BGHP-Betriebsratsberater – Update Arbeitnehmerrecht (5/2017)

Die Datenschutz-Grundverordnung

Ein Beitrag von Martin Fieseler

Die Datenschutz-Grundverordnung

25. Mai 2018: In knapp einem Jahr ist die Datenschutz-Grundverordnung anwendbar, sechs Jahre nachdem das europäische Gesetzgebungsverfahren begann. Die Datenschutz-Grundverordnung löst die zuvor geltende Richtlinie der EU zum Datenschutz aus dem Jahr 1995 ab. Ziel ist die Vereinheitlichung, Modernisierung und Stärkung des Datenschutzes, zugleich aber auch die Entlastung von Unternehmern.

Gleichzeitig mit der Datenschutz-Grundverordnung tritt das neue Bundesdatenschutzgesetz in Kraft, um deutsches Recht anzupassen und das bisherige Bundesdatenschutzgesetz zu ersetzen. Nach dem Bundestag hat dem neuen Bundesdatenschutzgesetz am 12. Mai 2017 auch der Bundesrat zugestimmt. Der Gesetzentwurf ist hier abrufbar. Knapp ein Jahr haben Betriebsräte nun Zeit, sich mit ihren Unternehmen und mit Hilfe ihrer Berater auf die neuen Regelungen einzustellen. Das ist gar nicht so viel Zeit, in Anbetracht des Umfangs der Datenschutz-Grundverordnung mit ihren 99 Artikeln und 173 Erwägungsgründen und des neuen BDSG mit seinen 85 Paragrafen, wobei immerhin rund die Hälfte der Paragrafen des BDSG im Betrieb keine direkte Rolle spielen, weil sie Ordnungs- und Strafverfolgungsbehörden betreffen. Auch in der Datenschutz-Grundverordnung sind nicht alle Artikel gleichermaßen relevant für den Datenschutz im Betrieb. Hinzu kommt aber, dass die Datenschutz-Grundverordnung und das BDSG nebeneinander gelten, länglich formuliert und selbst für Juristen nicht einfach zu verstehen sind. Folgende Fragen stellen sich:

- Was müssen Betriebsräte jetzt tun?

- Was für Auswirkungen hat die Datenschutz-Grundverordnung für bestehende Betriebsvereinbarungen?

- Und was sind nun eigentlich die wichtigsten Änderungen?

1. Was müssen Betriebsräte jetzt tun und was bedeutet die Datenschutz-Grundverordnung für bestehende Betriebsvereinbarungen?

Betriebsräte sollten sich zunächst zeitnah zur Datenschutz-Grundverordnung qualifizieren, da sich die Datenschutzlandschaft tiefgreifend verändert und Datenschutz-Grundverordnung und neues BDSG komplex sind. Zur Qualifizierung sollten sie deshalb auch für ein entsprechendes Seminar Zeit einplanen. Noch sind auch die Beteiligten auf der Arbeitgeberseite nicht umfassend mit Datenschutz-Grundverordnung und neuem BDSG vertraut, so dass sich die Chance bietet, einen Wissensvorsprung zu erlangen oder von Anfang an auf Augenhöhe zu verhandeln. Für das Seminar muss der Arbeitgeber die Betriebsratsmitglieder in der Regel auch bezahlt freistellen und die Kosten übernehmen.

Betriebsräte sollten sich jetzt im neuen Datenschutzrecht schulen und ihre Datenschutz-Betriebsvereinbarungen zeitnah überprüfen lassen.

Wenn Betriebsräte sichergehen wollen, dass ihr Betrieb ab dem 25. Mai 2018 im Einklang mit der neuen Rechtslage handelt, müssen Betriebsräte zudem ihre Betriebsvereinbarungen zum Datenschutz einer Prüfung unterziehen. Nur so lassen sich die Bußgeld- und Compliance-Risiken so weit wie möglich vermeiden. Die Prüfung bezieht sich darauf, ob die Betriebsvereinbarungen den generellen Anforderungen der Datenschutz-Grundverordnung sowie ihren spezifischen Anforderungen zum Beschäftigtendatenschutz Rechnung tragen. Hierfür bieten die im Folgenden dargestellten Änderungen und Handlungsempfehlungen erste Ansatzpunkte. Anwaltlicher Rat wird bei der Überprüfung der Betriebsvereinbarungen regelmäßig erforderlich sein, zumal es zur Datenschutz-Grundverordnung direkt noch keine Rechtsprechung gibt, auf die man sich stützen könnte.

Den neuen Anforderungen werden bestehende Betriebsvereinbarungen angesichts der Neuerungen häufig noch nicht vollständig entsprechen, auch wenn man aufgrund der im Wesentlichen gleichbleibenden Strukturgrundsätze sicher große Teile übernehmen können wird.

In Panik müssen Betriebsräte bei der Prüfung zwar nicht verfallen: Bis zum Wirksamwerden der Datenschutz-Grundverordnung ist noch nahezu ein Jahr Zeit. Aber die Verhandlung von Datenschutz-Betriebsvereinbarungen nimmt nicht unerheblich Zeit in Anspruch. Es ist mit Blick auf die Höhe möglicher Bußgelder deshalb dringend ratsam, die Verhandlungen frühzeitig, d.h. am besten schon jetzt oder spätestens nach der Sommerpause, zu beginnen.

2. Was sind die wichtigsten Änderungen?

a) Rechte des Arbeitnehmers

Bei den Rechten des Arbeitnehmers/Betroffenen[1] gibt es erwähnenswerte Neuerungen durch die Datenschutz-Grundverordnung:

Das Recht auf Information bei Erhebung von Daten

Ein Recht auf Benachrichtigung des Arbeitnehmers bei erstmaliger Speicherung ohne Kenntnis des Arbeitnehmers bestand schon im alten BDSG (§ 33 BDSG). Die Datenschutz-Grundverordnung erweitert die Auskunftsverpflichtung jedoch nun (Art. 13 und 14 DSGVO). Der Arbeitgeber/Unternehmer[2] muss jetzt von sich aus auch über die Dauer der beabsichtigten Speicherung informieren. Das ist u.a. deswegen gut, weil der Arbeitgeber sich so überlegen muss, wie lange er die Daten speichern will, was es wahrscheinlicher macht, dass er sie irgendwann von sich aus wieder löscht.

Zudem muss der Arbeitgeber neuerdings über die Absicht informieren, die Daten an ein Drittland, z.B. an ein amerikanisches Unternehmen, zu übermitteln, sowie darlegen, warum dies zulässig ist. Schließlich muss er auch über die weiteren Rechte auf Auskunft, Berichtigung, Löschung/Vergessenwerden, Einschränkung der Verarbeitung, Widerspruch aus besonderen Gründen (z.B. bei Profiling), Datenübertragbarkeit sowie das Beschwerderecht bei der Aufsichtsbehörde informieren.

---

1 Im Folgenden spreche ich von „Arbeitnehmer“, auch wenn die Datenschutz-Grundverordnung grundsätzlich für alle Betroffenen gilt und Arbeitnehmerinnen ebenso gemeint sind.

2 Im Folgenden spreche ich von „Arbeitgeber“, auch wenn die Datenschutz-Grundverordnung für alle gilt, die über die Verarbeitung personenbezogener Daten entscheiden; diese nennt die Datenschutz-Grundverordnung „Verantwortliche“.

Neue Rechte stellen unter dieser Aufzählung das Widerspruchsrecht (Art. 21 DSGVO), das Recht auf Datenübertragbarkeit (z.B. bei Wechsel des Arbeitgebers oder außerhalb des Arbeitsrechts eines sozialen Netzwerks oder Dienstleisters, Art. 20 DSGVO) und das Recht auf Vergessenwerden/Löschung (Art. 17 DSGVO) dar.

Betriebsräte sollten sicherstellen, dass in ihren Betrieben gewährleistet ist, dass der Arbeitgeber bei erstmaliger Speicherung von Beschäftigtendaten, die Beschäftigten über die neuerdings erforderlichen Angaben informiert.

Recht auf Vergessenwerden/Löschung

Vielfach in den Medien als neu und bahnbrechend hervorgehoben wurde das Recht auf Vergessen(werden) (Art. 17 DSGVO). Auch wenn eine Löschverpflichtung bereits im alten BDSG enthalten war (§ 35 Abs. 2 Satz 2 BDSG), und das Recht daher nicht ganz so bahnbrechend ist, ist es eine wichtige Neuerung. Denn insgesamt sieht dieses Recht umfassendere Löschpflichten vor, als sein Vorgänger. Es zählt – noch wie seine Vorgängervorschrift zum Löschen von Daten – bestimmte Fallgestaltungen auf, in denen Daten gelöscht werden müssen. Zu löschen sind Daten z.B. wenn sie nicht mehr für den Zweck, für den sie erhoben wurden, notwendig sind oder die Einwilligung zu ihrer Speicherung widerrufen wurde. Die Löschung muss der Arbeitgeber von sich aus vornehmen, oder aber auf (formlosen) Antrag des Arbeitnehmers hin.

Neu ist, dass der Arbeitgeber, Dritte, denen er die Daten übermittelt hat, nicht nur von der Löschung informieren muss, sondern auch davon, dass der Arbeitnehmer die Löschung verlangt hat (Art. 17 Abs. 2 DSGVO). Dies führt wiederum dazu, dass auch dieser verpflichtet ist, die Daten zu löschen, wenn ein Fall der Löschverpflichtung vorliegt und keine Ausnahme greift.

Betriebsräte sollten auch darauf hinwirken, dass in ihren Betrieben ein Verfahren besteht, mit dem die erforderlichen Löschungen vorgenommen und Löschbegehren geprüft und erfüllt werden.

Unentgeltlichkeit, Verständlichkeit und Schnelligkeit

Die Rechte, die die Datenschutz-Grundverordnung dem Arbeitnehmer einräumt, müssen unentgeltlich wahrgenommen werden können (Art. 12 DSGVO). Auskünfte müssen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache“ erfolgen. In der Regel müssen sie schriftlich oder elektronisch gegeben werden. Eine Auskunft muss unverzüglich, regelmäßig aber spätestens innerhalb eines Monats gegeben werden.

b) Datenschutz-Folgenabschätzung

Ein wesentlich neu gestaltetes Instrument des Datenschutzes im Betrieb, bei der der Betriebsrat ein Beteiligungsrecht hat, ist die Datenschutz-Folgenabschätzung.

Bisher bedurfte jede automatisierte Verarbeitung, die besondere Risiken für die Rechte der Betroffenen aufwiesen, etwa weil Gesundheitsdaten verarbeitet wurden, grundsätzlich der Prüfung durch den betrieblichen Datenschutzbeauftragen auf ihre Rechtmäßigkeit (§ 4d Abs. 5 und 6 BDSG).

Diese Vorabkontrolle wird nun durch die Datenschutz-Folgenabschätzung ersetzt (Art. 35 DSGVO).

Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn die Verarbeitungsform ein hohes Risiko für die Rechte von Betroffenen zur Folge hat. Dies kann der Fall sein, weil neue Technologien verwendet werden oder der Umfang oder Zweck der Verarbeitung risikoreich ist. Die Datenschutz-Grundverordnung nennt als Beispiele, wann dies der Fall ist, die umfassende Bewertung persönlicher Aspekte (etwa der Leistung) Betroffener mit automatisierten Verfahren und die umfangreiche Verarbeitung von besonderen Daten – wie (weiterhin) Gesundheitsdaten. Diese Regelung ist im Vergleich zur bisherigen Rechtslage in Deutschland etwas großzügiger, was sich am Beispiel der Gesundheitsdaten zeigt: So reicht nicht mehr die Verarbeitung von Gesundheitsdaten überhaupt, damit eine Datenschutz-Folgenabschätzung nötig ist, sondern es müssen umfangreich Gesundheitsdaten verarbeitet werden. Bestehende Ausnahmen wurden dagegen abgeschafft.

Die Datenschutz-Folgenabschätzung besteht aus folgenden Teilen:

- systematische Beschreibung der geplanten Verarbeitung und ihrer Zwecke
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der geplanten Verarbeitung
- Bewertung der Risiken für die Betroffenen
- Abhilfemaßnahmen zur Bewältigung der Risiken für die Betroffenen.

Bei den Abhilfemaßnahmen müssen auch die Vorkehrungen oder Verfahren dargestellt werden, die den Schutz personenbezogener Daten und die Einhaltung der Datenschutz-Grundverordnung sicherstellen.

Die Datenschutz-Folgenabschätzung wird nicht mehr durch den betrieblichen Datenschutzbeauftragten, sondern durch den Arbeitgeber selbst durchgeführt, der sich dabei vom betrieblichen Datenschutzbeauftragten beraten lassen muss (sofern ein solcher benannt ist). Diese neue Rollenverteilung nimmt den Arbeitgeber zwar selbst noch mehr in die Verantwortung, hat aber den Nachteil, dass sie die Prüfung dem fachlich unabhängigen Datenschutzbeauftragten aus den Händen nimmt.

Ein Betriebsrat hat ab dem 25.05.2018 das Recht, dem Arbeitgeber seinen Standpunkt zur Frage mitzuteilen, ob eine Datenschutz-Folgenabschätzung notwendig ist und wie er die Verarbeitung, deren Notwendigkeit, deren Verhältnismäßigkeit und deren Risiken bewertet sowie welche Maßnahmen er für erforderlich hält. Hierfür muss der Arbeitgeber ihn entsprechend unterrichten. Dass der Arbeitgeber den Betriebsrat auf diese Weise einbezieht sollten Betriebsräte rechtzeitig sicherstellen.

Hervorzuheben ist, dass der Arbeitgeber den Standpunkt betroffener Personen oder des Betriebsrats zu der beabsichtigten Verarbeitung einholen muss (Art. 35 Abs. 9 DSGVO). Damit der Betriebsrat seinen Standpunkt darlegen kann, muss er vorher unterrichtet werden. Die Konsultierung des Betriebsrats betrifft sowohl die Frage der Notwendigkeit der Datenschutz-Folgenabschätzung und damit das Vorliegen besonderer Risiken als auch die Durchführung der Folgenabschätzung selbst.

c) Konsultationspflicht

Bisher bestand eine generelle Meldepflicht von automatisierter Verarbeitungen personenbezogener Daten, wenn mehr als 9 Beschäftigte mit der Verarbeitung betraut waren und kein betrieblicher Datenschutzbeauftragter bestellt war (§ 4d Abs. 1 bis 4 BDSG). Diese Meldepflicht findet nun nicht mehr generell Anwendung, sondern nur noch, wenn die Datenschutz-Folgenabschätzung ein hohes Risiko für personenbezogene Daten ergibt (Art. 36 DSGVO).

d) Nachweispflicht

Der verantwortliche Arbeitgeber muss nachweisen können, dass er die Datenschutz-Grundverordnung einhält (Art. 5 Abs. 2, Art. 25 DSGVO). Die Einhaltung selbst erfolgt mittels geeigneter technischer und organisatorischer Maßnahmen.

Betriebsräte sollten darauf achten, dass der Arbeitgeber ab dem 25.05.2018 einen Nachweis über die Einhaltung der Datenschutz-Grundverordnung vorweisen kann.

e) Datenschutz durch Technikgestaltung und datenschutzfreundliche Grundeinstellungen

Der verantwortliche Arbeitgeber muss die Mittel seiner Datenverarbeitung technisch und organisatorisch so gestalten, dass die Vorschriften des Datenschutz wirksam umgesetzt werden (Art. 25 Abs. 1 DSGVO). Er muss u.a. sicherstellen, dass schon technisch nur Daten erfasst werden können oder schon organisatorisch nur solche Daten erfasst werden dürfen, die für die verfolgten Zwecke wirklich erforderlich sind. Er muss Daten, wenn möglich, anonymisieren oder pseudonymisieren. Pseudonymisieren heißt, dass eine Person nur identifizierbar wird, wenn man sie mit Hilfe eines getrennt aufbewahrten Schlüssels mit ihrem Datum verknüpft. Hierzu muss der Arbeitgeber die Software der Hersteller nutzen, die diese Funktionen anbieten. Die Pflicht besteht, sofern der Aufwand hierfür nicht in einem Missverhältnis zur Schwere des Risikos für das Recht auf Schutz personenbezogener Daten steht. Dies nennt sich Datenschutz durch Technikgestaltung („privacy by design“).

Zudem ist der Arbeitgeber zum Datenschutz durch datenschutzfreundliche Voreinstellungen verpflichtet („privacy by default“, Art. 25 Abs. 2 DSGVO). Er muss Maßnahmen implementieren, die sicherstellen, dass durch Programmvoreinstellung nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen Zweck erforderlich sind. Diese Maßnahmen beziehen sich auf die Menge der Informationen, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Betriebsräte können mit Blick auf das Inkrafttreten der Datenschutz-Grundverordnung fordern, dass die Grundsätze des Datenschutzes zugeschnitten auf die konkrete Situation technisch in die verwendeten Programme integriert werden oder nur solche Programme ausgewählt werden, die die Grundsätze zum Datenschutz berücksichtigen. Alternativ kann der Arbeitgeber entsprechende organisatorische Verfahren nutzen.

f) Minimalregelung zum Beschäftigtendatenschutz mit Regelungsauftrag

Neu ist in der Datenschutz-Grundverordnung vor allem auch, dass sie für den Beschäftigtendatenschutz nähere, allgemeine Vorgaben macht. Um detaillierte Vorgaben zu spezifischen Bereichen des Arbeitslebens, wie sie als „Beschäftigtendatenschutzgesetz“ seit Langem von vielen gefordert wird, handelt es sich dabei jedoch leider nicht. Vergleicht man die verschiedenen Entwurfsfassungen, stellt man fest, dass viele konkrete Vorschläge des Europäischen Parlaments, z.B. ein ausdrückliches Verbot der Videoüberwachung in Umkleideräumen, der heimlichen Videoüberwachung oder von schwarzen Listen von Arbeitnehmern aufgrund von Gewerkschaftszugehörigkeit – nicht im Einzelnen aufgegriffen wurde. Vielmehr wurden diese Vorschläge auf eine allgemeine Vorgabe zusammengeschmolzen.

Die Datenschutz-Grundverordnung besagt, dass Deutschland und die anderen EU-Mitgliedsstaaten zum Beschäftigtendatenschutz selbst eigene, „spezifischere“ Vorschriften als die übrigen Vorschriften der Datenschutz-Grundverordnung erlassen dürfen (Art. 88 Abs. 1 DSGVO).

Neu ist ebenfalls, dass die Datenschutz-Grundverordnung ausdrücklich festlegt, dass diese spezifischeren Vorschriften zur Verarbeitung von Beschäftigtendaten auch in Kollektivvereinbarungen, d.h. in Tarifverträgen oder Betriebsvereinbarungen, bestehen können. Das ist eine gute Nachricht für Betriebsräte, die zum Schutz der Daten der Beschäftigten ihres Betriebs bereits Betriebsvereinbarungen verhandelt haben oder abschließen wollen.

Betriebsvereinbarungen zum Schutz von Beschäftigtendaten sind ausdrücklich weiter möglich.

Die Datenschutz-Grundverordnung nennt einige Verarbeitungszwecke, zu denen spezifischere Gesetze, Tarifverträge oder Betriebsvereinbarungen erlassen bzw. abgeschlossen werden können. Verarbeitungszwecke zu denen spezifischere Vorschriften möglich sind, sind u.a. die der Einstellung, der Erfüllung des Arbeitsvertrags, der Planung und Organisation der Arbeit oder der Beendigung der Arbeitsverhältnisses; diese Zwecke sind in ähnlicher Formulierung bereits aus der bisherigen deutschen Vorschrift zum Beschäftigtendatenschutz bekannt (§ 32 BDSG). Mögliche Verarbeitungszwecke sind aber auch – konkreter als in der bisherigen deutschen Regelung – die Gleichheit und Diversität am Arbeitsplatz, die Gesundheit und Sicherheit am Arbeitsplatz oder der Schutz des Eigentums der Arbeitgeber oder der Kunden, oder auch des „Managements“. Diese Aufzählung ist nicht abschließend.

Allgemeine Vorgaben, wie die spezifischeren Vorschriften zum Beschäftigtendatenschutz ausgestaltet sein müssen, enthält die Datenschutz-Grundverordnung ebenfalls (Art. 88 Abs. 2 DSGVO): Die spezifischeren Vorschriften müssen „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte“ der betroffenen Person umfassen.

Auch Betriebsvereinbarungen müssen angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der Arbeitnehmer enthalten.

Mit der menschlichen Würde ist eines der Grundrechte angesprochen, die den Beschäftigtendatenschutz notwendig machen. Die Gesetze, Tarifverträge oder Betriebsvereinbarungen müssen zu deren Wahrung konkrete Maßnahmen regeln. Die konkreten Maßnahmen müssen den weiteren Grundrechten der Beschäftigten und ihren weiteren berechtigten Interessen angemessen Rechnung tragen. Was das im Einzelnen genau heißt, werden Anwälte, Gerichte, Datenschutzbehörden und sonstige Fachautoren vor allem nach Maßgabe des Grundrechts auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechtecharta) klären müssen. Derartige besondere Maßnahmen sollen insbesondere in Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe und Überwachungssysteme am Arbeitsplatz getroffen werden.

Diese Vorgaben machen bereits jetzt deutlich, dass die spezifischeren Vorschriften nicht beliebig nach unten von den übrigen Vorschriften der Datenschutz-Grundverordnung abweichen dürfen.

> Betriebsvereinbarungen müssen konkretere Regelungen als die Datenschutz-Grundverordnung treffen und dabei mindestens das Schutzniveau der übrigen Datenschutz-Grundverordnung bieten.

Dies gilt übrigens auch für Gesetze und Tarifverträge.

Die Datenschutz-Grundverordnung konkretisiert nach dem europäischen Gesetzgeber das Recht auf Schutz personenbezogener Daten. Das gleiche Schutzniveau muss auf Vorschriften Anwendung finden, die die Vorschriften der Datenschutzverordnung noch weiter konkretisieren bzw. sie noch spezifischer machen.

Deutschland hat die sich durch die Ermächtigungsvorschrift in der Verordnung bietende Gelegenheit leider nicht ergriffen, um ein Beschäftigtendatenschutzgesetz in Angriff zu nehmen. Grob gesagt haben Bundestag und Bundesrat die knappe Vorschrift zur Datenverarbeitung im Beschäftigtenverhältnis aus dem alten BDSG in das neue hinübergerettet und etwas verlängert.

Sie findet sich fast wortgleich im neuen BDSG wieder (dort jetzt § 26 BDSG-neu). Hinzugekommen ist die Zulässigkeit der Datenerhebung zur Ausübung oder Erfüllung der Rechte und Pflichten eines Betriebs- oder Personalrats.

> Das neue BDSG sieht die Zulässigkeit der Datenübermittlung an den Betriebsrat ausdrücklich vor, wenn dies zur Ausübung seiner Rechte oder Erfüllung seiner Pflichten erforderlich ist.

Erwähnenswert sind zudem eine ausdrückliche Regelung im neuen § 26 BDSG zur Einwilligung im Arbeitsverhältnis und eine Aufzählung, wer alles Beschäftigte sind, u.a. auch arbeitnehmerähnliche Personen (z.B. bestimmte freie Mitarbeiter, die einem Arbeitnehmer vergleichbar schutzbedürftig sind).

g) Drastische Erhöhung der Bußgelder

Eine geradezu drastische Änderung erfährt die Höhe des Bußgeldes, das staatliche Datenschutz-Aufsichtsbehörden für die Sanktionierung von Verstößen von Arbeitgebern verhängen können. War bisher in der Regel bis zu 50.000 € und bei schwereren Verstößen bis zu 300.000 € die Höchstgrenze für Verstöße (§ 43 Abs. 3 BDSG), so können jetzt bis zu 10 Mio. € oder 2 % des von einem Unternehmen weltweit erzielten Jahresumsatzes des vorangegangen Geschäftsjahres, je nachdem welcher Betrag höher ist, verhängt werden, und bei schwereren Verstößen bis zu 20 Mio. € oder 4 % des von einem Unternehmen weltweit erzielten Jahresumsatzes (Art. 83 Abs. 4 bis 6 DSGVO).

Diese Erhöhung ist aus Sicht von Arbeitnehmern und Betriebsräten mit Blick auf den Schutz von Beschäftigtendaten zu begrüßen. Denn diese Bußgeldhöhen dürften ihren Zweck, auch für größere Unternehmen abschreckend zu wirken, erfüllen. Der europäische Gesetzgeber meint seine Regelung zum Datenschutz ernst: Das was die Datenschutz-Grundverordnung inhaltlich regelt, soll auch befolgt werden. Es steht zu erwarten, dass mehr Unternehmen ein größeres Augenmerk auf die Einhaltung der Datenschutzvorschriften legen. Zu bemerken ist jedoch, dass die Aufsichtsbehörden über vorsichtige Aufstockungen ihres Personals hinaus noch besser ausgestattet werden müssten, um sich adäquat um die Einhaltung der Datenschutzvorschriften zu kümmern und ihre Sanktionen im Streitfall auch durchzusetzen.

Die Bußgelder für Verstöße gegen die Datenschutz-Grundverordnung sind sehr hoch bemessen. Dies dürfte die Aufmerksamkeit erhöhen, die Arbeitgeber Vereinbarungen zum Datenschutz mit dem Betriebsrat und Kritik durch den Betriebsrat schenken.

h) Was ist gleich geblieben?

Wesentliche Grundsätze des Datenschutzes enthält die Verordnung aber auch weiterhin, zum Teil aber begrifflich etwas anders und genauer gefasst. So ist weiterhin eine gesetzliche Erlaubnis oder Einwilligung (oder im Arbeitsrecht ein Tarifvertrag oder eine Betriebsvereinbarung) Voraussetzung für die Verarbeitung personenbezogener Daten (§ 4 BDSG /Art. 6 DSGVO).

Personenbezogene Daten dürfen nur für legitime Zwecke erhoben werden und nur dann, soweit und solange dies für den Zweck notwendig ist. Sie müssen sachlich richtig sein. Daten müssen zudem sicher sein, wofür entsprechende technische und organisatorische Maßnahmen zu ergreifen sind.

Dies waren die wichtigsten Änderungen der Rechtslage ab dem 25. Mai 2018 im Überblick.

Wenn ihr oder Sie, geschätzte Betriebsratsmitglieder, bei Schulung, Prüfung oder Verhandlung Unterstützung benötigt oder benötigen, stehen wir natürlich gerne zur Verfügung.

Rechtsanwalt Martin Fieseler

Berger Groß Höhmann & Partner Rechtsanwälte
Danziger Str.56 / Ecke Kollwitzstraße
10435 Berlin / Prenzlauer Berg
Tel.: 030-440330-19
Telefax: 030-440330-22
E-Mail: fieseler(at)bghp.de