.

Beispiele:

- Die Mitarbeiter geben ihre Abwesenheiten in einen Teamkalender, auf den alle Mitarbeiter Zugriff haben, ein. Sind sie krank, ver-

merkt die Personalabteilung dies im Teamkalender. In diesem Fall sollte für alle Abwesenheitsgründe ein einheitlicher Begriff gewählt werden. Denn der Austausch von besonderen personenbezogenen Daten (= „krank") ist für Zwecke des Beschäftigtenverhältnisses nicht erforderlich.

- Fotos von Mitarbeitern sollen im Intra- und Internet veröffentlicht werden. Fotos stellen personenbezogene Daten dar und unterliegen dem Kunsturhebergesetz. Die Veröffentlichung des Fotos eines Beschäftigten bedarf daher seiner Einwilligung, die für die konkreten Zwecke einzuholen ist.
- Das Unternehmen muss die Mitarbeiter aus Compliance-Gründen einem Terrorlistenscreening unterziehen. Die Prozesse sind festzulegen (z.B. werden nur EU-Terrorlisten verwendet, wer führt das Screening durch, wie wird mit Treffern umgegangen).
- Im Unternehmen wird gestohlen. Das Unternehmen möchte Videoüberwachungsmaßnahmen starten. Der Datenschutzbeauftragte muss sorgfältig vorab prüfen, ob diese Maßnahme mit §§ 32, 28 bzw. 6b BDSG im Einklang steht.

Risiko: Austausch von Daten

In der heutigen Unternehmenspraxis gehört der Austausch von Beschäftigtendaten zum Alltag:

- Beschäftigte greifen auf die Daten anderer Beschäftigter zu.
- Globale HR-Systeme sind in Unternehmensgruppen im Einsatz.
- Anfragen von Behörden zu Mitarbeitern oder auch die Speicherung von Beschäftigtendaten in einem auslagerten Rechenzentrum sind inzwischen Standard.

Austausch innerhalb des Unternehmens

Beschäftigtendaten sind in der Regel sensibel und sollten entsprechend behandelt werden. Daher bedarf bereits der Austausch der Daten innerhalb eines Unternehmens einer Erlaubnis, er muss also erforderlich sein.

Beispiele:

- Im Rahmen des Beurteilungsprozesses bewerten mehrere Vorgesetzte einen Mitarbeiter; an sie dürfen dessen Daten übermittelt werden.
- Kollegen wollen einem kranken Mitarbeiter einen Blumenstrauß senden. Die Privatadresse darf nur mit Einwilligung des Mitarbeiters an die Kollegen übergeben werden bzw. die Personalabteilung sollte den Strauß versenden.
- Der Zugriff auf Personaldaten wird über ein im Unternehmen festgelegtes Berechtigungskonzept gesteuert, das rollenbasiert festlegt, wer auf welche Personaldaten lesenden oder ändernden Zugriff hat.
- Ein Mitarbeiter ist krank und hat keinem Stellvertreter Zugriff auf sein E-Mail-Postfach eingeräumt. Hier sollte ein Prozess festgelegt sein, unter welchen Voraussetzungen der Zugriff durch einen Vertreter zulässig ist (z.B. Prüfung und Freigabe durch den DSB).

Austausch mit Dritten

Die Weitergabe der Daten erfordert – wie üblich – eine Rechtsgrundlage. Das gilt auch, wenn Daten zwischen den Unternehmen einer Konzerngruppe ausgetauscht werden. Das deutsche Datenschutzrecht kennt insoweit kein Konzernprivileg. Der Austausch muss daher auch innerhalb eines Konzerns entweder über die §§ 32, 28 BDSG oder aufgrund eines Auftragsdatenverarbeitungsvertrags nach § 11 BDSG gerechtfertigt werden.

Beispiele:

- Der Mitarbeiter hat einen internationalen Arbeitsvertrag abgeschlossen und ist für mehrere Unternehmen der Gruppe regelmäßig tätig. Der Austausch der Daten ist daher gemäß § 32 BDSG für sein Arbeitsverhältnis erforderlich.
- Organisatorisch ist festgelegt, dass der Vorgesetzte des Mitarbeiters in einem anderen Unternehmen arbeitet als der Mitarbeiter selbst; der Vorgesetzte ist gleichwohl für ihn zuständig. Auch hier ist der Austausch über § 32 BDSG gerechtfertigt.

Quelle: Wavebreakmedia Ltd/Wavebreak Media/Thinkstock

Im Bewerbungsprozess ist die Erhebung und Nutzung der Daten in der Regel erlaubt, wenn die Kenntnis der Daten für die angestrebte Tätigkeit erforderlich ist

Best Practice

- Ein IT-Provider hostet zentral das HR-System. Mit ihm wurde ein Auftragsdatenverarbeitungsvertrag gemäß § 11 BDSG geschlossen, der als Rechtsgrundlage für den Austausch dient.

Und: Risiko unsicherer Drittstaat

Besondere Risiken ergeben sich zudem, wenn die Daten an Unternehmen mit Sitz in einem Land, das kein dem europäischen Recht entsprechendes Datenschutzniveau aufweist, übermittelt werden (z.B. Indien oder Brasilien, sogenannte unsichere Drittstaaten).

In diesem Fall muss das verantwortliche Unternehmen, das die Daten übermittelt, zusätzlich zu den obigen Maßnahmen z.B. mit dem Empfänger der Daten die Standardvertragsklauseln der EU abschließen, die den Austausch der Daten legitimieren.

Die EU hat für den Fall des sogenannten Controller-Controller-Transfers (d.h. der Empfänger nutzt die Daten nicht im Auftrag des Übermittlers, sondern für eigene Zwecke) zwei Sets von Standardvertragsklauseln erlassen (Versionen 2001 und 2004). Die Version von 2004 ist zwar unternehmensfreundlicher, bedarf allerdings laut Auffassung der Datenschutzaufsichtsbehörden bei Einsatz für Beschäftigtendaten einer Ergänzung, um die Rechte der Arbeitnehmer sicherzustellen. Dies sollte berücksichtigt werden.

Auskunftsersuchen Dritter

Häufig wird die Personalabteilung auch mit Fragen von Behörden oder von anderen auskunftsersuchenden Stellen konfrontiert. Hier ist sorgfältig zu prüfen, ob die Daten unter Berücksichtigung des einschlägigen Datenschutzrechts weitergegeben werden dürfen. Grundsätzlich ist in solchen Situationen Zurückhaltung anzuraten; es sollte jedenfalls im Einzelfall die Identität der Stelle überprüft werden, und aus welchen Gründen sie die personenbezogenen Daten benötigt.

Es empfiehlt sich, einen Leitfaden zu erstellen, wie z.B. mit telefonischen Anfragen von Behörden umzugehen ist. Er sollte regeln, dass telefonische Anfragen nicht zu beantworten sind, sondern die Stelle aufzufordern ist, eine schriftliche Anfrage zu stellen. Sie muss Auskunft geben über die Identität der anfragenden Stelle, die Namen der Mitarbeiter, über die Auskunft begehrt wird, die Zwecke, für die diese Daten verwendet werden, und die rechtlichen Grundlagen, aufgrund derer das Auskunftsersuchen gestellt wird.

Auskünfte dürfen zudem nicht ohne Rücksprache bzw. nur mit Einwilligung des betroffenen Mitarbeiters erteilt werden. Die Einwilligung und auch der Umfang der Auskunft sind zu dokumentieren.

Beispiele:

- Der zukünftige Arbeitgeber fragt Informationen über einen ehemaligen Mitarbeiter ab. Der ehemalige Mitarbeiter muss vorab gefragt werden, ob er das möchte. Dies ist zu dokumentieren. Sofern der Mitarbeiter wünscht, dass seine personenbezogenen Daten weitergereicht werden, sollte auch dies schriftlich dokumentiert werden.
- Die ehemalige Gattin ruft an und fragt nach der Höhe des Bonus des Mitarbeiters, da sich danach ihr Unterhaltsanspruch berechnet. Die Einwilligung des Mitarbeiters ist erforderlich.

Phase 3: Das Ausscheiden

Wenn ein Mitarbeiter das Unternehmen verlässt, ist sicherzustellen, dass eine ordnungsgemäße Übergabe der von ihm benutzten Arbeitsmittel erfolgt und der Zugriff auf die von ihm in seinem E-Mail-Postfach oder auf der Festplatte des Laptops gespeicherten Daten sichergestellt wird.

Dabei sollten Prozesse im Unternehmen etabliert sein, die sowohl ein „ordnungsgemäßes" als auch ein außerplanmäßiges Ausscheiden abbilden. Ein ordnungsgemäßes Ausscheiden wäre z.B. eine ordentliche Kündigung des Mitarbeiters. Ein Mitarbeiter scheidet außerplanmäßig aus, wenn er etwa fristlos gekündigt wird oder überraschend verstirbt.

Neben Laufzetteln, die ausscheidende Mitarbeiter abarbeiten, sollte die Personalabteilung auch Standardprozesse einführen, die einen Zugriff auf die E-Mails überraschend ausscheidender Mitarbeiter sicherstellen (z.B. Informationsschreiben an die Mitarbeiter, Einbindung der Vorgesetzten, des DSB und der IT bei Sichtung der im Postfach gespeicherten geschäftlichen Korrespondenz).

Grundsätzlich sind personenbezogene Daten der Mitarbeiter zu löschen, sofern sie nicht mehr erforderlich sind, um das Arbeitsverhältnis zu begründen, durchzuführen oder zu beenden. Daher sind die Daten ausscheidender Mitarbeiter grundsätzlich zu löschen. Allerdings kann es Ausnahmen geben.

Beispiele:

- Für Zwecke der Zahlung von Renten oder Pensionen sind die Daten des ausgeschiedenen Mitarbeiters aufzubewahren.
- Es bestehen gesetzliche Aufbewahrungspflichten, z.B. aus steuerlichen Gründen.
- Der Mitarbeiter hat Regressansprüche gegen das Unternehmen geltend gemacht, oder deren Geltendmachung ist zu befürchten.

Sofern eine Löschung nicht zulässig ist, sind die Daten zu sperren. Es empfiehlt sich die Einführung entsprechender Archivierungs- bzw. Löschkonzepte.

Last but not least: Der technisch-organisatorische Teil

Bei der datenschutzkonformen Gestaltung von Personalprozessen darf nicht

vergessen werden, dass gerade die Personalabteilung besondere Sensibilität im Umgang mit den Daten zeigen muss. Neben der obligatorischen Verpflichtung aller Mitarbeiter der Personalabteilung auf das Datengeheimnis nach § 5 BDSG sollten speziell für die Personalabteilung zusätzliche Vorkehrungen getroffen werden.

Beispiele:

- Die Räumlichkeiten der Personalabteilung sind abzuschließen bzw. durch entsprechende Mechanismen abzusichern. Berechtigungen (Schlüsselregelungen etc.) sind schriftlich zu fixieren.
- PCs sind vor der Einsichtnahme durch Dritte zu schützen.
- Personaldaten sind nur auf den dafür vorgesehenen Netzlaufwerken bzw. in den dafür vorgesehenen IT-Systemen abzuspeichern; Zugriffe dürfen nur im Rahmen der Berechtigungssysteme erfolgen.
- Personalakten sind in abschließbaren Schränken aufzubewahren.
- Es gilt eine Clean Desk Policy.
- Es sind eigene Drucker und Faxgeräte für die Personalabteilung bereitzustellen.
- Ausdrucke etc. sind sofort vom Kopierer abzuholen.
- Fehldrucke oder nicht mehr benötigte Dokumente etc. sind datenschutzkonform zu entsorgen.
- Die Weitergabe der Daten darf nur verschlüsselt erfolgen.

Zentral: Schulungen und Handlungsanweisungen für die Personalabteilung

In der Praxis zeigt sich, dass regelmäßige Schulungen und Handlungsanweisungen, die eine im Unternehmen gelebte Datenschutzrichtlinie ergänzen, wirkungsvolle Maßnahmen sein können, um datenschutzkonforme Personalprozesse umzusetzen. Da ein Verlust bzw. ein unberechtigter Zugriff auf diese sensiblen Daten leicht zu einem Datenschutzvorfall nach § 42a BDSG führen kann, lohnt sich auch aus dieser Perspektive für jedes Unternehmen und für jeden Datenschutzbeauftragten ein engagierter Einsatz in diesem Bereich.

Silvia C. Bauer

Silvia C. Bauer ist Rechtsanwältin bei der Luther Rechtsanwaltsgesellschaft mbH, Köln.

IDACON 2015

Noch mehr zum Datenschutz in der Personalabteilung erfahren Sie auf der IDACON 2015, die vom 13. bis zum 15. Oktober stattfindet (*www.idacon.de*)!