Februar 2018 | 02

Schwerpunkt Compliance – gute Vorsätze für 2018?

Arbeitsrecht – gut zu wissen …

Unternehmen müssen sich bis 25. Mai 2018 an die EU-Datenschutzgrundverordnung anpassen.

Das Thema Datenschutz wird vom Mauerblümchen zu einem der zentralen Compliance-Themen für Unternehmen: Ab dem 25. Mai 2018 drohen bei Verstößen gegen datenschutzrechtliche Vorgaben Bußgelder bis zu EUR 20 Mio. oder 4 % des Jahresumsatzes der Unternehmensgruppe, wobei der jeweils höhere Betrag gilt. Im Gegensatz dazu sieht das derzeitige Bundesdatenschutzgesetz Bußgelder von maximal EUR 300.000 vor. Trotzdem ist die Bereitschaft in vielen Unternehmen noch gering, sich mit den anstehenden Neuerungen zu befassen.

Wir zeigen Ihnen, welche guten Vorsätze für 2018 Sie bereits jetzt fassen und idealerweise sogleich umsetzen sollten.

Neuregelungen ab dem 25. Mai 2018, Haftungsrisiko, Beweislastumkehr

Die EU-Datenschutzgrundverordnung (DSGVO) ist ab dem 25. Mai 2018 ohne weiteren nationalen Umsetzungsakt zwingend anwendbar und überlagert das nationale Recht. Es gibt keine Übergangsfrist nach dem 25. Mai 2018.

Auch das bislang geltende Bundesdatenschutzgesetz (BDSG) wird ersetzt, der deutsche Gesetzgeber hat zwischenzeitlich unter Berücksichtigung der DSGVO ein neues BDSG (BDSG-neu) beschlossen, das gleichzeitig mit der DSGVO am 25. Mai 2018 in Kraft tritt. Im BDSG- neu finden sich insbesondere Regelungen zum Beschäftigtendatenschutz, den die DSGVO dem nationalen Gesetzgeber überlässt.

Die europäische Datenschutzlandschaft wird durch die Neuregelungen in ihrer Struktur erhalten, allerdings kommen auch einige grundlegend neue Verpflichtungen hinzu. Diese werden flankiert von einem gesteigerten Haftungsrisiko für Unternehmen, wozu nicht nur der drastisch erhöhte Bußgeldrahmen gehört (Art. 83 DSGVO). Neu ist auch, dass neben staatlich verhängten Bußgeldern und einem zivilrechtlichen Schadensersatzanspruch ein Anspruch auf Schmerzensgeld im Fall von Datenschutzverstößen in Betracht kommt (Art. 82 DSGVO). Besonders praxisrelevant ist die Beweislastumkehr: Das Unternehmen wird nur dann von der Haftung befreit, wenn es nachweist, "in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich" zu sein (Art. 82 Abs. 3 DSGVO).

Sämtliche Unternehmen sind betroffen

Die Neuregelungen gelten für alle Unternehmen, die auf dem europäischen Markt tätig sind.

Besondere Herausforderungen ergeben sich für Unternehmen, die dem Datenschutz bisher keinen hohen Stellenwert beigemessen haben. Diese müssen nun bis zum 25. Mai 2018 eine vollständig neue Datenschutzarchitektur implementieren, was erhebliche Ressourcen und eine monatelange Vorbereitung erfordert. Hier muss nun schnell gehandelt werden.

Die deutschen Aufsichtsbehörden haben zwar erklärt, im Rahmen ihrer Kapazitäten Hilfe zu leisten, zugleich haben sie aber darauf hingewiesen, dass sie "nicht davor zurückschrecken, bei festgestellten Verstößen wirksame, verhältnismäßige und abschreckende Sanktionen auszusprechen, wie es die Datenschutz-Grundverordnung von uns verlangt" (Thomas Kranig, Präsident des Bayerischen Landesamts für Datenschutzaufsicht, BayLDA).

Orientierungshilfe

Nachfolgend stellen wir anhand eines Fragenkataloges ausgewählte Aspekte dar, auf die Arbeitgeber in Zukunft achten müssen. Die Fragen lehnen sich an den allgemeinen Fragebogen des BayLDA an. Diese Aufsichtsbehörde hat vor kurzem ausgewählte Unternehmen angeschrieben, um mit 50 Fragen "ein Gefühl darüber zu vermitteln, wie das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) beabsichtigt, ab Mai 2018 einen Teil der zu verstärkenden Prüfaktivitäten zu gestalten". Antworten enthielt der Fragebogen nicht.

Ist Datenschutz "Chefsache"?

Die Aufsichtsbehörden weisen zu Recht darauf hin, dass sich alle Entscheidungsträger in einem Unternehmen der Auswirkungen der Neuregelungen bewusst sein sollten und dass sie wissen sollten, was diese für den alltäglichen Betrieb in ihrem Unternehmen bedeuten. Die erforderlichen Prozesse können nicht nur in Teilbereichen aufgesetzt werden, sondern bedürfen einer übergreifenden Organisationsstruktur.

Wichtig ist, dass grundsätzlich die Unternehmensleitung hierfür rechtlich verantwortlich ist und nicht etwa der Datenschutzbeauftragte. Sollte die Unternehmensleitung noch nicht (ausreichend) informiert sein, ist dies deshalb sobald wie möglich nachzuholen.

Zudem haften insbesondere Geschäftsführer und Vorstände unter Umständen auch mit ihrem Privatvermögen. Datenschutz ist somit eindeutig "Chefsache".

Gibt es einen Datenschutzbeauftragten?

Nach Art. 37 Abs. 1 DSGVO muss ein Datenschutzbeauftragter insbesondere dann benannt werden, wenn das Unternehmen mit seiner Kerntätigkeit entweder durch die von ihm durchgeführten Datenverarbeitungsvorgänge Personen regelmäßig überwacht oder wenn als Kerntätigkeit sensitive Daten verarbeitet werden. Auf eine Mindestanzahl von Beschäftigten kommt es dabei nicht an. Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen (Art. 37 Abs. 7 DSGVO).

Das BDSG-neu geht über die Anforderungen der DSGVO hinaus. In Deutschland ist ein Datenschutzbeauftragter zu benennen, wenn ein Unternehmen in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt.

Beispiel: In der Personalabteilung sind fünf HR-Manager tätig, die Personalakten auch auf dem Server speichern. Sechs Vertriebsmitarbeiter bearbeiten elektronische Kundendatenbanken.

Wird in Deutschland ein Arbeitnehmer zum Datenschutzbeauftragten benannt, genießt er - vergleichbar einem Betriebsratsmitglied - Sonderkündigungsschutz. Das gilt allerdings nur, wenn die Benennung gesetzlich vorgegeben ist (§ 38 Abs. 2 i. V. m. § 6 Abs. 4 BDSG-neu).

Den Aufgabenkreis des Datenschutzbeauftragten erweitert die DSGVO. Er hat jetzt u. a. die Einhaltung der datenschutzrechtlichen Vorschriften zu überwachen (Art. 39 Abs. 1b) DSGVO). Die neue Überwachungspflicht hat in der Literatur die Frage aufgeworfen, ob dadurch - wie beim Compliance-Officer - eine Garantenpflicht und eine eigenständige Haftung begründet wird. Nach (unverbindlicher) Ansicht einiger Aufsichtsbehörden soll das nicht der Fall sein.

Ist sichergestellt, dass sämtliche Prozesse im Zusammenhang mit der Verarbeitung personenbezogener Daten von einer Rechtsgrundlage gedeckt sind?

Die Antwort darauf kann sich in der Praxis als sehr schwierig erweisen - insbesondere wenn die Frage erstmals gestellt wird. Es gibt keine allgemeingültige Rechtsgrundlage, die sämtliche Prozesse im Zusammenhang mit dem Beschäftigungsverhältnis abdeckt. Es hat eine Einzelfallbetrachtung zu erfolgen, wobei Anknüpfungspunkt der jeweils verfolgte Zweck der Datenverarbeitung ist.

- Das grundlegende System hat sich nicht geändert

Es bleibt bei dem bisherigen Grundsatz, dass jede Verarbeitung personenbezogener Daten einer Rechtsgrundlage bedarf. Ohne Rechtsgrundlage ist die Verarbeitung unzulässig (sog. Verbot mit Erlaubnisvorbehalt). Personenbezogene Daten sind alle Informatio-

nen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1 DSGVO).

Beispiele: Name, Geburtsdatum, Geschlecht, Familienstand, Anschrift, Kontonummer, Krankheitstage, Konfession, Ausbildung, Qualifikation, Foto, E-Mail-Adresse, IP-Adresse, aktueller Aufenthaltsort.

Gleichermaßen weit gefasst ist der Begriff der Verarbeitung. Darunter fallen "das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung." (Art. 4 Nr. 2 DSGVO). Im Beschäftigungskontext sind aufgrund der deutschen Sonderregelung auch nur in Papierform vorliegende Daten erfasst (§ 26 Abs. 7 BDSG-neu).

Beispiele: Speicherung der Stammdaten (Name, Anschrift, Geburtsdatum etc.), Einblick in die Personalakte, Abrufen von Informationen über die Personalsoftware, Google-Recherche über Bewerber, Mitarbeiterbeurteilungen, Berücksichtigung von Leistungsdaten zur Bonusermittlung, Veröffentlichung von Kontaktdaten auf der firmeneigenen Website, Entfernung einer Abmahnung, Durchführung einer Sozialauswahl, betriebliches Eingliederungsmanagement, Zeiterfassung, Videoaufzeichnungen, Torkontrollen, GPS-Ortung, Einsatz von Computern mit personalisiertem Zugang.

Keine Anwendung finden die Regelungen auf anonyme Informationen, d. h. solche, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen. Gleiches gilt für personenbezogene Daten, die so anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann (Erwägungsgrund 26 der DSGVO). Diese Definition ist sehr eng geworden: Nach der bisherigen Rechtslage (§ 3 Nr. 6 BDSG) reicht es für eine Anonymisierung, wenn die Zuordnung von Daten zu einer Person "nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" erfolgen kann.

- Allgemeine datenschutzrechtliche Rechtsgrundlagen im Bereich des Arbeitsrechts

Im Beschäftigungskontext kommt eine Rechtfertigung nach § 26 BDSG-neu (derzeit: § 32 BDSG) aufgrund einer Betriebsvereinbarung, einer Einwilligung oder auch allgemein gem. Art. 6 DSGVO in Betracht. Besonderheiten bestehen bei einer Übermittlung außerhalb der Unternehmensgrenzen, z. B. an die Muttergesellschaft und / oder in das außereuropäische Ausland.

– Gem. § 26 Abs. 1 BDSG-neu dürfen Daten von Beschäftigten verarbeitet werden, wenn dies für die Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses erforderlich ist. Im Kern sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten gegeneinander abzuwägen (Anwendung des Verhältnismäßigkeitsprinzips).

  Beispiel: Hat das Unternehmen eine freie Stelle ausgeschrieben, darf die Personalabteilung etwa die Kontaktdaten jedes Bewerbers speichern, um eine Absage zu senden oder um zu einem Bewerbungsgespräch einzuladen. Unzulässig wäre, auch die Kommunikationsabteilung die Kontaktdaten des Bewerbers einsehen zu lassen, um dem Bewerber zukünftig Werbung zu senden.

  Die deutsche Neuregelung soll den derzeit geltenden § 32 BDSG fortführen, einschließlich der dazu ergangenen Rechtsprechung. In der Gesetzesbegründung findet sich zwar der Vorbehalt, Teilbereiche durch weitere Gesetze zu regeln (z. B. Ausschluss heimlicher Kontrollen, Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken), jedoch sollen Neuregelungen nur Grundsätze betreffen, die bereits im Rahmen der Rechtsprechung zum geltenden Recht angelegt sind. Die Grundsatzurteile des Bundesarbeitsgerichts bleiben also relevant.

– Kollektivvereinbarungen wie Tarifverträge und Betriebsvereinbarungen können Rechtsgrundlage für die Verarbeitung personenbezogener Daten der Beschäftigten sein. Das entspricht der bisherigen Rechtsprechung des Bundesarbeitsgerichts und ist nun in § 26 Abs. 4 BDSG-neu ausdrücklich geregelt.

  Beispiel: Das Unternehmen möchte eine Software einführen, die ein Modul für die Personalentwicklung der Mitarbeiter beinhaltet. Einigen sich Arbeitgeber und Betriebsrat in einer Betriebsvereinbarung auf die

Einführung, kann sie (bei entsprechender Ausgestaltung) Rechtgrundlage für die Verarbeitung der Mitarbeiterdaten sein.

Konkrete Anforderungen an die Kollektivvereinbarungen hat der deutsche Gesetzgeber nicht festgelegt, sondern auf Art. 88 Abs. 2 DSGVO verwiesen. Betriebsvereinbarungen müssen somit den - insoweit unscharfen - Vorgaben der DSGVO, wozu insbesondere die Transparenz und die Verhältnismäßigkeit zählen, gerecht werden.

Beispiel: In der Betriebsvereinbarung sind Zweck und beabsichtigte Verwendung der Daten nicht klar geregelt. Die Betriebsvereinbarung eignet sich nicht als Rechtsgrundlage für die Datenverarbeitung.

Ab dem 25. Mai 2018 gelten die Anforderungen sowohl für neue als auch für alte Betriebsvereinbarungen. Es gibt keine Übergangsfristen. Unternehmen sind daher gut beraten, bestehende Betriebsvereinbarungen zu prüfen und bei aktuellen Verhandlungen bereits jetzt die neuen Anforderungen zu berücksichtigen.

– Nach wie vor kann eine Einwilligung Grundlage für eine Datenverarbeitung sein. Voraussetzung ist, dass die Einwilligung freiwillig, für einen bestimmten Fall und in informierter Weise erfolgt. Eine Pauschaleinwilligung für alle denkbaren Sachverhalte ist also - wie bisher - unzulässig. Die Wirksamkeit einer Einwilligung muss nachgewiesen werden können (Art. 7 Nr. 1 DSGVO).

  Während die DSGVO keine besondere Form vorschreibt, muss die Einwilligung nach § 26 Abs. 2 BDSG-neu grundsätzlich schriftlich vorliegen. Außerdem muss der Arbeitnehmer über den Zweck der Datenverarbeitung und sein Widerrufsrecht in Textform (z. B. per E-Mail) aufgeklärt werden.

  Neu ist die Klarstellung, dass auch im Arbeitsverhältnis freiwillige Einwilligungen grundsätzlich möglich sind. Das Gesetz nennt Indizien für eine Freiwilligkeit, etwa wenn dem Arbeitnehmer ein wirtschaftlicher Vorteil gewährt wird, wie es z. B. bei Gestattung der privaten Nutzung von IT der Fall ist.

  Beispiel: Das Unternehmen erlaubt Arbeitnehmern die private Nutzung des Internets. Die Arbeitnehmer willigen nach ausführlicher Information ein, dass bestimmte Daten (Zeitpunkt der Nutzung, angesteuerte Seiten etc.) zu bestimmten Zwecken (Datensicherheit, Vermeidung von Straftaten) erfasst werden.

  Allerdings ist mit einer Einwilligung im Beschäftigungskontext auch zukünftig vorsichtig umzugehen. Nicht zuletzt ist sie jederzeit mit Wirkung für die Zukunft widerruflich.

  Beispiel: Eine Mitarbeiterin widerruft ihre zuvor erteilte Einwilligung zur Verarbeitung ihrer Daten im Rahmen einer neuen Softwarelösung zur Persönlichkeitsanalyse. Das Unternehmen benötigt für die weitere Verarbeitung eine alternative Rechtsgrundlage.

  Nach derzeitiger Ansicht der Aufsichtsbehörden gelten in der Vergangenheit wirksam erteilte Einwilligungen fort, sofern diese unter der bestehenden Rechtslage wirksam erteilt wurden, freiwillig (nach Maßgabe der DSGVO) erfolgten und die Altersgrenze von 16 Jahren beachten (Beschluss des Düsseldorfer Kreises vom 13./ 14. September 2016). Für viele Unternehmen bedeutet das aber keinen Grund zum Aufatmen: Häufig sind Einwilligungserklärungen bereits nach geltendem Recht unwirksam (z. B. Pauschalregelung im Arbeitsvertrag). Es sollte also darauf geachtet werden, dass möglichst noch eine weitere Rechtsgrundlage für die Verarbeitung zur Verfügung steht.

– Eine Rechtfertigung kann auch nach der allgemeinen Regelung des Art. 6 Abs. 1 DSGVO in Betracht kommen, etwa zur Erfüllung einer rechtlichen Pflicht oder wenn die Verarbeitung zur Wahrung der berechtigten Interessen des Unternehmens / eines Dritten erforderlich ist und diese die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

  Beispiel: Übermittlung von Beschäftigtendaten im Rahmen eines Unternehmenskaufs an den Erwerber noch vor Wechsel der Arbeitgeberstellung.

– Trotz gesellschaftsrechtlicher und wirtschaftlicher Verbundenheit werden Konzerngesellschaf-

ten datenschutzrechtlich weiterhin wie Externe behandelt. Die Tochtergesellschaft, bei der ein Arbeitnehmer angestellt ist, darf dessen Daten also nicht ohne Weiteres an die Muttergesellschaft weitergeben. Notwendig ist eine der bereits genannten Rechtsgrundlagen (Betriebsvereinbarung, Einwilligung, Art. 6 DSGVO) oder eine vertraglich vereinbarte Auftragsverarbeitung, für die Art. 28 DSGVO strenge Anforderungen stellt.

Immerhin gibt es eine als "kleines Konzernprivileg" bezeichnete Erleichterung: Die Verarbeitung "für interne Verwaltungszwecke" ist ausweislich des Erwägungsgrunds 48 zur DSGVO als berechtigtes Interesse anerkannt, sodass bei entsprechendem Zweck die Interessenabwägung häufig zugunsten der Konzernunternehmen ausfallen dürfte.

– Für die Übermittlung in das außereuropäische Ausland sind - zusätzlich zur grundsätzlichen Verarbeitungserlaubnis (Rechtsnorm, Betriebsvereinbarung, Einwilligung) - weitergehende Voraussetzungen zu erfüllen (Art. 44 ff. DSGVO).

Weitgehend unproblematisch ist die Übermittlung in ein Drittland, dem die EU-Kommission ein angemessenes Schutzniveau bescheinigt hat. Da die bisher ergangenen Angemessenheitsbeschlüsse fortgelten (Art. 46 Abs. 5 S. 2 DSGVO), gelten Andorra, Argentinien, Färöer-Inseln, Guernsey, Isle of Man, Israel, Jersey, Kanada, Neuseeland, Schweiz und Uruguay weiterhin als "datenschutzrechtlich sichere Drittstaaten".

Beispiel: Die Konzernzentrale sitzt in Kanada. Die deutsche Tochtergesellschaft hat ihr einen Fernzugriff auf bestimmte (nicht sensible) Personaldaten eingerichtet. Die Übermittlung in den "sicheren Drittstaat" Kanada ist unproblematisch (1. Prüfungsstufe). Zu prüfen bleibt aber - ebenso wie bei einer Übermittlung innerhalb Deutschlands - ob die Verarbeitung (Bereitstellung) als solche gerechtfertigt ist (2. Prüfungsstufe), etwa nach Art. 6 Abs. 1 f) DSGVO i. V. m. Erwägungsgrund 48, wenn der Zweck z. B. der Aufbau einer konzernweiten Skill-Datenbank ist.

Für den EU-US Privacy Shield hat die Kommission die Angemessenheit des Datenschutzniveaus festgestellt, was allerdings auf mitunter heftige Kritik gestoßen ist.

Zulässig ist eine Übermittlung auch aufgrund verbindlicher Vereinbarung der EU-Standardklauseln, die ebenfalls fortgelten (Art. 46 Abs. 5 S. 2 DSGVO). Bei unveränderter Verwendung der Klauseln ist die Übermittlung genehmigungsfrei. Ferner können Übermittlungen auf - allerdings jeweils von der Aufsichtsbehörde vorab zu genehmigende - verbindliche interne Datenschutzvorschriften (Binding Corporate Rules), Verhaltensregelungen (Codes of Conduct), Zertifizierungen und einzeln ausgehandelte Vertragsklauseln gestützt werden.

Eine wirksame Einwilligung in die Datenübermittlung in ein Drittland ist ebenfalls möglich. Schließlich kann die Übermittlung in - regelmäßig eng auszulegenden - Sonderfällen legitimiert sein, wie z. B. bei Erforderlichkeit zur Vertragserfüllung oder bei Verfolgung von Rechtsansprüchen.

Wichtig ist, dass es bei einer Änderung des Zwecks der Datenverarbeitung ggf. einer anderen Rechtsgrundlage bedarf. Eine mit dem ursprünglichen Zweck unvereinbare Verarbeitung ist unzulässig (Art. 5 Abs. 1b) DSGVO).

Sind die Verarbeitungstätigkeiten bekannt und werden diese dokumentiert bzw. ist dies kurzfristig möglich?

Vergleichbar dem bisherigen (internen) Verfahrensverzeichnis (vgl. §§ 4g Abs. 2, 4e BDSG) sind Verarbeitungstätigkeiten nach Art. 30 DSGVO in einem Verzeichnis zu erfassen. Das Verzeichnis muss u. a.

– den Namen und die Kontaktdaten des / der Verantwortlichen einschließlich des Vertreters sowie eines etwaigen Datenschutzbeauftragten,
– die Zwecke der Verarbeitung,
– eine Beschreibung der Kategorien betroffener Personen und der
– Kategorien personenbezogener Daten,
– die Kategorien von Empfängern (in Drittländern),
– etwaige Übermittlungen an ein Drittland,
– möglichst die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien und

- möglichst eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (gem. Art. 32 Abs. 1 DSGVO) enthalten.

Die Aufsichtsbehörden haben entsprechende Muster angekündigt.

Eine Ausnahme gilt für Unternehmen mit weniger als 250 Mitarbeitern: Sie müssen kein Verzeichnis führen, es sei denn die Verarbeitung

- birgt ein Risiko für Rechte und Freiheiten der Betroffenen,
- erfolgt nicht nur gelegentlich oder
- betrifft besonders sensitive Daten (z. B. Gesundheit, Herkunft, Gewerkschaftszugehörigkeit).

Die Relevanz der Ausnahme dürfte in der Praxis gering sein. Nach Ansicht der nationalen Aufsichtsbehörden erfolgt insbesondere die regelmäßige Verarbeitung von Beschäftigtendaten "nicht nur gelegentlich".

Das Verzeichnis, das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, ist ein Baustein, um der Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO zu genügen: Wer Daten verarbeitet, muss nachweisen können, dass er die strengen Grundsätze über die Datenverarbeitung aus Art. 5 Abs. 1 DSGVO einhält.

Die Aufsichtsbehörden weisen mit Recht darauf hin, dass das Verzeichnis eine wesentliche Rolle spielen wird: Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherzustellen. Es ist daher dringend anzuraten, das Verzeichnis bis zum 25. Mai 2018 zu erstellen oder - falls bereits eines geführt wird - zu überarbeiten.

Ist bekannt, wie und in welchen Fällen eine Datenschutz-Folgenabschätzung durchzuführen ist?

Art. 35 DSGVO sieht eine Pflicht zu einer sog. Datenschutz-Folgenabschätzung vor, wenn die Form der Verarbeitung - insbesondere bei Verwendung neuer Technologien - voraussichtlich ein "hohes Risiko" für die Rechte und Freiheiten natürlicher Personen zur Folge hat. In diesem Fall sind u. a. das Verfahren, die Zwecke und die berechtigten Interessen zu beschreiben. Die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung, Risiken für Betroffene und geplante Schutzmaßnahmen einschließlich des Nachweises der Wirksamkeit sind darzustellen.

Wann ein "hohes Risiko" für Rechte und Freiheiten natürlicher Personen besteht, ist nicht abschließend geregelt. Art. 35 Abs. 3 DSGVO nennt beispielhafte Fallgruppen, u. a. die systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen mittels automatisierter Verarbeitung, die als Grundlage einer bestimmten Entscheidung dient.

Beispiele: Erfasst sein können Profiling, Assessmentverfahren, Beförderungsranglisten, Skill-Datenbanken, Big-Data-Applikationen (sofern nicht nur aggregierte Daten verarbeitet werden).

Es ist vorgesehen, dass die Aufsichtsbehörden Positiv-/Negativlisten erstellen, wann eine Datenschutz-Folgenabschätzung erforderlich ist bzw. unterbleiben kann (Abs. 4, 5). Solche Listen gibt es bisher nicht. Die Artikel- 29-Datenschutzgruppe hat aber in einer Stellungnahme (WP 248) einen ersten Kriterienkatalog aufgestellt. Danach muss ein Unternehmen insbesondere bei der Überwachung der Aktivitäten von Arbeitnehmern einschließlich der Überwachung des Arbeitsorts vorab eine Datenschutz-Folgenabschätzung durchführen.

Die Aufsichtsbehörde ist einzuschalten, wenn die geplante Verarbeitung ausweislich der Datenschutz-Folgenabschätzung ein hohes Risiko zur Folge hätte und keine Maßnahmen zur Eindämmung dieses Risikos getroffen werden (Art. 36 Abs. 1 DSGVO).

Nach neuem Recht obliegt die Untersuchung dem Verantwortlichen (Unternehmen); lediglich der Rat eines benannten Datenschutzbeauftragten ist bei der Durchführung einzuholen (Art. 35 Abs. 2 DSGVO).

Können die gesteigerten Anforderungen an die Informationspflicht gegenüber den Betroffenen fristgerecht umgesetzt werden?

Das Unternehmen muss die betroffenen Personen (Bewerber, Arbeitnehmer, Leiharbeitnehmer, Auszubildende etc.) über die sie betreffenden Datenverarbeitungsvorgänge informieren. Sofern die Daten bei den Personen direkt erhoben werden, muss das sofort erfolgen (Art. 13 Abs. 1 DSGVO), etwa bei Abschluss des Arbeitsvertrages. Werden die Daten bei Dritten erhoben, muss die Information spätestens innerhalb eines Monats erfolgen (Art. 14 Abs. 3a) DSGVO).

Die Informationspflicht umfasst im Wesentlichen die im Verfahrensverzeichnis zu erfassenden Angaben, insbesondere den Zweck der Verarbeitung und die Kategorien von Empfängern der Daten. Wegen dieser In-

formationspflicht kann ein Verfahrensverzeichnis auch unterhalb des Schwellenwerts von 250 Mitarbeitern zweckmäßig sein.

Zusätzlich zum Zweck ist der betroffenen Person die Rechtsgrundlage der Verarbeitung zu nennen (Art. 13 Abs. 1c) DSGV). Sollen die Daten in ein EU-Drittland übermittelt werden, ist auch dies zu spezifizieren. Es sind also Angaben zu etwaigen Angemessenheitsbeschlüssen der EU- Kommission zu machen (z. B. EU-US Privacy Shield) bzw. die Garantien zu nennen (z. B. Vereinbarung von EU-Standardklauseln, Binding Corporate Rules). Im letztgenannten Fall muss der betroffenen Person die Möglichkeit eröffnet werden, die Garantien in Kopie zu erhalten oder einzusehen. Einmal mehr zeigt sich, dass Unternehmen Datenfluss und Rechtsgrundlagen geklärt haben müssen, da sie anderenfalls die gesetzlichen Pflichten nicht erfüllen können. Weiter mitzuteilen ist die Dauer, für die personenbezogene Daten gespeichert werden, oder es sind jedenfalls die Kriterien für die Festlegung dieser Dauer zu nennen. Ausgangspunkt der Ermittlung ist der Grundsatz, dass personenbezogene Daten zu löschen sind, sobald deren Aufbewahrung für die Erfüllung des vorausgesetzten Zwecks nicht mehr erforderlich ist. Das bedarf wiederum einer Einzelfallbetrachtung. So werden einige Daten bereits nach wenigen Monaten nicht mehr benötigt, z. B. bei abgelehnten Bewerbern im Hinblick auf die kurze Ausschlussfrist des § 15 Abs. 4 AGG. In anderen Fällen können Daten noch nach Jahren relevant sein, z. B. zwei Jahre für Arbeitszeitnachweise (vgl. § 16 Abs. 2 ArbZG) und mindestens fünf Jahre für sozialversicherungsrechtliche Nachweise (vgl. § 28f Abs. 1 i. V. m. § 28 p SGB IV).

Der Verantwortliche hat der betroffenen Person ferner Angaben zu den Rechten auf Auskunft, Berichtigung, Löschung und Beschwerde bei den Aufsichtsbehörden sowie über die Widerruflichkeit einer erteilten Einwilligung zur Verfügung zu stellen. Es ist zudem darüber zu informieren, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte.

Die umfassenden Informationspflichten werden wohl u. a. dazu führen, dass - wie bereits treffend angemerkt wurde - Arbeitsverträge künftig mit einem "Beipackzettel" versehen werden müssen.

Ist sichergestellt, dass jeder Datenschutzverstoß innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden kann?

Derzeit besteht gem. § 42 a BDSG die Pflicht, den Verlust bestimmter sensibler personenbezogener Daten (u. a. zu Bank- oder Kreditkartenkonten) unter bestimmten Voraussetzungen der Aufsichtsbehörde und ggf. auch den Betroffenen zu melden bzw. sogar Anzeigen in Tageszeitungen zu schalten. Verstöße können mit einem Bußgeld geahndet werden.

Beispiel: Ein Mitarbeiter sendet eine E-Mail nebst unverschlüsselter Excel-Tabelle mit Kontodaten von Arbeitnehmern versehentlich an einen unbekannten Dritten.

Die ab dem 25. Mai 2018 anwendbaren Art. 33, 34 DSGVO enthalten noch strengere Vorgaben - bei einer Bußgelddrohung von bis zu EUR 20 Mio. bzw. 4 % des weltweiten Umsatzes. Eine Mitteilung hat grundsätzlich innerhalb von 72 Stunden nach Bekanntwerden an die zuständige Aufsichtsbehörde zu erfolgen. Dabei knüpft die Meldepflicht nicht an die Qualität der Daten an, sondern bezieht sich allgemein auf "personenbezogene Daten". Eine Meldepflicht soll nur entfallen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Allerdings ist zu beachten, dass das Risiko nicht "erheblich" sein muss, sodass eine Meldepflicht grundsätzlich auch bei abhanden gekommenen verschlüsselten Dateien bestehen kann.

Beispiel: Die Personalleiterin verliert einen USB-Stick mit sensiblen Mitarbeiterdaten. Die Daten sind zwar verschlüsselt, die Verschlüsselungstechnik ist aber veraltet.

Es ist dringend anzuraten, Prozesse einzurichten, um Datenverluste möglichst zu unterbinden. Das Grundproblem besteht darin, dass Unternehmen Datenschutzverstöße häufig gar nicht mitbekommen. Daher sollten in Richtlinien / Betriebsvereinbarungen u. a. eine Pflicht zum verschlüsselten Versand sowie Mitteilungspflichten festgelegt werden. Mitarbeiter sollten geschult und sensibilisiert werden.

Ruhe bewahren und handeln!

Die Neuregelungen verlangen Unternehmen einen unbestreitbar hohen Arbeitsaufwand ab. Ein erster Schritt ist die frühzeitige Prüfung, inwieweit Handlungsbedarf besteht. Der nächste - die Umsetzung - darf nicht ausbleiben: Werden die Neuregelungen schlicht ignoriert, kann dies beträchtliche finanzielle Folgen mit sich bringen. Demgegenüber helfen klare Regelungen zu Verantwortlichkeiten und Prozessen sowie das Bewusstsein über die besonderen Datenschutzrisiken dabei, Bußgelder und zivilrechtliche Haftungsansprüche zu vermeiden.

Verantwortlichen ist daher dringend zu raten, eine Projektgruppe einzurichten, die gemeinsam mit externen Experten die Anforderungen der Datenschutzgrundverordnung im Unternehmen implementiert. Dann ist die Frist bis 25. Mai 2018 einzuhalten.

Bei Fragen EU-Datenschutzgrundverordnung stehen wir Ihnen gerne jederzeit zur Verfügung.

Mit freundlichen Grüßen

CMS Deutschland
Geschäftsbereich Arbeitsrecht

C/M/S/ Law-Now™

Law.Tax

Ihr kostenloser juristischer Online-Informationsdienst.

E-Mail-Abodienst für Fachartikel zu vielfältigen juristischen Themen.
cms-lawnow.com

C/M/S/ e-guides

Law.Tax

Ihre juristische Online-Bibliothek.

Profunde internationale Fachrecherche und juristisches Expertenwissen nach Maß.
eguides.cmslegal.com

---

cms.law