PRODATIS®

The eBusiness Solution Company.

Datenverarbeitung von der Bewerbung bis zum Jobwechsel

Einführung

Nirgends im Unternehmen finden sich so viele personenbezogene Daten wie in der Personalabteilung, auch Human Ressources genannt: Vom Namen über Geburtsdatum, von Adresse, über Gehaltsangaben bis zu Daten, welche unter «sensibel» klassifiziert werden. Letztere sind als be- sondere Kategorien personenbezogener Daten zu verstehen und in der gesetzlichen Terminologie gemäss Art. 9 DSGVO als spezielle Kategorien von Daten bezeichnet. Dazu gehören Daten, die in die sehr private, wenn nicht intime Sphäre eines Individuums fallen. Etwa Angaben zur Religionszugehörigkeit, zur politischen Meinung oder zur Gesundheit. Doch was müssen Unternehmen beachten, um «Human Ressources»-Daten (HR-Daten) sicher zu verarbeiten? Was gilt es datenschutzrechtlich zu beachten? Mithilfe des vorliegenden Beitrags soll ein Grundverständnis rund um die Thematik des Datenschutzes im Beschäftigtenverhältnis geschaffen werden.

Die Datenverarbeitung im Arbeitsverhältnis

Personalabteilungen verarbeiten relevante Informationen eines Angestellten, die sich im Laufe des Arbeitsverhältnisses ansammeln. Dabei geht es oftmals um sensible Angaben, welche der Angestellte als vertraulich behandelt wissen möchte. Sie sollen nur für Zwecke verarbeitet werden, die dem Arbeitsverhältnis dienen. Kein Mitarbeiter wünscht, dass seine Daten ohne Kenntnis und Einwilligung zweckentfremdet an Dritte weitergegeben werden oder bei einem Hackerangriff abgegriffen und womöglich im Darknet verkauft werden. Der Personalabteilung kommt somit große Verantwortung zu.

Bei der Verarbeitung von HR-Daten sind die betroffenen Datensubjekte neben den internen oder externen Angestellten auch Bewerber und ausgeschiedene Mitarbeiter. In der Datenschutz-Grundverordnung (DSGVO) werden Datenarten nicht in dem Sinne kategorisiert, dass Vorschriften zu etwaigen «Arbeitnehmerdaten» vorzufinden sind. Vielmehr definiert Art. 4 Nr. 1 DSGVO personenbezogenen Daten als solche, «die sich auf eine identifizierte oder identifizierbare natürliche Person» beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, «insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der

physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann». Dazu zählen allgemeine Kontaktdaten wie Name, Adresse, Telefonnummer oder andere Personalien wie Geburtsdatum, Staatsangehörigkeit, Zivilstand und Geschlecht. Auch etwaige Legitimationsdaten wie Pass- oder Ausweisnummern, Steuer- und Kontonummern sowie Informationen über die Bonität des Bewerbers kommen in Betracht.

In den HR-Akten werden auch fortlaufende Angaben zum Arbeitsverhältnis an sich festgehalten, etwa Daten aus dem Performance-Management hinsichtlich des persönlichen beruflichen Fortkommens, dem Learning-Management oder den Zielvereinbarungen innerhalb eines Geschäftsjahres. Daneben werden auch Daten gemäss Art. 9 (1) DSGVO verarbeitet. Dabei geht es um jene Daten, «aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie die Verarbeitung von genetischen Daten». Auch biometrischen Daten zur Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person dürfen demnach nicht erhoben werden. Dieses Verbot ist jedoch «nur» ein Verbot mit Erlaubnistatbeständen und so darf beispielsweise gemäss Art.9 (1) DSGVO die Verarbeitung durch eine rechtsgültige Einwilligung stattfinden.

Zur Datenerhebung im Beschäftigungsverhältnis gilt im Allgemeinen in der Schweiz und in Deutschland, dass der Arbeitnehmer die Privatsphäre des Arbeitnehmers zu beachten hat. In Deutschland lassen sich noch spezifische datenschutzrechtliche Bestimmungen in verschiedenen Gesetzen verorten, etwa in § 39 Abs. 8 Einkommensteuergesetz oder § 18 f Sozialgesetzbuch (SGB) Viertes Buch (IV) sowie im kollektiven Arbeitsrecht § 75 (2) BetrVG. In der DSGVO lässt die Vorschrift des Art. 88 (1) DSGVO den Mitgliedstaaten Freiraum, durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften hinsichtlich der Verarbeitung personenbezogener Daten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung und zur Erfüllung des Arbeitsvertrags zu erlassen. Aus deutscher Sicht ist § 26 BDSG zur «Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses » ausschlaggebend.

Lebenszyklus der Daten

Um sich einen Überblick über die erhobenen Daten zu verschaffen, sollte ein Blick auf die verschiedenen Etappen des Lebenszyklus der Daten geworfen werden. Ein solcher Zyklus beinhaltet das Verfahren von der Bewerbung bis zum Ausscheiden des Arbeitnehmers aus dem Unternehmen. Vorab ist zu erwähnen, dass bei der Datenverarbeitung im gesamten Zyklus stets die Datenschutzprinzipien auch im Rahmen eines Arbeitsverhältnisses gelten. Dazu zählen nach Art. 5 DSGVO die Rechtmässigkeit (Verarbeitung nach Treu und Glauben/Transparenz), die Zweckbindung, die Datenminimierung, die Richtigkeit, die Speicherbegrenzung, die Integrität und Vertraulichkeit und die Rechenschaftspflicht. Bei sorgfältiger Umsetzung ist der Grundstein des datenschutzkonformen Umgangs gelegt. Um der Rechenschaftspflicht nachzukommen, sollte die Verarbeitung dokumentiert und technische und organisatorische Massnahmen angepasst werden. Mittels eines Verzeichnisses von Verarbeitungstätigkeiten kann einfach und übersichtlich eine gute Basis für die Dokumentation gelegt werden. Es wird geraten, dass auch Unternehmen unter 250 Mitarbeitern dieses führen sollten.

Bewerbungsverfahren

Es gibt zahlreiche Möglichkeiten, als Bewerber in das Bewerbungsverfahren zu gelangen. Gewöhnlich geschieht dies durch Initiativbewerbung oder durch das Bewerben auf eine Stellenanzeige. Der Bewerber schickt in der Regel ein Motivationsschreiben, seinen Lebenslauf und seine Zeugnisse. Darin gibt er auf Verlangen des potenziellen Arbeitgebers Auskunft über personenbezogene Daten aller Art, welche von allgemeinen Kontaktdaten bis hin zu Geburtsdatum, Staatsangehörigkeit, Zivilstand und Geschlecht reichen. Dazu kommen die oben bereits ausgeführten Daten. Des Weiteren können durch extracurriculare Aktivitäten weitere Daten im Sinne von Art. 9 DSGVO hinzukommen.

Der Grundsatz der Verhältnismässigkeit aus Art. 5 DSGVO

gebietet seitens des Arbeitgebers, dass stets nur Angaben eingefordert werden, welche auch erforderlich sind für das zu begründende Arbeitsverhältnis. Dies gilt auch für Fragen zu einer Schwangerschaft bei einem Bewerbungsgespräch. Wenn diese nicht für die zu besetzende Stelle von absoluter Relevanz ist - etwa für eine gefährliche oder beschwerliche Arbeit - muss der Arbeitgeber sich damit abfinden, dass die betroffene Person keine Angaben macht. Dies darf beim nachträglichen Entdecken der Schwangerschaft auch nicht zu einer Anfechtung des Arbeitsverhältnisses führen. Zudem darf diese Frage aus rechtlicher Perspektive ohnehin nicht gestellt werden, da sie das im Gleichstellungsgesetz verankerte Diskriminierungsverbot verletzt. Nur solche Fragen, welche für die Entscheidungsfindung wichtig sind, dürfen gemäss des Grundsatzes der Datenminimierung aus Art. 5 (1) lit. c DSGVO gestellt werden. Arbeitgebern ist es nur gestattet personenbezogene Daten zu sammeln und zu erheben soweit es für die angestrebte Position erforderlich ist. Bei der Stellenausschreibung empfiehlt der Schweizer Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB), dass der Arbeitgeber sich vor der Ausschreibung einer vakanten Stelle über die mitzubringenden Qualifikationen und das Anforderungsprofil ein präzises Bild von den gewünschten Anforderungen macht. Bewerberinformationen sollten nicht nach Belieben erfragt werden, um erst im Nachhinein zu entscheiden, welche dieser Angaben tatsächlich benötigt werden.

Bei der Benutzung von cloudbasierten HR-Anwendungen ist zudem zu berücksichtigen, dass Daten grenzüberschreitend übermittelt werden können. Dagegen spricht auch nichts, solange das Land gemäss Art. 4 DSGVO ein angemessenes Datenschutzniveau gewährleistet oder geeignete Garantien getroffen wurden. Für große Unternehmen mit einer ausgereiften Datenschutzstruktur eignen sich zudem gemäss Art. 47 DSGVO die verbindlichen internen Datenschutzvorschriften. Die Daten, welche an den Empfänger gelangen, sollten dabei nur auf das erforderliche Maß einsehbar sein. Hier sei angemerkt, dass seit dem EuGH-Urteil vom 16.07.2020 (Schrems II, C-3111/18) gilt, dass das „Privacy Shield“ nicht mehr als zulässiger Mechanismus eingesetzt werden darf, um personenbezogene Daten von der EU in die USA zu übermitteln. Dieser bahnbrechende Entscheid stellt die USA jenen Ländern gleich, welche ausserhalb der EU/EWR oder nicht in einem Kommissionsbeschluss als Land mit einem datenschutzrechtlich angemessenen Schutzniveau bezeichnet wurden.

Was das Löschen angeht, sollte auf Fristen geachtet werden: Will ein Bewerber eine Benachteiligung wegen eines vom Allgemeinen Gleichbehandlungsgesetz (AGG) verbotenen Merkmals geltend machen, muss er dies innerhalb einer Frist von zwei Monaten tun. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW) hält eine Speicherung von Bewerbungsunterlagen nach Abschluss des Auswahlverfahrens über vier Monate hinaus für nicht erforderlich. Er empfiehlt Arbeitgebern, nach Ablauf dieser Zeitspanne eine Löschung zu veranlassen. Sollten Profile in ein Bewerberpool zur Besetzung neuer Stellen aufgenommen werden, ist eine Einwilligung des Betroffenen erforderlich. Dabei sollten die Datenschutzhinweise konkret formuliert werden. Hierbei ist insbesondere auf die jederzeitige Widerrufsmöglichkeit der Einwilligung hinzuweisen.

Im laufenden Arbeitsverhältnis

Ist der Bewerber erfolgreich in das Arbeitsverhältnis eingetreten, hinterlässt er im Arbeitsalltag Datenspuren. Bei vielen Unternehmen wird bei Arbeitsbeginn und Arbeitsende die Zeit erfasst. Per Mail und über andere digitale Kommunikationswege findet ein permanenter Austausch statt, Fotos werden erstellt oder Social-Media-Kanäle bedient. Zudem sammelt die HR-Abteilung wichtige Daten im Personaldossier. Darunter fallen Personalien und Adressdaten, Bewerbungsunterlagen, Referenzauskünfte, der Arbeitsvertrag und Entgelte, Angaben über Arbeitsausfälle, Krankheiten und Arztzeugnisse, Lohn- und Versicherungsdaten, Angaben zum Performance Management oder mögliche Disziplinarmassnahmen wie Verwarnungen, Verweise oder Bußgelder. Der Schweizer EDÖB empfiehlt hier, dass das Personaldossier einer regelmässigen Selektion -in der Regel jedes zweite Jahr- unterzogen werden sollte und die in dem Rahmen nicht mehr benötigten Unterlagen entfernt werden.

Die Einwilligung

Eine Besonderheit im Rahmen des Arbeitsverhältnisses stellt die Verarbeitung aufgrund der Einwilligung dar, wenn die gesetzlichen Erlaubnistatbestände nach Art. 6 (1) lit. b bis f DSGVO nicht greifen. Erwägungsgrund 42 DSGVO schreibt zur Einwilligung gemäss Art. 7 DSGVO vor, dass nur dann davon ausgegangen werden sollte, dass eine Person ihre Einwilligung freiwillig gegeben hat, wenn sie eine «echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden». Gemäss Erwägungsgrund 43 sollte «in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern».

Im Rahmen des Beschäftigtenverhältnisses stellt sich also die Frage nach der Freiwilligkeit einer durch den Angestellten abgegebenen Willenserklärung: Wie freiwillig ist eine Einwilligung in Anbetracht des Abhängigkeitsverhältnisses, welches ein Arbeitsverhältnis mit sich bringt? Dieses Problem bezieht sich dem Grunde nach auf alle Arten von Abhängigkeitsverhältnissen. Das Vorliegen einer Freiwilligkeit wird oftmals als problematisch angesehen, da die wirtschaftliche und persönliche Abhängigkeit des Arbeitnehmers suggeriert, dass die Person in einer Zwangslage steckt und somit nicht frei entscheiden kann. Arbeitnehmer seien selten in der Lage tatsächlich freiwillig einzuwilligen. Dies bestätigt auch das LfDI Baden-Württemberg, wonach es in der Praxis an der notwendigen Freiwilligkeit der Einwilligung fehle. Eine abgegebene Einwilligung kann aber nur dann wirksam sein, wenn der Arbeitnehmer die Möglichkeit hat, selber zu bestimmen, ob und wie seine Daten verwendet werden können. Dazu gehört auch, dass er ohne Furcht vor möglichen Konsequenzen seine Einwilligung jederzeit entziehen kann.

Für die Einwilligung im Rahmen des Beschäftigungsverhältnisses gelten somit spezielle Anforderungen: Der Betroffene muss hinreichend bestimmt und transparent über die konkrete Tragweite seiner Entscheidung aufgeklärt werden. Erfolgt die Einwilligung via schriftlicher Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen der Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache derart erfolgen, dass von anderen Sachverhalten klar zu unterscheiden ist. Erwägungsgrund 32 fügt hinzu, dass die Einwilligung durch eine eindeutige bestätigende Handlung erfolgen sollte, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist (etwa in Form einer schriftlichen oder einer mündlichen Erklärung). Erstere kann auch elektronisch erfolgen.

Die Einwilligung ist dem LfDI Baden-Württemberg nach, in Konstellationen möglich, die nicht das Arbeitsverhältnis als solches, sondern Zusatzleistungen des Arbeitgebers betreffen. Etwa bei der Erlaubnis, den Dienstwagen nicht nur für berufliche, sondern auch für private Zwecke zu nutzen, der Arbeitgeber dem Arbeitnehmer das Diensthandy und andere EDV-Geräte zum privaten Gebrauch überlässt oder wenn der Arbeitnehmer seinen Namen auf eine Geburtstagsliste setzen lässt.

Die Verarbeitung personenbezogener Daten von Beschäftigten sei im Grunde oft zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich und könne deshalb auf § 26 BDSG als gesetzliche Grundlage gestützt werden. Somit muss und sollte erst gar nicht das Gewicht primär auf die Einwilligung gelegt werden, solange es um essentielle Sachverhalte zum Arbeitsverhältnis geht. Wenn eine Einwilligung doch zum Zuge kommt, hat der deutsche Gesetzgeber mit § 26 (2) S.2 BDSG normiert, dass erst dann eine sogenannte Freiwilligkeit vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen.

Weitere technische Massnahmen des Arbeitgebers

Im Arbeitsverhältnis fallen unter Umständen auch Daten durch Tracking und Monitoring an. Das Aushändigen von Laptops, Handys und Tablets ermöglicht ein mobiles Arbei-

ten im Auto, im Zug oder von Zuhause. Von letztere Option sind durch Covid 19 viele Arbeitnehmer betroffen und haben ihren Arbeitsort ins Homeoffice verlegt. Der Arbeitnehmer gewinnt damit an Flexibilität und Freiheit, zugleich möchte der Arbeitgeber die Geräte vor Hackerangriffen und Malware schützen. Dazu gehört mitunter auch eine physische Ortung der Geräte. Besonders in Handwerksberufen ist es üblich, dass GPS-Ortungs- und Trackingfunktionen in Mobilgeräten, Laptops oder in Autos eingebaut werden. Zudem ist es weit verbreitet, dass das Bedürfnis des Arbeitgebers besteht, Mobilgeräte und Laptops nachzuverfolgen, falls diese abhandenkommen.

In diesem Rahmen wird auch in die Privatsphäre des Arbeitnehmers eingegriffen. Der Arbeitgeber wird dies gemäss Art. 6 (1) lit. d DSGVO mit der Wahrung der berechtigten Interessen rechtfertigen und dies zweckdienlich unter den Aspekt der Sicherheit subsumieren. Dabei sollte der Arbeitgeber stets die Möglichkeit wählen, welche für das Datensubjekt am wenigsten invasiv ist (Prinzip der Verhältnismässigkeit). Dadurch lässt sich ein missbräuchliches Überwachen des Arbeitnehmers vermeiden. Zu erinnern ist dabei stets an den Lidl-Überwachungsskandal 2008, bei dem der Discounter in die Negativschlagzeilen geriet. Dies zeigt, dass viele Compliance-Risiken nicht «nur» Sanktions-Risiken beinhalten, sondern auch ein Reputationsrisiko.

Um dies zu vermeiden, sollte das Augenmerk auf Art. 25 DSGVO und Art. 35 DSGVO gelegt werden («data protection by design and by default» und «data protection impact assessments»). Datenschutz muss danach eine Schlüsselkomponente bereits bei der Festlegung des Mittels – etwa einer Applikation- sein. «Data Protection by default» hingegen legt die Pflicht fest, angemessene technische und organisatorische Massnahmen zu treffen zum Wohle der Datensparsamkeit sowie «privacy-freundliche» Features.

Es ist sinnvoll, im Vorhinein in einer Richtlinie festzulegen, über welche Zwecke Protokolldaten wann und von wem abgerufen werden können. Daran können sich die Angestellten orientieren, um sie über eine akzeptable und inakzeptable Nutzung des Netzes zu informieren. Dies ermöglicht es, dass das Nutzerverhalten so angepasst werden kann, dass eine Überwachung überflüssig wird.

Mailzugriff bei unvorhersehbaren Abwesenheiten

Eine gegenwärtige Frage, welche aber noch nicht geregelt ist, stellt der Mailzugriff bei unvorhergesehenen Abwesenheiten des Arbeitnehmers dar. Dies betrifft Abwesenheiten beispielsweise bei Krankheiten oder Unfällen, die den Arbeitnehmer ad hoc über einen längeren Zeitraum daran hindern, seiner geschäftlichen Tätigkeit nachzugehen. Unter Umständen ist es nötig, auf die Mails des Betroffenen zuzugreifen, mit der Gefahr, dass dabei auch private Nachrichten eingesehen werden. Die Frage wird unterschiedlich gehandhabt. Einige Arbeitnehmer untersagen gänzlich den privaten Mailverkehr über die Arbeits-E-Mail-Adresse, während andere ihn hingegen gewähren. Der einfachste aber zugleich radikalste Weg, sich abzusichern, wäre eine vollständige Untersagung der Privatnutzung. Weniger drastische Alternativen stellen das Ernennen eines Stellvertreters dar, der Zugriff auf die Mails hat, oder eine automatische Weiterleitung der Mails an denselben. Beides birgt aber wieder das Risiko, dass private Nachrichten mitgelesen werden könnten.

Welcher Weg auch gegangen wird, es ist wichtig, dass im Vorfeld das Einverständnis des Mitarbeiters unter Darlegung des Zwecks schriftlich eingeholt wird. Wenn daraufhin der Zugriff auf das Postfach erfolgt, darf keinesfalls eine Mail, welche offensichtlich privater Natur ist (etwa im Betreff als «Privat» gekennzeichnet), durch den Arbeitgeber verarbeitet werden. Um unliebsame Überraschungen zu vermeiden, sollte dieser Umgang in einem firmeninternen Reglement festgehalten werden, damit der Arbeitnehmer weiss, wie bei unerwarteter Abwesenheit mit seinen Mails umgegangen wird. So können sich sowohl Arbeitnehmer als auch Arbeitgeber auf ihre Rechte und Pflichten einstellen. Auf diese Weise wird dem Transparenzgebot nachgekommen. Dies entschied auch der Europäischen Gerichtshofs für Menschenrechte (EGMR) bei einem Überwachungssachverhalt, wonach die Internetkommunikation der Beschäftigten überwacht werden dürfe, sofern die Arbeitnehmer vorab über die Möglichkeit allfälliger Überwachungsmassnahmen informiert werden. Die Entscheidung

unterstreicht, dass bei Zugriffen auf das Postfach stets der vorherigen Informationspflicht nachgekommen werden sollte.

Auflösung des Arbeitsverhältnisses

Grundsätzlich ist es geboten, die Daten nach Beendigung des Arbeitsverhältnisses aufgrund des Zweckentfalls30 oder gemäss des Grundsatzes der Datenminimierung zu löschen - es sei denn es gelten gesetzlich vorgeschriebene Aufbewahrungspflichten. Persönliche Daten wie Eignungstests, Qualifikationsberichte und psychologische Tests, die nicht mehr zweckdienlich sind und somit nicht mehr den Anforderungen aus Art. 5 Abs. 1 lit. c DSGVO genügen, sind umgehend zu vernichten.

Etwas anderes gilt bei Daten, die aufgrund einer gesetzlichen Pflicht aufbewahrt werden müssen oder bei denen, deren Aufbewahrung im Interesse der Angestellten liegt. Im Regelfall sollten aufbewahrungspflichtige Daten mit einer Frist von fünf Jahren gespeichert werden, die – wenn das Gesetz dies vorsieht – auf zehn Jahre verlängert werden kann. Dafür sollten klare Löschkonzepte eingeführt werden, um der Speicherbegrenzung nach Art. 5 (1) lit. e DSGVO nachzukommen. Ein solches Löschkonzept stellt durch technische und organisatorische Massnahmen sicher, dass nach Beendigung der rechtskonformen Datenverarbeitungsaktivität die Löschung der Daten auch tatsächlich erfolgt.

Wichtig ist, dass bei der Verarbeitung im gesamten Zyklus, gegen externe als auch gegen interne Gefahren, technische und organisatorische Massnahmen gem. Art. 32 DSGVO ergriffen werden, um ein angemessenes Schutzniveau zu gewährleisten. Dies ist ein elementarer Schritt, damit es nicht zu einer unbefugten Einsichtnahme, unzulässigen Verarbeitung oder sonstigen «Datenpanne » gemäss Art. 4 Nr. 12 DSGVO kommt. Es ist essenziell, dass passende Zugriffsberechtigungen etabliert sind oder dass die Kommunikation verschlüsselt erfolgt. Es empfiehlt sich, Identity and Access Management-Lösungen wie Zeitzertifikate einzurichten, um sicherzustellen, dass kein Unberechtigter Zugriff auf die Daten hat. Die DSGVO stärkt die Betroffenenrechte und verpflichtet die Verantwortlichen zur umfassenden Auskunftserteilung, welche dem Angestellten zustehen. Unternehmen sollten sich also nicht nur auf vermehrte Anfragen von Kunden, sondern auch auf Fragen der eigenen Mitarbeiter einstellen.

Fazit

Die Datenverarbeitung im Arbeitsverhältnis ist durch viele Besonderheiten geprägt. Als Faustregel kann gesagt werden, dass sich bei jedem Vorhaben die allgemeinen Datenschutzprinzipien wie ein roter Faden durch die Verarbeitungsaktivitäten ziehen sollten. Diese bieten jedem Verarbeiter einen zuverlässigen Anhaltspunkt. Wenn sie richtig angewendet werden, verringert man das Risiko einer unrechtmässigen Datenverarbeitung. Als Arbeitgeber gilt es darauf zu achten, dass dies im Rahmen der Verhältnismässigkeit vonstatten geht. Wenn tatsächlich auf die Erhebung mittels Einsatzes einer bestimmten Massnahme nicht verzichtet werden kann und dafür ein legitimer Grund vorliegt, sollte man besonders auf die Datensparsamkeit achten. Nur wenn das Vorhaben tatsächlich erforderlich ist für den jeweiligen angestrebten Zweck und keine alternativen, milderen Möglichkeiten ersichtlich sind, sollte die Massnahme ergriffen werden. Es ist davon auszugehen, dass in näherer Zukunft mehr behördliche Informationen zum Thema Beschäftigtendatenschutz verfügbar sind.

Quelle:
Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. (www.bvdnet.de)