Vorwort

Gesetzliche Bestimmungen zum Schutz personenbezogener Daten sind in Österreich bereits seit den Siebzigerjahren des 20. Jahrhunderts etabliert und wurden im Laufe der Jahrzehnte wiederholt an geänderte gesellschaftliche und technische Sachverhalte angepasst. Ein wesentlicher Meilenstein dieser Weiterentwicklung war zuletzt durch die EU-Datenschutz-Richtlinie aus dem Jahr 1995 gesetzt worden. Auf dieser Richtlinie beruht das bis heute gültige, jedoch in Detailfragen mehrfach novellierte österreichische Datenschutzgesetz 2000 (DSG 2000).

Diese derzeit noch gültigen Bestimmungen beruhen also auf europarechtlichen Vorgaben, die zu einer Zeit entstanden sind, als Mobiltelefonie und Internet ihre massenhafte Verbreitung noch vor sich hatten. Die heute unter dem Schlagwort „Digitalisierung" diskutierte Automatisierung von Arbeits- und Produktionsschritten war damals ebenfalls erst in Ansätzen absehbar.

Aktuell sind wir zweifellos erneut mit einem Meilenstein in der Weiterentwicklung des europäischen und österreichischen Datenschutzrechts konfrontiert. Am 25. Mai 2018 werden die auf europäischer Ebene beschlossene Datenschutz-Grundverordnung (DS-GVO) sowie das im österreichischen Parlament beschlossene Datenschutz-Anpassungsgesetz 2018[1] wirksam werden.

Die EU-Datenschutz-Richtlinie wird somit durch eine unmittelbar gültige EU-Verordnung ersetzt. In allen Mitgliedstaaten werden dann wortwörtlich dieselben Datenschutzbestimmungen wirksam sein.

Trotz der inzwischen eingetretenen weitreichenden technologischen Veränderungen haben sich die Bestimmungen der EU-Datenschutzrichtlinie aus dem Jahr 1995 in einigen Bereichen bis heute als tragfähig erwiesen. Entsprechend erfolgt durch die neue Datenschutz-Grundverordnung keine völlige Neukonzeption des Datenschutzes, sondern werden bewährte Konzepte fortgeführt und weiterentwickelt.

Nicht alle diese Weiterentwicklungen stoßen auf uneingeschränkte Zustimmung. Vielmehr sind sich wohl alle Interessengruppen in einem Punkt einig: Nicht alle Bestimmungen der DS-GVO sind positiv zu bewerten. Darüber, welche es nicht sind, herrschen naheliegenderweise unterschiedliche Ansichten.

Die wesentlichen Neuerungen durch die DS-GVO sind unter anderem:

- Entfall der DVR-Meldepflicht sowie der Vorabkontrolle durch die Datenschutzbehörde;
- Schaffung einer neuen innerbetrieblichen Dokumentationspflicht;
- Einführung der Funktion des Datenschutzbeauftragten, die in bestimmten Fällen verpflichtend einzurichten ist;
- Stärkung und Erweiterung der Rechte der Betroffenen. Zum Recht auf Information, Auskunft, Richtigstellung und Löschung treten ein Recht auf Datenübertragbarkeit und ein Recht auf Einschränkung der Verarbeitung hinzu;
- Verankerung eines risikobasierten Ansatzes: Das Risiko der Datenverarbeitung für die Rechte und Freiheiten der Betroffenen wird als zentrales Bewertungskriterium etabliert;
- Schaffung einer Verpflichtung, Anforderungen des Datenschutzes durch technische Mittel umzusetzen; Stichworte: „Datenschutz durch (Technik-)Gestaltung" und „datenschutzfreundliche Voreinstellungen";
- wesentliche Stärkung der Datenschutzaufsicht und Rechtsdurchsetzung.

1 DSG idF Datenschutz-Anpassungsgesetz 2018, BGBl I 120/2017.

Eine weitere Änderung, die möglicherweise wesentlich zu einem stärkeren Datenschutzbewusstsein beitragen wird, betrifft den gegenüber dem DSG 2000 deutlich erhöhten Strafrahmen. Begleitet wird dies von einem gesteigerten Interesse der Öffentlichkeit und verstärkter Sensibilität der Stakeholder. Für Unternehmen zählen dazu neben den Kunden bzw Usern auch Auftraggeber, Geschäftspartner, Eigentümer und nicht zuletzt Beschäftigte sowie der Betriebsrat.

Ziel dieses Ratgebers ist es, Datenschutzbeauftragten, Betriebsräten und Betroffenen gleichermaßen Werkzeuge an die Hand zu geben, um in sachlich-konstruktiver Weise die Etablierung einer betrieblichen Datenschutzkultur und eine ausgewogene Umsetzung der rechtlichen Vorgaben im Betrieb fördern und bewerkstelligen zu können.

Die weiterhin rasant fortschreitende technische Entwicklung verändert viele Aspekte des Arbeitslebens und wird auch in Zukunft zahlreiche Weichenstellungen erfordern, um wirtschaftliche Interessen, Datenschutz sowie Arbeitnehmer- und Arbeitgeberinteressen in Einklang zu bringen.

Das wirtschaftliche Interesse am Einsatz bestimmter Technologien und an der Effizienzsteigerung durch die Verarbeitung diverser (und vor allem immer mehr) Daten steht im permanenten Spannungsfeld zur Überwachung der ArbeitnehmerInnen und dem Schutz ihrer Persönlichkeitsrechte. Das Beschäftigungsverhältnis ist dabei von einer besonderen Abhängigkeit geprägt – finanziell, rechtlich und technisch.

Dieser zwangsläufige Interessenkonflikt zwischen dem/der ArbeitgeberIn und den ArbeitnehmerInnen soll durch die umfassende Interessenvertretungsaufgabe des Betriebsrats entschärft werden. Zu den individuellen Ansprüchen, die der/die Einzelne direkt aus dem Datenschutzrecht ableiten kann, treten daher auch die arbeitsrechtlichen (kollektiven) Mitwirkungsrechte der Belegschaft bzw ihres Vertretungsorgans, des Betriebsrats.

Entsprechend vielseitig fällt die Behandlung des Themas auch in den Beiträgen dieses Bandes aus. Den Auftakt der drei **einleitenden Beiträge** macht Andreas Krisch, er begründet die demokratiepolitische Notwendigkeit von Datenschutz. Clara Fritsch und Nina Rotheneder zeichnen die politische Geschichte der Datenschutz-Grundverordnung und der darin (nicht) verankerten betriebsrätlichen Mitbestimmungsrechte nach und Thomas Riesenecker-Caba legt die technisch-organisatorischen Fundamente für die weitere Erörterung, indem er einen Überblick über die erstaunliche Vielfalt der betrieblichen IKT-Systeme verschafft.

Der **zweite Teil** erörtert die Datenschutz-Grundverordnung aus juristischer Sicht. Susanne Haslinger erläutert die rechtlichen Grundsätze einer „ordentlichen" rechtskonformen Datenverarbeitung nach der DS-GVO. Die drei folgenden Beiträge gehen auf verschiedene Aspekte der Durchsetzung der DS-GVO ein: Mario Kalod behandelt das Haftungs- und Sanktionsregime, Ruth Ettl stellt die Bestimmungen rund um die Datenschutzbehörde dar und Andreas Krisch zeigt auf, welche Rechte Betroffene geltend machen können.

Neben dem individuellen Schutz der ArbeitnehmerInnen durch die Datenschutz-Grundverordnung (und das Datenschutzgesetz) sollen auch die Mitwirkungsbefugnisse des Betriebsrats – hier insbesondere in Form des Abschlusses von Betriebsvereinbarungen – weiterhin die Wahrung der Grundrechte der Arbeitnehmer und Arbeitnehmerinnen sicherstellen. Die diesbezüglichen Möglichkeiten nach dem Arbeitsverfassungsgesetz behandelt der **dritte Teil** dieses Bandes.

Martina Chlestil legt anhand von OGH-Entscheidungen dar, welche Bestimmungen des ArbVG für die Behandlung typischer Fragen des Beschäftigtendatenschutzes relevant sind. Clara

Fritsch und Susanne Haslinger geben einen Überblick, wie die Vorgaben der DS-GVO im Rahmen von Betriebsvereinbarungen zu Datenverarbeitungssystemen zu berücksichtigen sind und welchen Nutzen sowohl Unternehmensleitung als auch Belegschaft vom Abschluss derartiger Betriebsvereinbarungen haben. Wolfgang Goricnik untersucht, inwiefern einerseits aufgrund der neuen Rechtslage bestehende Betriebsvereinbarungen angepasst werden müssen und andererseits neue Gestaltungsmöglichkeiten für den Neu-Abschluss von Betriebsvereinbarungen entstehen. Die Mindestinhalte einer Betriebsvereinbarung sind im Kapitel elf noch einmal übersichtlich zu einer praxistauglichen Checkliste zusammengefasst.

Die Beiträge des **vierten Teils** gehen in Form von „Frequently Asked Questions" (FAQ) auf verschiedene praxisrelevante Themen ein. Thomas Riesenecker-Caba gibt Antwort auf die scheinbar triviale Frage, was denn nun mitbestimmungspflichtige personenbezogene Daten sein können, und gemeinsam mit Andreas Krisch zeichnet er die Schritte zur Etablierung einer betrieblichen Datenschutzkultur vor. Nina Rotheneder lichtet die Nebel über dem Wesen des/der Datenschutzbeauftragten und Mario Kalod gibt einen kurzen Überblick, welche unterschiedlichen Interventionsmöglichkeiten Beschäftigten in Betrieben – sowohl mit Unterstützung ihres Betriebsrats als auch ohne Betriebsrat – zur Verfügung stehen. Wolfgang Goricnik konfrontiert Betriebsräte mit der Tatsache, dass auch sie, sollten sie als Datenverarbeiter tätig werden, Verantwortung übernehmen müssen, und Clara Fritsch zeigt den Weg zur Datenübermittlung in Nicht-EU-Länder. Andreas Krisch schließt den Reigen, indem er die Konzepte des Datenschutzes durch Technikgestaltung und Voreinstellungen erläutert. Literatur-, Stichwort- und Autorenverzeichnis runden den Band ab.

Über diese Beiträge hinaus können KäuferInnen des gedruckten Buchs auch auf eine **E-Book-Version** im PDF-Format und **online** unter der URL *www.beschäftigtendatenschutz.at* **auf weitere Inhalte** zugreifen. Die Anleitung dazu findet sich auf der vorderen inneren Umschlagseite.

Die HerausgeberInnen

Susanne Haslinger *Andreas Krisch* *Thomas Riesenecker-Caba*

Wien, im Oktober 2017

Warum Datenschutz?

Andreas Krisch

Kapitel 1

1. Ein Mensch – Viele gesellschaftliche Rollen

Jeder Mensch nimmt in der Gesellschaft laufend unterschiedliche Rollen ein. Wir sind Familienmenschen, Freunde, ArbeitnehmerInnen, Vereinsmitglieder, ehrenamtliche HelferInnen, Patienten und vieles mehr.

Diese Rollen werden von uns relativ klar getrennt und unsere Mitmenschen haben je nach aktueller Rolle unterschiedliche Erwartungen an uns und unser Verhalten. So unterscheidet sich unsere Rolle als Kinder gegenüber unseren Eltern deutlich von unserer Rolle als Teil einer Partnerschaft oder als Elternteil gegenüber unseren Kindern.

Auch unterscheiden sich unsere Rollen innerhalb der Familie wiederum deutlich von den Rollen, die wir in unserem Freundeskreis (etwa am Sportplatz, bei Festen oder im Musikverein) und an unserem Arbeitsplatz einnehmen.

Informationen, die wir in einer Rolle gerne mit anderen teilen, können uns schaden, wenn sie in einem anderen Zusammenhang bekannt werden. Daher trennen wir sehr genau, wem wir welche Einblicke in unser Leben geben. Unsere Eltern wissen sicherlich andere Dinge über uns als unsere Freunde. Mit unseren Freunden wiederum teilen wir andere Informationen als mit unserem Vorgesetzten oder unseren Ärztinnen und Ärzten.

Entsprechend haben wir je nach Rolle, die wir gerade einnehmen, auch andere Erwartungen daran, was die Menschen, denen wir begegnen, über uns wissen. Und wir präsentieren uns diesen Menschen gegenüber auch unterschiedlich. Wir benehmen uns also am Sportplatz deutlich anders als in der dienstlichen Besprechung mit unserer/unserem Vorgesetzten.

Diese Trennung unserer Rollen – also die Möglichkeit uns in unterschiedlichen Situation unterschiedlich zu präsentieren und unterschiedliche Dinge über uns preis zu geben – ist ein wesentlicher Grundpfeiler unserer Freiheit. Sie ermöglicht es uns, unser Leben in allen Aspekten selbstbestimmt zu gestalten und auch die Kontrolle darüber zu behalten, wer unsere beruflichen oder privaten Entscheidungen beeinflussen darf.

Die Trennung unserer Rollen schützt uns beispielsweise meistens davor, dass unser Freizeitverhalten negative Auswirkungen auf unser Berufsleben hat und umgekehrt.

Insgesamt ermöglicht diese Trennung der Rollen erst unsere freie Entfaltung als Menschen. Wird diese Trennung der Rollen von anderen missachtet, empfinden wir das üblicherweise als unzulässigen Eingriff und Verletzung unserer Privatsphäre. Wir erwarten zu Recht, dass die von uns gezogenen Grenzen von unseren Mitmenschen respektiert werden und respektieren ganz selbstverständlich auch selbst die Grenzen anderer.

2. Privatsphäre

Der Schutz unserer Privatsphäre ist ein Menschenrecht, das als Recht auf Achtung des Privat- und Familienlebens in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK)[1] verankert ist. Die EMRK steht in Österreich im Verfassungsrang.

1 Europäische Menschenrechtskonvention (EMRK) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10000308.

Grundverordnung, warum hast du so wenig Mitbestimmung?

Eine kurze Geschichte der DS-GVO

Clara Fritsch, Nina Rotheneder

Kapitel 2

Entschuldigen Sie bitte das Missverständnis …

Als wäre die komplexe Querschnittsmaterie Datenschutzrecht per se nicht schon herausfordernd genug, wurde der Begriff „Datenschutz" selbst auch noch etwas unglücklich gewählt. Die Terminologie ist wohl mit ein Grund, warum Datensicherheit und Datenschutz(recht) vor allem im allgemeinen Sprachgebrauch oft miteinander verwechselt werden. Geht es doch nicht um den Schutz von Daten an sich, sondern um den Schutz von Interessen von Personen (Betroffenen) an der Geheimhaltung von Informationen über sie selbst – konkret eben ihren personenbezogenen Daten. Um Artikel 1 Abs 2 DS-GVO zu zitieren: *„Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten."*

Im Englischen tut man sich ein wenig leichter, sind doch „safety" (Maschinen-/Produkt-Sicherheit: Geht von der Maschine ein Risiko für den Menschen/die Umwelt aus?) und „security" (Daten-/IT-Sicherheit: Kann der Mensch bei der Maschine Schaden anrichten?) von „privacy" (Privatsphäre) relativ leicht zu unterscheiden. Schutzobjekt sind also nicht die Informationen, die verarbeitet werden, sondern die Interessen der Personen, über die Informationen verarbeitet werden. Hat man diesen zentralen Unterschied einmal verinnerlicht, fällt das Verständnis für die Materie allgemein um einiges leichter.

Es lohnt der Blick zurück

Noch leichter versteht man datenschutzrechtliche Normen dann, wenn man sich vor Augen führt, dass diese nicht vom Himmel fallen. Sie werden in demokratisch gewählten Parlamenten beschlossen, um den Umgang mit personenbezogenen Daten und die damit möglicherweise verbundenen Beeinträchtigungen der Privatsphäre bzw. unseres Zusammenlebens zu regulieren. Unser Umgang mit personenbezogenen Daten ist untrennbar damit verknüpft, welche technischen Möglichkeiten uns zur Verfügung stehen. Ganz neue Herausforderungen ergeben sich etwa durch das inzwischen so gut wie flächendeckend vorhandene und umfassend genutzte Internet.[1] Vor 50 Jahren sah die Welt noch ganz anders aus – es lohnt daher der Blick zurück.

1. Datenschutzgesetz 1978 – Grundrecht auf Datenschutz

Die ersten Datenschutznormen wurden in Europa ab Beginn der 1970er-Jahre erlassen, und zwar als Reaktion auf staatliche Bestrebungen Datenbestände in nationalen „Zentraldatenbanken" zu speichern. Datenverarbeitung war in ihren Anfängen keine beiläufige, alltägliche Tätigkeit für jedermann. Vielmehr wurde sie als „Großrisiko" begriffen, ähnlich der Kernenergie.[2] Ziel der Regulierung war es daher, diese Datensammlungen einer gewissen Kontrolle zu unterwerfen.

1 *Jahnel*, Handbuch Datenschutzrecht, 2010, 2.
2 *Mayer-Schönberger/Brandl/Kristoferitsch*, Datenschutzgesetz3 (2014), 3.

Überblick der mitbestimmungspflichtigen IKT-Systeme

Thomas Riesenecker-Caba

Kapitel 3

Die letzten Jahrzehnte waren auf betrieblicher Ebene von vielfältigen Umbrüchen geprägt. Einer der spürbarsten ist der fortschreitende technologische Wandel, die damit verbundenen Erweiterungen der technischen Systeme im Unternehmen und die Verbreitung mobiler Endgeräte als neue Arbeitsmittel.

Die Verarbeitung personenbezogener Daten erfolgt dabei zu sehr unterschiedlichen Zwecken, von der Unterstützung bei der Bewältigung betrieblicher Aufgaben und Optimierung der betrieblichen Abläufe bis hin zur Kontrolle von Beschäftigten. Die Vielfalt der technischen Systeme, die im Bereich der Informationsverarbeitung und Kommunikation zum Einsatz kommen, ist nur mehr schwer zu überblicken, und die gesetzlich notwendige Einbeziehung des Betriebsrats, insbesondere nach den Bestimmungen der §§ 96–97 ArbVG, hängt oft von der aktiven Information der Arbeitgeberin/des Arbeitgebers und den zur Verfügung gestellten Informationen ab. Denn erst nach umfassender Information und Analyse der technischen Systembeschreibungen ist es für Betriebsräte nachvollziehbar,

- welche Daten der Beschäftigten verarbeitet werden,
- welche Auswertungen oder Analysen das betreffende System ermöglicht,
- wer eigentlich Zugriff auf diese Daten und Systemfunktionen besitzt und
- wie eine ordnungsgemäße Verarbeitung der Daten kontrolliert werden kann (zB über Protokolle).

Dieser Beitrag fasst die wesentlichen IKT-Systeme, die unter die Mitwirkungsrechte des Betriebsrats (bzw der Personalvertretung) fallen, zusammen. Dabei werden je System kurz die Zwecke der Nutzung beschrieben, es wird auf mögliche Gefahren der Leistungs- und Verhaltenskontrolle hingewiesen, und Ansätze zur betrieblichen Regelung und Gestaltung dieses Systems werden gegeben. Diese möglichen Lösungsansätze können rechtlicher (zB Art der Information durch den Dienstgeber), technischer (zB welche Auswertungen sind möglich) oder organisatorischer (zB Mitwirkung des Betriebsrats bei Veränderungen) Natur sein. Dabei sei vorausgeschickt, dass eine umfassende technische Erklärung aufgrund des Umfangs dieses Beitrags unterbleiben muss, auf die wesentlichen Aspekte wird aber im Hinblick auf die Verarbeitung personenbezogener Daten der Beschäftigten hingewiesen.

Anhand der folgenden Kurzbeschreibungen ist für Betriebsräte nachvollziehbar, wo sie ihre arbeitsrechtlichen Mitwirkungsrechte geltend machen können und welche Regelungsbereiche bei den jeweiligen Einsatzgebieten zu beachten sind.

Vor Regelung eines konkreten Systems empfiehlt es sich, Kapitel 11 dieses Buches „Checkliste Betriebsvereinbarung – das Prüfschema“ zu lesen.

Für alle in Folge je System beschriebenen Lösungsansätze gibt es Muster-Betriebsvereinbarungen bei den Fachgewerkschaften. Dabei ist jedoch zu beachten, dass diese Mustervereinbarungen allgemein gültige Punkte enthalten, die im Zusammenhang mit dem konkret im Unternehmen eingesetzten System abzugleichen sind. Vereinbarungen aus anderen Betrieben sind mit Vorsicht zu genießen, da diese ein Verhandlungsergebnis darstellen.

Grundsätze der Datenverarbeitung

Susanne Haslinger

Kapitel 4

Ziel der DS-GVO ist die Gewährleistung eines gleichmäßigen und hohen Datenschutzniveaus für natürliche Personen in allen Mitgliedstaaten der Europäischen Union unter gleichzeitiger Ausräumung sämtlicher Hemmnisse für einen freien Datenverkehr innerhalb der Union. Hierzu wurde mit der DS-GVO ein einheitliches Datenschutzrecht geschaffen, das nur noch ausnahmsweise länderspezifische Bestimmungen zulässt.

Die Grundsätze zur Verarbeitung personenbezogener Daten (und natürlich in weiterer Folge auch die daran anknüpfenden Vorschriften) sollen sicher stellen, dass die Grundrechte der Betroffenen, deren Daten verarbeitet werden sollen, gewahrt bleiben. Im Mittelpunkt steht dabei natürlich das Recht auf Schutz personenbezogener Daten.

Die Datenschutzgrundverordnung widmet sich in einem eigenen Abschnitt den Grundsätzen der Verarbeitung von personenbezogenen Daten.[1] Diese beziehen sich einerseits auf die grundsätzliche Frage der **Zulässigkeit** der jeweiligen Datenverarbeitung, andererseits definieren sie klare **Beschränkungen** zB durch eine strikte Zweckbindung und eine Einschränkung auf das Notwendigste – sowohl im umfänglichen als auch im zeitlichen Sinn. Parallel dazu finden sich Grundsatzbestimmungen zur Sicherheit der verarbeitenden Daten und den Rechten und Interessen der Betroffenen, vor allem das Recht auf Auskunft („Transparenz") sowie auf Richtigstellung und Löschung von Daten (siehe Kapitel 7 „Betroffenenrechte").

Während Artikel 5 der DS-GVO sämtliche Grundsätze der Datenverarbeitung auflistet, werden diese in den nachfolgenden Art 6 bis 10 näher ausgeführt.

1. Das Grundrecht auf Datenschutz

Das Grundrecht auf Datenschutz findet sich in Österreich im § 1 des Datenschutzgesetzes[2] und steht im Verfassungsrang. Demnach hat jedermann, insb in Hinblick auf die Achtung seines/ihres Privat- und Familienlebens, Anspruch auf Geheimhaltung seiner/ihrer personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Ein solches Interesse ist dann ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf die/den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

Auf europäischer Ebene – genauer gesagt in Anwendung des Unionsrechts – ist das Grundrecht auf Datenschutz in Art 8 der Grundrechtecharta[3] festgelegt, demnach dürfen personenbezogene Daten nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

1 Abschnitt 2, Art 5–11 DS-GVO.

2 Mit dem Datenschutz-Anpassungsgesetz 2018 wurde der § 1 des DSG 2000 entgegen den Vorschlägen des Ministerialentwurfs (letztlich aufgrund der fehlenden für die Verfassungsänderung notwendigen Zweidrittelmehrheit) nicht abgeändert. Auch nach dem Ministerialentwurf wäre jedoch - abseits der Geltungseinschränkung auf natürliche Personen - kein materieller Eingriff in die Grundrechtsbestimmung erfolgt, sondern im wesentlichen lediglich redaktionelle Änderungen, die einer besseren Verständlichkeit dienen sollen. Offen ist, ob die gewünschte Anpassung in der kommenden Gesetzgebungsperiode nachgeholt wird. Vgl ErlRV 1664 BlgNR XXV. GP 3.

3 Charta der Grundrechte der Europäischen Union. Abl 2012/C 326/02.

Strafen, Haftungen, Risiken

Mario Kalod

Kapitel 5

1. Einleitung1. Einleitung

Die Angleichung des Datenschutzniveaus auf europäischer Ebene ab 25.05.2018 durch die DS-GVO ist seit geraumer Zeit in aller Munde und verursacht teilweise Nervosität. Einer der Hauptgründe für die längst überfällige Beschäftigung mit dem Thema Datenschutz ist nicht zuletzt die Erhöhung der Strafen. Der maximale Strafrahmen in Österreich gemäß DSG 2000 lag bei lediglich 25.000 Euro. Die DS-GVO sieht nun ein Vielfaches dieser Summe bei Verstößen vor. Doch wie hoch können die Strafen tatsächlich ausfallen und vor allem: Wen trifft die Haftung bei Verstößen gegen die Bestimmungen der DS-GVO?

2. Abhilfebefugnisse der nationalen Aufsichtsbehörde

2.1. Abhilfebefugnisse iSd DS-GVO

Die nationale Aufsichtsbehörde, im Falle Österreichs die Datenschutzbehörde (DSB),[1] verfügt iSd Art 58 Abs 2 über zahlreiche Abhilfebefugnisse, die es ihr erlauben, bevor noch Strafen verhängt werden, einen rechtskonformen Zustand durch den Verantwortlichen herstellen zu lassen. Die DS-GVO gestattet der Aufsichtsbehörde, folgende Befugnisse auszuüben:

a) einen Verantwortlichen oder einen Auftragsverarbeiter zu warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen die DS-GVO verstoßen;
b) einen Verantwortlichen oder einen Auftragsverarbeiter zu verwarnen, wenn er mit Verarbeitungsvorgängen gegen die DS-GVO verstoßen hat;
c) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, den Anträgen der betroffenen Person auf Ausübung der ihr nach der DS-GVO zustehenden Rechte zu entsprechen;
d) den Verantwortlichen oder den Auftragsverarbeiter anzuweisen, Verarbeitungsvorgänge gegebenenfalls auf bestimmte Weise und innerhalb eines bestimmten Zeitraums in Einklang mit der DS-GVO zu bringen;
e) den Verantwortlichen anzuweisen, die von einer Verletzung des Schutzes personenbezogener Daten betroffene Person entsprechend zu benachrichtigen;
f) eine vorübergehende oder endgültige Beschränkung der Verarbeitung, einschließlich eines Verbots, zu verhängen;
g) die Berichtigung oder Löschung von personenbezogenen Daten oder die Einschränkung der Verarbeitung und die Unterrichtung der Empfänger, an die diese personenbezogenen Daten offengelegt wurden, über solche Maßnahmen anzuordnen;
h) eine Zertifizierung zu widerrufen oder die Zertifizierungsstelle anzuweisen, eine erteilte Zertifizierung zu widerrufen, oder die Zertifizierungsstelle anzuweisen, keine Zertifizierung zu erteilen, wenn die Voraussetzungen für die Zertifizierung nicht oder nicht mehr erfüllt werden.

1 Siehe § 31 Abs 1 DSG 2018.

Die Datenschutzbehörde

Ruth Ettl

Kapitel 6

1. Die Datenschutzbehörde als Aufsichtsbehörde iSd DS-GVO

1.1. Allgemein (Art 51 DS-GVO, § 18 DSG 2018[1])

Die DS-GVO schreibt jedem Mitgliedstaat der EU vor, eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung einzurichten. Sie sollen die **Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung** schützen und den **freien Verkehr personenbezogener Daten in der Union** erleichtern.

In Österreich wird die bereits bestehende **Datenschutzbehörde (DSB) als nationale Aufsichtsbehörde** gemäß Art 51 DS-GVO eingerichtet.

Die DSB in Österreich ist nicht neu, sondern hat eine lange Geschichte. Schon mit dem ersten Datenschutzgesetz, BGBl. Nr. 565/1978, wurde die sogenannte Datenschutzkommission zur Kontrolle der Einhaltung des Datenschutzes geschaffen. Anlässlich eines Urteils des Europäischen Gerichtshofs[2] wurde 2014 die Datenschutzkommission mittels einer Novelle des Datenschutzgesetzes 2000 (DSG 2000) durch die DSB ersetzt, um deren völlige Unabhängigkeit zu gewährleisten. Damit wurde den Vorgaben der Datenschutz-Richtlinie[3] entsprochen. Die DSB war und ist damit nur mehr organisatorisch beim Bundeskanzleramt angesiedelt.

Die DSB hat im Bereich der Privatwirtschaft vor allem beratende Funktion – im Gegensatz zu deutschen Datenschutzbehörden, die eine lange Tradition auch in der Sanktionierung von Datenschutzvergehen deutscher Unternehmen (zB Lidl, Deutsche Bahn) besitzen. Mit der DS-GVO werden die Kompetenzen der Datenschutzbehörde massiv verstärkt. [4] Sie kann nun zB bei Datenschutzverletzungen Verwaltungsstrafen gegen Unternehmen im privaten Bereich verhängen.

In regelmäßigen Abständen informiert die DSB mittels Newsletter[5] über ihre Entscheidungen und Empfehlungen sowie über gesetzliche Veränderungen im Bereich des Datenschutzes.

In Folge wird die Rolle der DSB anhand der neuen rechtlichen Bestimmungen dargestellt.

1.2. Organisation

1.2.1. Aufbau und Leitung (Art 53, 54 DS-GVO, §§ 18, 20 DSG 2018)

Die DSB ist **monokratisch** strukturiert (im Gegensatz zu einer kollegialen Zusammensetzung), das heißt, letztendlich entscheidet nur der/die LeiterIn und kein Gremium.

Die Leitung (LeiterIn und StellvertreterIn) der DSB wird dabei vom Bundespräsidenten/von der Bundespräsidentin auf Vorschlag der Bundesregierung **für fünf Jahre bestellt**. Wiederbestellungen sind zulässig.

Für die Leitung sind gewisse Qualifikationen Voraussetzung, wie etwa ein Studium der Rechtswissenschaften und ausgezeichnete Kenntnisse des Datenschutzrechts.

Nach Art 53 DS-GVO *endet das Amt der Leitung* mit Ablauf der Amtszeit, Rücktritt oder verpflichtender Versetzung in den Ruhestand. Eine Amtsenthebung ist laut DS-GVO nur bei einer

1 Datenschutzgesetz (DSG idF Datenschutz-Anpassungsgesetz 2018, BGBl I Nr 120/2017 v 31.07.2017).
2 EuGH 16.10.2012, C-614/10, Kommission/Österreich.
3 RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.
4 Siehe ausführlich unter 3.
5 Siehe: https://www.dsb.gv.at/newsletter (geprüft September 2017).

Betroffenenrechte

Andreas Krisch

Kapitel 7

Betroffenenrechte

Gegenüber den bisherigen Bestimmungen der DS-RL wurden die Betroffenenrechte in der DS-GVO deutlich ausgeweitet. Neue Rechte, wie das Recht auf Datenübertragbarkeit, sind hinzugekommen, bestehende Rechte, wie das Recht auf Einschränkung der Verarbeitung, wurden ausgeweitet. Darüber hinaus ist für Verletzungen dieser Rechte regelmäßig der höhere Strafrahmen von bis zu 20 Millionen Euro bzw. 4 % des Jahresumsatzes des Verantwortlichen vorgesehen.

Die „Rechte der betroffenen Person", so die genaue Bezeichnung, stehen natürlichen Personen zu, deren personenbezogene Daten von einem Verantwortlichen verarbeitet werden. Diese Rechte umfassen

- die Informationspflichten des Verantwortlichen,
- das Auskunftsrecht,
- das Recht auf Berichtigung,
- das Recht auf Löschung,
- das Recht auf Einschränkung der Verarbeitung,
- die Mitteilungspflicht des Verantwortlichen im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung der Verarbeitung,
- das Recht auf Datenübertragbarkeit,
- das Widerspruchsrecht sowie
- die Rechte im Zusammenhang mit automatisierten Entscheidungen im Einzelfall einschließlich Profiling.

1. Informationspflichten des Verantwortlichen

Hinsichtlich der Informationspflichten des Verantwortlichen werden zwei Fälle unterschieden. Die Erhebung von personenbezogenen Daten bei der betroffenen Person[1] (oder kurz: dem Betroffenen) und die Erhebung der personenbezogenen Daten bei anderen Quellen als dem Betroffenen.[2]

Im ersten Fall erhält der Verantwortliche die personenbezogenen Daten also direkt vom Betroffenen, zB über ein Formular, in das der Betroffene seine Daten eingibt, im Rahmen eines Gesprächs mit dem Betroffenen oder aus Dokumenten, die der Betroffene selbst vorlegt. Der Einfachheit halber wird nachfolgend die Formulierung „die Daten stammen vom Betroffenen selbst" verwendet.

Im zweiten Fall erhält der Verantwortliche die personenbezogenen Daten nicht vom Betroffenen selbst, sondern aus einer anderen Quelle. So kann der Verantwortliche zB Bonitätsdaten von einem Kreditauskunftsdienst einholen, ohne dass der Betroffene in diesen Vorgang eingebunden ist oder überhaupt davon weiß. Nachfolgend wird für diesen Fall der Einfachheit halber die Formulierung, dass „die Daten nicht vom Betroffenen selbst stammen", verwendet.

1 Die diesbezügliche Informationspflicht ist in Artikel 13 DS-GVO normiert.
2 Die Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden, ist in Artikel 14 DS-GVO normiert.

Mitwirkung des Betriebsrates bei der Verwendung von personenbezogenen Beschäftigtendaten

Martina Chlestil

Kapitel 8

Das friedliche Nebeneinander von Arbeitsverfassungsrecht und Datenschutzrecht

In Betrieben kommen zahlreiche Informations- und Kommunikationssysteme zur Anwendung, die Beschäftigtendaten verarbeiten. Das Arbeitsverfassungsgesetz (ArbVG) stellt dem Betriebsrat Regelungen zur Verfügung, die es ihm ermöglichen, die Interessen der ArbeitnehmerInnen bei der Verwendung ihrer Daten im Betrieb zu wahren. Wie vom OGH[1] bereits bestätigt (siehe Abschnitt 1.), handelt es sich dabei um **„Pflichtbefugnisse"** des Betriebsrates, die durch das Datenschutzgesetz 2000 (DSG 2000) nicht beschränkt werden.

Auch im neuen, mit 25. Mai 2018 in Kraft tretenden **Datenschutzgesetz (DSG 2018)**[2] – das DSG 2000 wurde im Zuge der notwendigen Durchführung mehrerer Bereiche der Europäischen Datenschutz-Grundverordnung (DS-GVO)[3] umfassend novelliert – soll das bestehende Verhältnis zwischen dem Datenschutzrecht und dem Arbeitsverfassungsrecht fortgeschrieben werden. Die entsprechende Bestimmung findet sich in **§ 11 DSG 2018** zur **Verarbeitung personenbezogener Daten im Beschäftigungskontext** und lautet wie folgt: *„Das Arbeitsverfassungsgesetz – ArbVG, BGBl. Nr. 22/1974, ist, soweit es die Verarbeitung personenbezogener Daten regelt, eine Vorschrift im Sinne des Art. 88 DSGVO.* **Die dem Betriebsrat nach dem ArbVG zustehenden Befugnisse bleiben unberührt**."

Das bedeutet, dass das DSG 2018 – wie schon in gleicher Weise das DSG 2000 und das DSG 1978 – generell nicht in die Betriebsverfassung eingreifen will; die Mitwirkungsbefugnisse des Betriebsrates nach dem ArbVG sollen nicht beschnitten werden. Allfällige Geheimhaltungsinteressen eines betroffenen Arbeitnehmers treten kraft gesetzgeberischer Wertung des ArbVG hinter das Belegschaftsinteresse an einer entsprechenden Datenverarbeitung durch den Betriebsrat, der selbst einer strengen Verschwiegenheitspflicht unterliegt, zurück. Die Datenverwendung durch den Betriebsrat und dessen Mitglieder hat ebenfalls datenschutzkonform (insbesondere unter Einhaltung entsprechender Datensicherheitsmaßnahmen etc) zu erfolgen.[4]

In Österreich besteht kein eigentliches Beschäftigtendatenschutzrecht. Wie das DSG 2000 (und zuvor das DSG 1978) enthält auch das DSG 2018 keine eigenen zentralen Regelungen zum **Beschäftigtendatenschutz** iSd Art 88 DS-GVO. Die ArbeitnehmerInnen sind aber nicht rechtlos innerhalb ihrer Arbeitsverhältnisse: Es gelten generell die Vorschriften des **DSG 2018** sowie der **DS-GVO** (zB die allgemeinen Grundsätze der Datenverarbeitung, die Zulässigkeit einer konkreten Datenverwendung, die Rechte der Betroffenen, weitere datenschutzrechtliche Verpflichtungen des Auftraggebers, wie Datensicherheitsmaßnahmen, Geheimnisschutz) selbstverständlich auch im Beschäftigtenverhältnis.[5] Hervorzuheben sind weiters die Regelungen zum Beschäftigtendatenschutz in **arbeitsrechtlichen Vorschriften**[6], wie etwa die Regelungen des ArbVG (§§ 89ff) oder § 10 Arbeitsvertragsrechts-Anpassungsgesetz (AVRAG).

1 OGH 17.9.2014, 6 ObA 1/14m.
2 Datenschutzgesetz (DSG idF Datenschutz-Anpassungsgesetz 2018, BGBl I Nr 120/2017 v 31.7.2017).
3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
4 Siehe hiezu *Goricnik*, Datenübermittlung an den Betriebsrat, DRdA 2015/33.
5 *Chlestil/Fritsch*, Wichtige Änderungen durch das neue Datenschutzrecht mit 25. Mai 2018, DRdA-infas 4/2017.
6 Vgl dazu auch § 11 DSG und die dazugehörigen Erläuterungen.

DS-GVO im Betrieb?

Die Betriebsvereinbarung bringt's!

Clara Fritsch, Susanne Haslinger

Kapitel 9

Die Betriebsvereinbarung ist eines der wichtigsten Instrumente, das das Gesetz dem Betriebsrat (BR) zur Wahrung der Interessen der Belegschaft zur Verfügung stellt. Mit ihr können kollektive (für die gesamte Belegschaft geltende) Rechte und Pflichten geschaffen werden.

Eine gewisse Sonderstellung nehmen die Betriebsvereinbarungen nach den **§§ 96 und 96a ArbVG** ein, da sie sogenannte **„Erlaubnistatbestände"** regeln – mit ihnen erteilt der BR dem/der BetriebsinhaberIn die Erlaubnis zur Verwendung bestimmter Instrumente oder zur Durchführung bestimmter Maßnahmen.

Der BR hat hier eines seiner stärksten **Mitbestimmungsrechte**. Im Fall von Betriebsvereinbarungen nach § 96 ArbVG (im Zusammenhang mit Datenschutzfragen betrifft dies vor allem Überwachungsmaßnahmen, die die Menschenwürde berühren) kann der/die BetriebsinhaberIn ohne Zustimmung des Betriebsrats in Form einer Betriebsvereinbarung (BV) die gewünschte Maßnahme nicht setzen. Bei Maßnahmen im Sinn des § 96a ArbVG (hier vor allem die Einführung von Systemen zur automationsunterstützten Datenverarbeitung) kann der/die BetriebsinhaberIn bei Weigerung des Betriebsrats ersatzweise die Schlichtungsstelle anrufen, die dann einen Kompromiss erlässt (siehe Kapitel 8 und 10).

> Sinn und Zweck dieses starken Mitbestimmungsrechts ist es nicht unbedingt, dem BR ein absolutes Veto gegen bestimmte Maßnahmen in die Hand zu geben und ihn damit zum „Verhinderer" zu machen, sondern vielmehr ihn mit dem **notwendigen Druckmittel auszustatten, um zu einer sinnvollen, alle Interessen ausgleichenden innerbetrieblichen Regelung zu gelangen.**

Selbstverständlich gibt es auch Situationen, in denen der BR seine Zustimmung jedenfalls verweigern wird, zB dann, wenn der/die BetriebsinhaberIn unlautere Zwecke verfolgt oder weit über das genannte Ziel hinausschießt. Denn grundsätzlich dient der Abschluss einer BV nach § 96 oder § 96a ArbVG dem Einfangen von typischerweise mit dem eingeführten System oder der Technologie verbundenen **Risiken** für die Beschäftigten. Damit geht gleichzeitig auch eine hohe Verantwortung des Betriebsrats einher: Wer die erforderliche Zustimmung des Betriebsrats als Abnicken von Vorschlägen des Betriebsinhabers/der Betriebsinhaberin versteht, wird der Belegschaft selten einen Gefallen tun.

Eine BV entsteht – von Ausnahmen der Anrufung der Schlichtungsstelle abgesehen – durch **gemeinsames Aushandeln.**[1] Mithilfe von Betriebsvereinbarungen wird ein **Interessensausgleich** zwischen dem Interesse des Arbeitgebers/der Arbeitgeberin am Einsatz einer bestimmten Technologie und dem Schutz der dadurch gefährdeten Persönlichkeitsrechte und der Menschenwürde der Beschäftigten geschaffen. Daneben, nahezu im „Vorbeigehen", regeln viele Betriebsvereinbarungen, wie das Miteinander im Unternehmen funktionieren soll; das trifft besonders auf die BV nach den §§ 96 und 96a ArbVG, aber auch auf einen Teil der Betriebsvereinbarungen nach dem § 97 ArbVG zu (wie zB Ordnungsvorschriften nach Z 1 oder die Benutzung von Betriebsmitteln nach Z 6). Die BV schützt Beschäftigte vor einseitig seitens der Geschäftsführung getroffenen Maßnahmen (zB disziplinären Maßnahmen, Kontrollmaßnahmen, Ordnungsvorschriften), kann aber auch aus allgemeinen Formulierungen (zB wertschätzender

1 Zum mitunter langwierigen Prozess des Entstehens einer guten BV mit vielen Praxistipps: *Achitz/Fritsch/Haslinger/Müller*, Leitfaden Betriebsvereinbarungen (2015), 335 ff.

Adaption und Neu-Abschluss von Betriebsvereinbarungen zum Datenschutz im Lichte der DS-GVO

Wolfgang Goricnik

Kapitel 10

1. Einleitung

Ab 25.5.2018 wird bekanntlich die **EU-Datenschutz-Grundverordnung** VO (EU) 2016/679 ABl L 2016/119, 1 (im Folgenden: DS-GVO) gem deren Art 99 **anwendbar** sein, die ein neues, unmittelbar geltendes Datenschutzrecht in der EU bringt. Zusätzlich macht das österreichische Datenschutz-Anpassungsgesetz 2018, das ein von Grund auf **erneuertes Datenschutzgesetz** schafft (im Folgenden: **DSG 2018**), von einer **europarechtlichen Öffnungsklausel** (dazu näher im Kapitel 2 „Geschichte der DS-GVO") Gebrauch und normiert unter dem Titel „Verarbeitung personenbezogener Daten im Beschäftigungskontext", dass das *Arbeitsverfassungsgesetz*, soweit es die Verarbeitung personenbezogener Daten regelt, *eine Vorschrift im Sinne des Art 88 DS-GVO ist* und die dem *BR nach dem ArbVG zustehenden Befugnisse unberührt bleiben* (§ 11 DSG 2018).

Diese neue Rechtslage bedeutet einerseits, dass Überlegungen zum rechtlichen Schicksal **bestehender Betriebsvereinbarungen,** die die Verarbeitung von ArbeitnehmerInnendaten beinhalten, insb im Sinne deren **Anpassungsbedarfs**, angestellt werden müssen. Überlegungen müssen auch angestellt werden, ob es damit nicht zu allfälligen **neuen Vorgaben** für den **Neu-Abschluss** von solchen Betriebsvereinbarungen kommt. Andererseits dürfen aber auch Überlegungen angestellt werden, ob damit nicht auch **neue Möglichkeiten** im Sinne neuer wirksamer Gestaltungsrechte für den Neu-Abschluss von solchen Betriebsvereinbarungen entstehen.

2. Allgemeines zu BV mit dem Regelungsgegenstand der Verarbeitung von AN-Daten

Die Verarbeitung von AN-Daten (vor allem iSe Verbesserung des Datenschutzes) kann zwar im Kontext vielfältiger BV geregelt werden[1], **zumeist** wird aber eine **„gemischte" BV** vorliegen, die insb auch auf der Rechtsgrundlage des mit der ArbVG-Novelle 1986[2] iZm der Einführung neuer Technologien[3] geschaffenen § 96a Abs 1 Z 1 beruhen wird; bei einer die Menschenwürde berührenden Kontrolleignung des eingesetzten Systems kommt auch der BV-Tatbestand des § 96 Abs 1 Z 3 ArbVG ins Spiel.

2.1. BV gemäß § 96 Abs 1 Z 3 ArbVG

Voraussetzung für diese (notwendige) Mitbestimmungspflicht ist die Einführung einer Kontrollmaßnahme bzw eines technischen Systems zur Kontrolle der AN sowie ein dadurch bedingtes Berühren der Menschenwürde. Beides muss in Kombination gegeben sein.[4] Die rechtliche Beurteilung dieses Mitwirkungsrechts des BR setzt daher die Auslegung der Begriffe „Kontrollmaßnahme" (bzw technisches System zur Kontrolle der AN) sowie das „Berühren der Menschenwürde" voraus.

1 ZB die Regelung der dienstlichen IKT-Nutzung in einer BV gem § 97 Abs 1 Z 6 ArbVG.
2 BGBl 394/1986.
3 So die Begründung der Novellierung im AB, 1062 BlgNR XVI. GP, 2.
4 *Felten/Preiss* in *Gahleitner/Mosler*, Arbeitsverfassungsrecht III[5] (2015) § 96 Rz 43.

Checkliste Betriebsvereinbarung – das Prüfschema

Clara Fritsch, Susanne Haslinger

Kapitel 11

Die folgende Checkliste soll Betriebsräten helfen, Schritt für Schritt zu einer runden Datenschutz-BV für ein jeweils konkretes System zu gelangen. Unabhängig davon, ob es sich um eine BV nach § 96 ArbVG handelt, weil mit dem eingeführten System nicht nur Daten verarbeitet werden, sondern auch eine verdichtete MitarbeiterInnen-Überwachung droht, oder ob es sich um eine „herkömmliche" Datenschutz-BV zu einem konkreten zum Einsatz kommenden System nach § 96a ArbVG handelt: Wenn die folgenden Punkte berücksichtigt werden, kann sowohl sichergestellt werden, dass die geplante Datenverarbeitung DS-GVO-konform geschieht, als auch die Datenschutz-Rechte und sonstigen Interessen der MitarbeiterInnen gewahrt werden.

Ein wesentliches Ziel der Betriebsvereinbarungen nach § 96 ArbvG und § 96a ArbVG ist der Schutz der ArbeitnehmerInnen vor Überwachung, übermäßigen Eingriffen in ihre Privatsphäre und missbräuchlicher Datenverwendung. Um all diese Bereiche in der Betriebsvereinbarung gut abdecken zu können, sollen die folgenden Fragen weiterhelfen:

Wichtige betriebliche Instrumente, die die DS-GVO neu einführt, sind das unter gewissen Umständen zu erstellende Verarbeitungsverzeichnis und die Datenschutz-Folgenabschätzung bei besonders risikoreichen Anwendungen (siehe beides detaillierter im Kapitel 9 „Die DS-GVO im Betrieb? – Die Betriebsvereinbarung bringt's!"). Die bereits hierfür geklärten Fragen und gesammelten Informationen können eine wertvolle Basis für den Abschluss einer Betriebsvereinbarung bieten.

1. Welches System soll konkret eingeführt werden?

In aller Regel wird der/die BetriebsinhaberIn auf den Betriebsrat zukommen und ihn von der beabsichtigten Einführung einer Videoüberwachung, eines GPS-Fahrtenbuchs, einer MitarbeiterInnenbeurteilung, eines Mobile Device Managements oder Ähnlichem in Kenntnis setzen. Geschieht dies nicht und erhält der Betriebsrat anderweitig von der geplanten Einführung eines solchen Systems Kenntnis, hat er natürlich im Rahmen seiner Informations- und Interventionsrechte (vor allem nach § 89 und § 91 Abs 2 ArbVG) die Möglichkeit, den/die BetriebsinhaberIn damit zu konfrontieren und detaillierte Informationen zu verlangen.

2. Gibt es spezielle Mitwirkungsrechte des Betriebsrats?

Gibt es im Zusammenhang mit der geplanten Einführung eines technischen Systems spezielle Mitwirkungsrechte des Betriebsrats? Gibt es einen **Tatbestand zum Abschluss einer Betriebsvereinbarung**?[1] Wenn ja, welchen? Wie groß ist hierbei die Mitwirkungsbefugnis des Betriebsrats?

In Frage kommen in aller Regel eine Betriebsvereinbarung nach § 96 oder § 96a, die dem Betriebsrat sehr umfangreiche Mitwirkungsbefugnisse einräumt. Ist die geplante Datenverar-

1 Vgl ausführlich *Achitz/Fritsch/Haslinger/Müller*, Leitfaden Betriebsvereinbarungen (2016).

FAQ – Was können mitbestimmungspflichtige personenbezogene Daten sein?

Thomas Riesenecker-Caba

Kapitel 12

Eine Grundvoraussetzung für die Mitbestimmung des Betriebsrats oder zur Prüfung datenschutzrechtlicher Anforderungen beim Betrieb technischer Systeme ist, dass in diesen Systemen personenbezogene Daten der Beschäftigten verarbeitet werden.

Die Datenschutz-Grundverordnung (DS-GVO) definiert personenbezogene Daten in ihrem Artikel 4 Z 1 wie folgt. Es sind

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (…] „betroffene 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."*

Gegenüber der bisherigen Definition des DSG 2000 (*„Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist"*) fällt zuerst auf, dass sich die Definition der DS-GVO ausschließlich auf natürliche (und nicht wie im DSG 2000 angegeben „natürliche und juristische") Personen bezieht. Ähnlich der Definition im DSG 2000 werden auch identifizierte Personen (bisher bestimmte) von identifizierbaren Personen (bisher bestimmbaren) unterschieden, gänzlich neu ist jedoch die umfassende Erklärung, was denn unter identifizierbar zu verstehen ist.

Von den Rechtsfolgen, dh insbesondere den Mitwirkungsrechten des Betriebsrats, sind die beiden Datenarten gleich zu bewerten, ein genauerer Blick auf betriebliche Systeme anhand dieser Definition von personenbezogenen Daten unterstützt jedoch das Handlungsfeld des Betriebsrats.

1. Personenbezogene Stamm- und Bewegungsdaten

Eindeutig identifiziert werden kann eine Person aufgrund ihres Namens oder ihrer Personalnummer. Hier ist es für die Betroffenen auch relativ leicht zu verstehen, dass aufgrund dieser Daten ihre Identität erkennbar ist. Diese Datenarten werden auch oft als Teil der **Stammdaten** (ein Begriff aus der Informatik) beschrieben. Stammdaten sind allgemeine Angaben zur einer bestimmten Person und ändern sich im Laufe des Berufslebens wenig bis gar nicht (zB Sozialversicherungsnummer, Privatadresse, Kostenstelle, Bankverbindung).

Etwas schwieriger ist die Wahrnehmung der Daten, über die eine Person identifizierbar ist. Tagtäglich wird eine Vielzahl an Daten über einzelne Beschäftigte gespeichert, die diese durch ihre Tätigkeit und der Verwendung von technischen Systemen erzeugen (zB Abholen eines Kopierauftrags, Arbeit an einer Produktionsmaschine, Fahrt mit einem Firmenfahrzeug). Wann immer die Möglichkeit besteht, durch Verknüpfung unterschiedlicher Informationen eine Person zu erkennen, ist diese (im Sinne der Begriffsdefinition der DS-GVO) identifizierbar. Für die obigen Beispiele wäre das zB möglich, wenn sich eine Person an einer Kopier-/Druckstation mittels Code oder Karte anmeldet, die Zuordnung zu einer Produktionsmaschine über Schicht-/Dienstplan nachvollziehbar ist oder bekannt ist, welche/r FahrerIn mit welchem Fahrzeug unterwegs ist. In diesem Zusammenhang spricht man auch oft von **Bewegungsdaten**. Diese Da-

FAQ: Etablierung einer betrieblichen Datenschutzkultur

Andreas Krisch, Thomas Riesenecker-Caba

Kapitel 13

Die ab Mai 2018 neuen datenschutzrechtlichen Anforderungen der DS-GVO verfolgen als Hauptziel, im Bereich der Europäischen Union ein **einheitliches Datenschutzrecht** zu etablieren. Bei Verstößen gegen die datenschutzrechtlichen Bestimmungen können von den Aufsichts-(Datenschutz-)behörden hohe Geldbußen ausgesprochen werden. Dies führt auch dazu, dass dem Thema Datenschutz auf betrieblicher Ebene von den verantwortlichen Geschäftsführungen ein höherer Stellenwert beigemessen wird.

Dieser Beitrag beleuchtet das Thema Datenschutz und Datensicherheit aus zwei Richtungen. Zuerst werden die Anforderungen, die die DS-GVO an ArbeitgeberInnen als datenschutzrechtliche Verantwortliche stellt, beschrieben. Daraus abgeleitet wird die Frage gestellt, inwieweit daraus eine neue Datenschutzkultur, die auch Mitbestimmungs- und Mitgestaltungsrechte des Betriebsrats beinhaltet, entstehen kann.

1. Muss dokumentiert oder gemeldet werden, welche Datenverarbeitungen ein Unternehmen durchführt?

Gemäß den bisherigen Bestimmungen des DSG 2000 sind Verarbeitungen personenbezogener Daten unter bestimmten Voraussetzungen an das Datenverarbeitungsregister zu melden. Diese Meldepflicht entfällt mit Wirksamwerden der DS-GVO (Mai 2018). Stattdessen sind Verantwortliche (bisheriger Begriff im DSG 2000: Auftraggeber) und AuftragsverarbeiterInnen (bisheriger Begriff im DSG 2000: Dienstleister) gemäß Artikel 30 DS-GVO unter bestimmten Voraussetzungen verpflichtet ein **Verzeichnis von Verarbeitungstätigkeiten** (auch Verfahrensverzeichnis oder VVZ genannt) zu führen.

2. Unter welchen Voraussetzungen muss ein Verfahrensverzeichnis geführt werden? Wer ist dafür zuständig?

Die Pflicht zur Führung eines Verfahrensverzeichnisses trifft gemäß Artikel 30 Abs 5 DS-GVO alle Unternehmen und Einrichtungen, die 250 oder mehr MitarbeiterInnen beschäftigen. Darüber hinaus unterliegen auch Unternehmen und Einrichtungen, die weniger als 250 MitarbeiterInnen beschäftigen, dieser Pflicht, wenn

- die von ihnen vorgenommene Verarbeitung ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt oder
- die Verarbeitung nicht nur gelegentlich erfolgt oder
- besondere Kategorien von Daten[1] bzw. Daten über strafrechtliche Verurteilungen und Straftaten[2] verarbeitet werden.

In der Praxis ist daher zu erwarten, dass nahezu jedes Unternehmen bzw jede Einrichtung, die MitarbeiterInnen beschäftigt, zur Führung eines Verfahrensverzeichnisses verpflichtet sein

1 Siehe Artikel 9 Abs 1 DS-GVO sowie die Ausführungen zur Verarbeitung „sensibler" Daten in Kapitel 4 „Grundsätze".
2 Siehe Artikel 10 DS-GVO.

Wer? Wie? Wann? Warum? Wieso?

Fragen rund um den/die Datenschutzbeauftragte/n

Nina Rotheneder

Kapitel 14

1. Wer? Wie? Wann? Warum? Wieso?

Seit dem Jahr 1995 bis zu ihrer „Ablösung" durch die DS-GVO sieht bzw. sah die EG-Datenschutzrichtlinie 95/46/EG die Position des/der **Datenschutzbeauftragten** – im Englischen auch **Data Protection Officer** (DSB/DPO) – als mögliche nationale Alternative vor, von der nur wenige Mitgliedstaaten tatsächlich Gebrauch gemacht haben – allen voran Deutschland. Hier hatte das erste Bundesdatenschutzgesetz 1977, ebenso wie das BDSG 1990, die verpflichtende Bestellung von DSB/DPO vorgesehen.[1] Österreich hat von dieser Möglichkeit nie Gebrauch gemacht.

Es gibt in österreichischen Unternehmen und auch öffentlichen Stellen zwar durchaus Personen – oft aus den Bereichen IT, Recht oder Compliance –, die mit einschlägigen Aufgaben zu Datenschutz und Datensicherheit betraut werden, gesetzlich geregelt ist ihre Position jedoch nicht, dementsprechend existiert auch kein einheitliches Rollenbild.[2]

Da die Rolle des/der DSB/DPO hierzulande neu ist, handelt es sich bei ihr um eine der interessanteren Neuerungen durch die DS-GVO. Es stellen sich in der aktuellen Diskussion jede Menge Fragen rund um die Funktion, Gerüchte ranken sich um die mit ihr verbundenen Aufgaben, die notwendigen Ressourcen und möglichen Sanktionen. Ziel dieses Beitrags ist es, einige dieser Fragen zu beantworten bzw. dort, wo dies nicht möglich ist, die unterschiedlichen Meinungen abzubilden – ohne jeden Anspruch auf Vollständigkeit.

2. Wozu eine/n DSB/DPO?

Der/Die DSB/DPO ist als Instrument der Eigenkontrolle beim Verantwortlichen/Auftragsverarbeiter zu sehen – eine weniger bürokratische Ergänzung zur behördlichen Aufsicht. Dies ist insofern relevant, als die bisher bestehenden behördlichen Vorabkontrollpflichten von erweiterten Informationspflichten „abgelöst" wurden.[3]

Ganz abgesehen von einer etwaigen Bestellpflicht darf an dieser Stelle aus einer Praxishilfe der deutschen Gesellschaft für Datenschutz und Datensicherheit (GDD) zitiert werden: „Jemand muss den Job machen!" Die DS-GVO mit ihrem massiv erhöhten Bußgeldrahmen bringt einiges an Herausforderungen und Neuerungen für die Unternehmen – in diesem Zusammenhang leistet der/die DSB/DPO als fachkundiges Beratungs- und Kontrollorgan einen wertvollen Beitrag zur Risikominimierung.[4]

3. Wo finden sich die gesetzlichen Regelungen zum/zur DSB/DPO?

Die DS-GVO sieht in ihrem Kapitel IV zu „Verantwortlicher und Auftragsverarbeiter" in einem eigenen Abschnitt 4 zum/zur Datenschutzbeauftragten drei Artikel betreffend die Regelungen

1 *Jaksch*, Die Bestellungspflichten eines Datenschutzbeauftragten gem DSGVO in ZIIR 2017/2, 140.
2 *König*, Der Datenschutzbeauftragte, in *Knyrim* (Hg): Datenschutz-Grundverordnung, 2016, 231.
3 *Paal*, Benennung eines Datenschutzbeauftragten, in *Paal/Pauly*, DS-GVO, 2017, 476 f.
4 GDD-Praxishilfe DS-GVO I, Stand November 2016, 11.

FAQ Interventionsmöglichkeiten für Beschäftigte

Mario Kalod

Kapitel 15

FAQ Datenschutz im BR-Büro

Wolfgang Goricnik

Kapitel 16

FAQ Datenübermittlung in Drittländer

Clara Fritsch

Kapitel 17

1. Ist es ein Unterschied ob personenbezogene Daten der Beschäftigten *innerhalb oder außerhalb* der EU übermittelt werden?

Ja.

Innerhalb der EU ist die DS-GVO der für alle geltende rechtlich Rahmen und so lange man sich an diesen hält, ist jeder Datentransfer erlaubt.

Außerhalb der EU gibt es unterschiedlichste rechtlich legale Varianten, wie Daten von einem Land ins andere übermittelt werden können, wie weiter unten dargestellt ist.

2. Was muss ich generell beachten, wenn Beschäftigtendaten außerhalb der EU verarbeitet werden?

Jede Datenverwendung von personenbezogenen Daten, also auch der Datentransfer ins Ausland und auch die Speicherung im Ausland, unterliegen den Grundsätzen des Datenschutzes (vgl Kapitel 4 „Grundsätze der Datenverarbeitung nach der DS-GVO"). Es darf also nur dann passieren, wenn ein **eindeutiger und legitimer Zweck** gegeben ist. Dieser Zweck ist dann auch in der dazugehörigen Betriebsvereinbarung niederzuschreiben. Denn (fast) *jede* Datenübermittlung in Drittländer muss auch dem ArbVG folgen und ist daher zustimmungspflichtig.

3. Muss ich für den Datentransfer in Drittländer eine Betriebsvereinbarung abschließen?

Zu 99% ja.

Hier liegt dieselbe BV-Pflicht vor, die auch sonst besteht. Sobald personenbezogene Daten der Beschäftigten ins Nicht-EU-Ausland transferiert werden sollen (zB internationale Qualifikationsdatenbanken), sobald eine Kontrollmaßnahme vorliegt (zB Videoaufnahmen werden im Ausland gespeichert), sobald Fragebögen ausgewertet werden (zB eine externe Firma erstellt Fragebögen über die Zufriedenheit der ArbeitnehmerInnen) muss eine BV abgeschlossen werden (vgl Kapitel 9 „ DS-GVO im Betrieb? – Die Betriebsvereinbarung bringt's!").

In einer solchen BV sollte dann unbedingt festgehalten werden, zu welchem Zweck die Daten übermittelt werden, wohin die Daten gehen, wer Zugriff hat, wie lange die Daten dort verarbeitet/ gespeichert werden. Nähere Ausführungen zur Gestaltung der BV finden sich in Kapitel 9 „ DS-GVO im Betrieb? – Die Betriebsvereinbarung bringt's!".

4. Darf der Arbeitgeber/ Verantwortliche personenbezogene Daten in Nicht-EU-Länder übermitteln?

Ja, wenn er eine der zahlreichen Möglichkeiten (siehe unten) auswählt und sich an die Vorgaben der DS-GVO hält.

FAQ: Datenschutz durch Technik

Andreas Krisch

Kapitel 18

1. Was versteht man unter „Privacy by Design“?

Der Begriff “Privacy by Design“ ist in der deutschsprachigen Fassung der DS-GVO mit dem Begriff Datenschutz durch Technikgestaltung übersetzt[1]. Gemeint ist damit die gezielte Gestaltung von Datenverarbeitungsvorgängen entsprechend den Anforderungen der datenschutzrechtlichen Vorgaben.

Datenschutz durch Technikgestaltung ist eines der neuen Grundkonzepte der DS-GVO. Die Überlegung dahinter ist, dass mit technischen Systemen, die grundsätzlich nach den Anforderungen des Datenschutzrechts gestaltet wurden, der Datenschutz in der Praxis besser sichergestellt werden kann, als dies mit Systemen der Fall ist, die auf die Einhaltung datenschutzrechtlicher Vorgaben nicht ausdrücklich Rücksicht nehmen.

Die Umsetzung dieses Konzepts erfordert ein entsprechendes Umdenken in weiten Bereichen der IT-Wirtschaft und insbesondere der Softwareentwicklung. So sind künftig die Anforderungen des Datenschutzes bereits im Rahmen der Anforderungsanalyse zu berücksichtigen und stellen ein wesentliches Qualitätsmerkmal für moderne und praxisgerechte IT-Lösungen dar.[2] Der Fokus liegt dabei auf einem sorgsamen Umgang mit personenbezogenen Daten und auf der Bereitstellung transparenter Informationen über die Auswirkungen der jeweiligen Verarbeitungsschritte. Neue Funktionalitäten sind dabei jeweils auf ihre Übereinstimmung mit den Anforderungen des Datenschutzes zu überprüfen.

Entsprechend dem von der DS-GVO geforderten risikobasierten Ansatz hat die/der Verantwortliche für ihre/seine Verarbeitungen geeignete technische und organisatorische Maßnahmen zu treffen, damit die Datenschutzgrundsätze[3] wirksam umgesetzt werden und die übrigen Anforderungen der DS-GVO und anderer datenschutzrechtlicher Vorgaben erfüllt werden. Diese Verpflichtung trifft sie/ihn bereits im Zuge der Gestaltung bzw. Festlegung ihrer/seiner technischen Systeme (Design-Phase) und dauert darüber hinaus über die gesamte Verarbeitungsdauer an.

Bei der Umsetzung hat die/der Verantwortliche den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen.

Das bedeutet, dass ein angemessenes Gleichgewicht zwischen diesen, einander teils widersprechenden, Anforderungen gefunden werden muss. Im Zuge dieser Abwägung werden die Implementierungskosten in der Praxis häufig als wesentliches Kriterium genannt. Dabei ist jedoch zu beachten, dass im Ergebnis jedenfalls ein angemessenes Datenschutzniveau erreicht werden muss, um die Zulässigkeit der Verarbeitung nicht zu gefährden[4]. Eine ausschließliche Orientierung an den Kosten greift also deutlich zu kurz. Wobei selbst bei rein kostenbasierter Betrachtung zu berücksichtigen wäre, dass das Kostenrisiko von Verstößen gegen die Bestimmungen der DS-GVO allfällige Kosten für IT-technische Adaptierungen bei weitem übersteigen könnte.

---

1 Siehe Artikel 25 Abs 1 DS-GVO.

2 Siehe dazu *Krisch*, DSGVO: Chancen und Risiken für die IT-Wirtschaft. In *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016).

3 Zu den Grundsätzen des Datenschutzes siehe Kapitel 4 „Grundsätze der Datenverarbeitung.“

4 Siehe dazu auch *Hötzendorfer* in *Gantschacher/Jelinek/Schmidl/Spanberger* (Hrsg), Datenschutz-Grundverordnung: Rechtskommentar (2017), 277.