DIE DIGITALISIERUNG VON HR-PROZESSEN ZUM ZEIT- UND KOSTENVORTEIL MACHEN

IMPULSE FÜR DIE PROFESSIONALISIERUNG DER PERSONALARBEIT

Bild: ©Piscine26 - stock.adobe.com

FOKUS: WAS BISHER GESCHAH

Die in Papierform vorhandenen Personalakten werden oft von einem Dienstleister eingescannt und im Anschluss zurückgegeben. Die digitale Personalakte befindet sich somit – genau wie die Stamm- und Abrechnungsdaten der Mitarbeiter – im HR-System. Nach dem Scanprozess wird eine Qualitätskontrolle durch das Personalmanagement vorgenommen. Die Mitarbeiter erhalten sodann Gelegenheit, Einsicht in ihre Papierakte zu nehmen, und im Anschluss sollen die Papierunterlagen vernichtet werden, um Medienbrüche zu vermeiden.

MBA Dipl.-Ing. Raschid Bouabba,
Geschäftsführer der MCGB GmbH
Unternehmensberatung,
www.mcgb.de

rauszugeben ist, selbst wenn dies für das betroffene Unternehmen einen enormen Aufwand darstellt.

Vom Auskunftsrecht erfasst sind Namen, Adressen und Kontaktdaten sowie eine Vielzahl weiterer Daten. Kopien von Daten, die nicht selbsterklärend sind (beispielsweise Codes oder „Rohdaten"), müssten der auskunftssuchenden Person in jedem Fall verständlich und nachvollziehbar erläutert werden. Um in der Lage zu sein, unverzüglich und im Regelfall spätestens innerhalb eines Monats ordnungsgemäß Auskunft zu erteilen, müssen sich nach Auffassung der

Die Zeit drängt, und die Digitalisierung schreitet unaufhaltsam voran. Es gilt, die Personalarbeit insgesamt zu professionalisieren und an die Erfordernisse der digitalen Arbeitswelt heranzuführen. Gleichzeitig müssen Wirtschaftlichkeit (Effizienz) und Wirksamkeit (Effektivität) bei der Durchführung personalwirtschaftlicher Maßnahmen erhöht werden.

Es stellt sich nun für eine revisionssichere Archivierung die Frage, welche Papierunterlagen trotz Digitalisierung im Unternehmen aufbewahrt werden müssen. Die verschiedenen gesetzlichen Bestimmungen lassen nicht einheitlich erkennen, welche Unterlagen das im Einzelnen sind und welche gesetzlichen Anforderungen zu erfüllen sind.

Weiterhin steht die Frage im Raum, wie lange Papierunterlagen, die nicht vernichtet werden dürfen, im Unternehmen aufbewahrt werden müssen. Dies dient der Beweisführung durch schriftliche Verfassung von Vereinbarungen, einseitigen Wissens- oder Willenserklärungen, um auch für die Zukunft die Gewissheit zu haben, einen Sachverhalt im Rechtsstreit jederzeit nachweisen zu können. Leider existiert häufig keine einheitliche Verfahrensbeschreibung für alle Unternehmen.

FOKUS: AUSKUNFTSMANAGEMENT

Die neuen Leitlinien des Europäischen Datenschutzausschusses zum Auskunftsrecht (EDSA) erfordern eine Überprüfung interner Prozesse und Dokumentationen zum Datenschutz im Unternehmen, um Bußgelder und Schadensersatzforderungen wegen unzureichender Auskünfte zu vermeiden. Der EDSA hat daher neue Leitlinien zum Auskunftsrecht nach der Datenschutz-Grundverordnung (DS-GVO) veröffentlicht. Darin formulieren die Aufsichtsbehörden strenge Anforderungen an die Erteilung von datenschutzrechtlichen Auskünften. Vor allem zementieren diese neuen Leitlinien die von den Aufsichtsbehörden schon bislang und mehrheitlich vertretene strenge Linie, wonach bei Auskünften grundsätzlich auch eine Kopie sämtlicher personenbezogener Daten he-

EDSA die Unternehmen proaktiv auf die zu erwartenden Auskunftsersuchen vorbereiten und die notwendigen internen Prozesse hierfür schaffen.

FOKUS: GESETZLICHE AUFBEWAHRUNGSPFLICHTEN

Die historisch gewachsenen Aufbewahrungsfristen unterscheiden sich in den für das Personalmanagement relevanten Bereichen doch sehr deutlich. So gelten im Arbeitsrecht, im Steuerrecht, im Sozialversicherungsrecht oder im Recht der betrieblichen Altersversorgung erhebliche Unterschiede, und dies schafft große Unsicherheiten bei der Digitalisierung. All dies wird deutlich, wenn durch die gesetzlichen Vorschriften (EU-DS-GVO, BDSG etc.) die Vorgaben zur Erstellung eines Verfahrensverzeichnisses in die betriebliche Praxis umgesetzt werden.

Gleichwohl kann die Verletzung von Aufbewahrungspflichten straf- und berufsrechtliche, aber auch prozessuale Konsequenzen haben. Beispiele finden sich etwa in der Verletzung der handelsrechtlichen Buchführungspflicht, denn dies kann eine Insolvenzstraftat nach §§ 283 ff. StGB darstellen.

FOKUS: BEWEISFÜHRUNG UND URKUNDEN

Auch wenn es für die Wirksamkeit eines Arbeitsvertrags nicht auf die Schriftform ankommt, so gilt das nicht in allen Fällen. In diesem Zusammenhang ist darauf zu achten, dass weiterhin für die Wirksamkeit einer Befristung gem. § 8 Abs. 5 Satz 1 TzBfG die Schriftform gesetzlich vorgeschrieben ist. Das gilt gleichermaßen gem. § 626 BGB für die Beendigung von Arbeitsverträgen durch Kündigung oder einen Aufhebungsvertrag. Eine elektronische Signatur kann dies in den genannten Fällen derzeit noch nicht ersetzen. In Streitfällen vor Gericht ist dies nachzuweisen. Hier gilt gem. § 427 ZPO der Inhalt der Abschrift einer Urkunde als bewiesen, wenn der Gegner der Anordnung, die in seinen Händen befindliche Urkunde vorzulegen, nicht nachgekommen ist.

Die (Papier-)Urkunde ist das sicherste Beweismittel, da das Gericht, sofern die Echtheit der Unterschrift feststeht, hinsichtlich der Bestimmung des Beweiswerts des Dokuments Beweisregeln unterliegt. Elektronische Dokumente mit qualifizierter Signatur sind Urkunden gleichgestellt. Nicht signierte elektronische Dokumente können ebenfalls in einen Prozess als Beweismittel eingeführt werden; das Gericht ist allerdings in seiner Beweiswürdigung frei. Sofern die Echtheit des Dokuments strittig ist, muss der Beweispflichtige weiterführende Nachweise erbringen. Ob dies gelingt, hängt von den konkreten Umständen ab und dürfte bei ungesicherten Dokumenten schwierig sein.

FOKUS: DATENSCHUTZ-COMPLIANCE

In vielen Geschäftsprozessen und IT-Anwendungen werden personenbezogene Daten verwendet. Diese unterliegen den Bestimmungen des Datenschutzes, welche unter anderem fordern, die Prinzipien der

Erforderlichkeit, Datenvermeidung und Datensparsamkeit im Umgang mit zu beachten und auch eine Löschung derartiger Daten zu gewährleisten.

Zu den einschlägigen datenschutzrechtlichen Vorschriften zählen etwa Gesetze oder Verordnungen (Betriebs- oder Dienstvereinbarungen), auf deren Grundlage personenbezogene Daten erhoben, verwendet und gelöscht werden müssen. Daher ist im Löschkonzept festzulegen, wie die datenschutzrechtlichen Pflichten zur Löschung erfüllt werden. Löschprotokolle dienen als Nachweis der fristgerechten Löschung personenbezogener Daten dar.

FOKUS: HAFTUNG BEI DATENSCHUTZVERSTÖSSEN

Die Frequenz neuer Verfahren und Urteile zu immateriellen Schadensersatzansprüchen im Datenschutzrecht steigt stetig an. Für Unternehmen war das Risiko, nach einem Datenschutzverstoß von Betroffenen zivilrechtlich in Anspruch genommen zu werden, noch nie so groß wie heute. Diese Entwicklung wird verstärkt durch die Medienberichterstattung. Dadurch wird eine breite Öffentlichkeit auf mögliche Datenschutzverstöße aufmerksam gemacht.

Die rechtlichen und tatsächlichen Entwicklungen lassen schon jetzt erkennen, dass sich Unternehmen absehbar mit einer Zunahme von Schadensersatzforderungen konfrontiert sehen werden – und dies reicht bis hin zu Massenverfahren. Diese private Rechtsdurchsetzung (sogenannte „Private Enforcement“) ergänzt zunehmend die behördliche Durchsetzung des Datenschutzrechts und verleiht dem Datenschutzrecht als Compliance-Thema insofern mehr Gewicht.

Nach Art. 82 Abs. 1 DS-GVO können Personen, die einen immateriellen Schaden durch einen Datenschutzverstoß erleiden, Schadensersatz verlangen. Wann ein immaterieller Schaden entsteht und in welcher Höhe Ersatz zu leisten ist, ist bisher nicht höchstrichterlich geklärt. Da die Anspruchsgrundlage aus dem Unionsrecht stammt, ist sie unionsrechtskonform auszulegen.

Die Rechtsprechung zu anderen im deutschen Recht vorgesehenen immateriellen Schadensersatzansprüchen ist daher nicht unmittelbar anzuwenden. Nach Inkrafttreten der DS-GVO haben zunächst offene Rechtsfragen und die traditionell restriktive Haltung deutscher Gerichte zu immateriellen Schäden dafür gesorgt, dass die Schadensersatzansprüche wegen Datenschutzverletzungen in der Vergangenheit eher selten durchgesetzt wurden.

Doch zu Beginn des Jahres 2021 hat das Bundesverfassungsgericht einigen Argumenten,

mit denen Gerichte Schadensersatzansprüche wegen Datenschutzverletzungen bisher leicht ablehnen konnten, einen Riegel vorgeschoben. In der Folge etabliert sich in Deutschland nun zunehmend eine klägerfreundliche Rechtsprechung. Urteile, die mitunter Schadensersatzsummen von bis zu 5.000 Euro pro Schadensfall zusprechen, ermutigen immer mehr Personen dazu, nach Datenschutzverstößen Schadensersatzansprüche geltend zu machen.

Zur Klärung offener Rechtsfragen zum „immateriellen Schaden" im Sinne des Art. 82 DS-GVO sind bereits mehrere Entscheidungsersuchen deutscher Gerichte beim Europäischen Gerichtshof (EuGH) anhängig. Die zu erwartende klarstellende Rechtsprechung durch den EuGH hat das Potenzial, den Startschuss für eine massenhafte Geltendmachung von Schadenersatzforderungen wegen vermuteter Datenschutzverstöße zu setzen.

FOKUS: SCHADENSERSATZ-MANAGEMENT

Bei Verstößen gegen Auskunftspflichten drohen einerseits behördliche Maßnahmen und empfindliche Bußgelder. So hat beispielsweise die Hessische Datenschutzbehörde in ihrem Tätigkeitsbericht für das Jahr 2020 Verstöße gegen Auskunftspflichten mit Bußgeldern im mittleren fünfstelligen Bereich geahndet. Die strengen Vorgaben der Aufsichtsbehörden dürften allerdings auch den aktuell zu beobachtenden Entwicklungen im Hinblick auf Schadenersatzforderungen im Datenschutzrecht weiter Vorschub leisten.

Für Verstöße gegen die Auskunftspflicht hat beispielsweise das Landesarbeitsgericht Hamm jüngst in einem Fall immateriellen Schadensersatz in Höhe von 1.000 Euro zugesprochen. Das Arbeitsgericht Düsseldorf erkannte für eine verspätete Auskunft sogar immateriellen Schadensersatz in Höhe von 5.000 Euro zu. Diese Entwicklung dürfte immer mehr Personen dazu ermutigen, auch bei Verstößen gegen Auskunftspflichten Schadensersatzansprüche geltend zu machen.

FOKUS: REVISIONSSICHERE DATENVERARBEITUNGSPROZESSE

Es ist notwendig, die internen Prozesse sowie die Dokumentation zum Datenschutz im Unternehmen auch vor dem Hintergrund der oben erwähnten neuen Leitlinien des EDSA sorgfältig zu prüfen und im Bedarfsfall anzupassen. Vor allem Vorgaben (Richtlinien, Leitfäden, Checklisten) zur Handhabung von Datenschutzanfragen sowie Standardvorlagen für die Auskunftserteilung sollten einer Überprüfung unterzogen werden, um für Auskunftsanfragen gewappnet zu sein. Es ist anzuraten, die vom EDSA formulierten Anforderungen bereits jetzt zu berücksichtigen, zumal die veröffentlichte Fassung der Leitlinien die gemeinsame Linie der europäischen Aufsichtsbehörden wiedergibt.

Für Unternehmen wird es durch die aktuellen Entwicklungen zudem immer wichtiger, sich frühzeitig und strategisch mit den Herausforderungen, Chancen und Risiken der Gerichtsverfahren im Bereich Datenschutz auseinanderzusetzen. Das Datenschutzrecht bildet dabei den Schwerpunkt und die Verbindung zu anderen Bereichen wie den maßgeblichen Verfahrens- und Prozessregelwerken.

FAZIT: PROZESSE IM DIGITALEN WANDEL

Der Übergang vom Papier zum elektronischen Dokument schreitet schnell voran. Die elektronische Abwicklung von Geschäftsprozessen resultiert vor allem in Zeit- und Kostenvorteilen. Einsatzfelder für Digitalisierungsmöglichkeiten im Personalmanagement sind Personalauswahl, Personalentwicklung, betriebliches Gesundheitsmanagement, Zeitmanagement sowie die Personaleinsatzsteuerung. Nachholbedarf besteht in vielen Unternehmen und insbesondere bei zunehmender Teilzeitarbeit sowie wachsenden Flexibilitätserfordernissen. ■