IN DIESER AUSGABE:

Newsletter Juli 2022

Datenschutz

Liebe Leserinnen und Leser,

in unserem Newsletter möchten wir Sie konkret auf Themen aufmerksam machen, die in der Praxis immer wieder gern für Fragen oder Verwirrung sorgen. Auch wenn wir an dieser Stelle nur einen kurzen informativen Überblick geben können, stehen wir Ihnen gerne beratend zur Seite.

Ein kleiner Hinweis: aus Platzgründen wird im Folgenden das generische Maskulinum des jeweiligen Begriffs verwendet.

Viel Spaß beim Lesen!

Ihre ANMATHO AG

Betriebsrätemodernisierungsgesetz

Zunächst die gute Nachricht: Der neue Paragraf § 79a BetrVG schafft Klarheit bezüglich der Verantwortung bei der Datenverarbeitung durch den Betriebsrat.

Bisher war unklar, inwieweit der Betriebsrat als verantwortliche Stelle bei der Verarbeitung personenbezogener Daten der im Unternehmen beschäftigten Mitarbeiter galt. Diese Lücke wurde nun durch das am 18. Juni 2021 in Kraft getretene Gesetz geschlossen. Nur noch der Arbeitgeber gilt als Verantwortlicher im Sinne der DS-GVO Art. 4 Nr. 7. Das betrifft auch die Verarbeitung personenbezogenen Daten im Rahmen der Tätigkeit des Betriebsrates.

Geht die Datenverarbeitung durch den Betriebsrat jedoch über seine gesetzlich zugewiesenen Aufgaben hinaus, ist der Arbeitgeber nicht mehr verantwortlich zu machen. Vielmehr können unter Umständen die Mitglieder des Betriebsrats persönlich haften, da dem Betriebsrat als Körperschaft hier die eigenständige Rechtsfähigkeit fehlt.

Um beim heiklen Thema Datenschutz zwischen den verschiedenen Fraktionen zu vermitteln, wurde seitens des Gesetzgebers ein Kooperationsgebot (§ 79a S. 3 BetrVG) eingeführt. Wie diese Zusammenarbeit jedoch konkret aussehen soll, bleibt weiterhin offen. Um diese Lücke zu füllen und hier möglichen Problemen im Vorhinein zu vorzubeugen sind betriebsinterne Vereinbarungen nötig. Ein klar definierter Umgang mit den (gemeinsam) genutzten Daten, wie z.B. deren Verarbeitung oder Speicherfristen, ist hier dringend angebracht.

Auch für den betrieblichen Datenschutzbeauftragten (bDSB) stellen sich in diesem Zusammenhang schwierige Fragen. Aus seiner Berichtspflicht an die höchste Managementebene (Art. 38 Abs. 3 Satz 3 DS-GVO) und seiner Verschwiegenheitspflicht gegenüber dem Arbeitgeber gem. § 79a BetrVG ergibt sich ein potenzieller Konflikt, der durch das neue Betriebsrätemodernisierungsgesetz ungelöst bleibt.

Für weitere Informationen bietet der Deutsche Gewerkschaftsbund (DGB) auf seiner Webseite im Downloadcenter eine Broschüre zum Download .

Verpflichtungserklärungen

Grundsätzlich dürfen die Mitarbeiter des Unternehmens personenbezogene Daten nur auf ausdrückliche Weisung des Verantwortlichen verarbeiten (Artt. 29 und 32 Abs. 4 DS-GVO). Die im Unternehmen angewendeten Verfahrensweisen müssen also durch die Unternehmensleitung z.B. in Form von Richtlinien und Arbeitsanweisungen usw. verbindlich geregelt sein. Natürlich nützen die besten Gesetze und Regelungen nichts, wenn sie bei den Mitarbeitern unbekannt sind oder nicht beachtet werden.

Bei einem Datenschutzverstoß prüfen die Aufsichtsbehörden deshalb auch schon mal, inwieweit die Mitarbeiter angemessen informiert sind und sich zu den datenschutzrechtlichen Verhaltensweisen bekannt haben. Versäumnisse in diesem Bereich können dazu führen, dass Bußgelder gegenüber dem Unternehmen verhängt oder erhöht werden.

Das Unternehmen kann durch eine Vielzahl von Maßnahmen den notwendigen Wissenstand bei den Mitarbeitern herstellen, z.B. durch Informationsveranstaltungen oder Online-Schulungen. Wichtig ist bei all diesen Veranstaltungen, dass eine Dokumentation über Inhalte und die Teilnehmer erstellt wird. Diese Dokumentation kann gegenüber der Aufsichtsbehörde als Nachweis für die durchgeführten Maßnahmen verwendet werden.

Eine weitere wichtige Maßnahme ist es, die Mitarbeiter auf die Datenschutz-Gesetze und die internen Richtlinien hinzuweisen und ausdrücklich auf die Einhaltung und Beachtung zu verpflichten. Gegebenenfalls erhält das Unternehmen damit auch eine vertragliche Grundlage, um bei vorsätzlichen oder fahrlässigen Verhalten arbeitsrechtliche Sanktionen zu verhängen und den Beschäftigten gegebenenfalls mit in Regress für z.B. Geldbußen zu nehmen.

Die Texte der zu beachtenden Gesetze und internen Regelungen sollten für die Beschäftigten im vollen Wortlaut zur Verfügung stehen, z. B. durch Veröffentlichung im Intranet.

Eine Verpflichtungserklärung hinsichtlich der Datenschutz-Regelungen kann natürlich zweckmäßiger Weise auch eingebunden werden in eine allgemeine Vertraulichkeitserklärung des Mitarbeiters gegenüber dem Unternehmen zum Schutz von z.B. Wirtschaftsdaten, Geschäftsgeheimnissen usw.

Eine Verpflichtungserklärung sollte von allen Mitarbeitern abgegeben werden und folgende Inhalte haben:

- Eine kurze Beschreibung / Erklärung des Zwecks der Verpflichtungserklärung
- Die konkrete Benennung der zu beachtenden Regelungen
- Ein Hinweis auf die Risiken für den Beschäftigten bei Nichtbeachten der Regelungen
- Eine konkrete Verpflichtungsklausel
- Die Empfangsbestätigung des Beschäftigten und die Annahme der Verpflichtung durch eigenhändige Unterschrift.

Die Verpflichtungserklärung verliert nach einer gewissen Zeit natürlich ihre Wirkung - auch im rechtlichen Sinne. Eine jährliche Wiederholung der Verpflichtung ist daher ratsam.

Soweit ein Betriebsrat im Unternehmen eingerichtet ist, empfiehlt es sich, zu den Datenschutzthemen eine spezielle Betriebsvereinbarung abzuschließen. Umfang und Regelungsdetails der Verpflichtungserklärung können hier mit aufgenommen werden.

Das Unternehmen muss die Einholung der Verpflichtungserklärungen vollständig sicherstellen und die unterschriebenen Unterlagen z.B. in der Personalakte ablegen. Sollte ein Mitarbeiter sich weigern, die Verpflichtungserklärung abzugeben, bleibt dem Unternehmen nichts anderes übrig: um das eigene Risiko zu begrenzen, müssen dem Mitarbeiter die Zugangsrechte zu personenbezogenen oder anderen schützenswerten Unternehmensdaten entzogen werden.

Einen konkreten Textentwurf für eine mögliche Datenschutz-Verpflichtung finden Sie im ‚Kurzpapier 19 des DSK' (https://www.datenschutzzentrum.de/artikel/1235-Kurzpapier-Nr.-19-Unterrichtung-und-Verpflichtung-von-Beschaeftigten-auf-Beachtung-der-datenschutzrechtlichen-Anforderungen-nach-der-DSGVO.html#extended) .

Behandlung von Datenschutzverletzungen

Nach der europäischen Datenschutzgrundverordnung (DS-GVO) sind die Unternehmen als verantwortliche Stelle verpflichtet, Verletzungen des Schutzes personenbezogener Daten (‚Datenpannen') innerhalb von 72 Std der Aufsichtsbehörde zu melden (Art. 33 DS-GVO). Die Beachtung dieser Meldepflicht wird bei bekannt gewordenen Datenpannen von den Aufsichtsbehörden sehr streng nachverfolgt und bei Missachtung mit Bußgeld geahndet (siehe hierzu auch den ANMATHO Newsletter 06/2022).

In bestimmten Fällen sind außerdem auch die Betroffenen über die Datenpanne und die daraus entstehenden Folgen und persönlichen Risiken zu informieren (Art. 34 DS-GVO).

Datenpannen können ganz verschiedene Ursachen und ganz unterschiedliche Auswirkungen auf Rechte und Freiheiten natürlicher Personen haben. Dabei handelt es sich nicht nur um aufsehenerregende Hackerangriffe auf die großen Datenbestände von z.B. Energieversorgern oder Internetportalen. Beispiele für Datenpannen sind auch

- der im Zug liegen gelassene Laptop mit Kundendaten,
- falsch adressierte Schreiben an Kunden mit vertraulichen Kontodaten,
- der Verkauf / Weiternutzung von alten Festplatten mit ungelöschten Daten der Mitarbeiter,
- die Übermittlung von nicht korrekt gefilterten Datenbeständen an externe Dienstleister,
- die Übermittlung von Daten an Empfänger ohne ausreichende Rechtsgrundlage oder Zweckdefinition.

Insgesamt kann eine Meldung der Datenpannen natürlich nur dann erfolgen, wenn im Unternehmen überhaupt festgestellt wird, dass eine solche eingetreten ist. Neben dem eigentlichen Schutz der Daten durch technische und / oder organisatorische Maßnahmen (wie. z.B. Festplatten-Verschlüsselung bei Laptops) muss das Unternehmen also zusätzliche technische und / oder organisatorische Vorkehrungen treffen, um Datenpannen festzustellen. Hierbei kann es sich z.B. um Protokollverfahren des innerbetrieblichen / externen Datenverkehrs, Verschlussprotokolle des Sicherheitsdienst o.a. handeln.

Datenpannen werden aber nicht nur durch Administratoren oder Sicherheitspersonal festgestellt. Viele Ereignisse passieren viel mehr auf der Ebene von Fachbereichen und den dort Beschäftigten oder werden dort festgestellt. Das Unternehmen muss also unbedingt dafür Sorge tragen, dass auch diese ‚kleinen' Datenpannen zuverlässig an eine zentrale Stelle, z.B. an ein ‚Krisenteam', gemeldet werden. Das Krisenteam wiederum benötigt Handlungsvollmachten, um weitere Schäden umgehend zu verhindern oder einzugrenzen. Die Erforderlichkeit und der Umfang von Meldungen an die Aufsichtsbehörde und / oder die betroffenen Personen müssen durch das Krisenteam entschieden und entsprechend eingeleitet werden können.

Die Handlungsanweisungen für die Beschäftigten und die Regelungen für das Krisenteam müssen verbindlich festgelegt und im Unternehmen – soweit nicht Vertraulichkeitsbeschränkungen bestehen - veröffentlicht werden. Hierfür empfiehlt sich die Erstellung einer entsprechenden Unternehmensrichtlinie zur Behandlung von Datenschutzverstößen. Bei Prüfungen seitens der Aufsichtsbehörden nach dem Eintritt von Datenpannen kann das Unternehmen damit nachweisen, dass geordnete und angemessene Verfahren zur Schadensbehandlung und zu Risikoeingrenzung eingeführt und angewendet werden.

Der Themenumfang bei Datenpannen von personenbezogenen Daten ist zum Teil deckungsgleich mit den IT-Sicherheitsvorfällen, die vom Unternehmen beachtet werden müssen. Auch hierbei handelt es sich um unrechtmäßige Abflüsse, Veränderungen oder Verlust von Daten. Soweit das Unternehmen ein Managementsystem gemäß der Normengruppe ISO 27000 betreibt, können die datenschutzrechtlichen Anforderungen durch Anwendung der Regelungen aus der Norm ISO 27701 weitgehend umgesetzt werden.

Wenn Sie Interesse an weiteren Informationen zu den vorgestellten Themen haben, wenden Sie sich gern an Ihren Datenschutzbeauftragten der ANMATHO AG oder an info@anmatho.de.