EU-Vorgaben zum Datenschutz: War das schon alles?

Mit der am 25. Mai 2018 in Kraft tretenden EU-Datenschutz-Grundverordnung (DSGVO) werden die Parameter für den Datenschutz in Europa neu gesetzt. Der veränderte rechtliche Rahmen bedeutet einen erheblichen Organisationsaufwand für den Unternehmer. Er sollte aber darüber hinaus Anlass für die Wahrnehmung des Wertewandels sein, der sich beim Umgang mit Daten im Unternehmen seit geraumer Zeit vollzieht.

VON **DR. STEFAN SIMON** UND **HEIKE SCHULZE BRANDHOFF**

ZU DEN PERSONEN

Dr. Stefan Simon ist Rechtsanwalt und Partner der SPITZWEG Partnerschaft mbB. Die interdisziplinäre Sozietät mit Sitz in München berät ihre Mandanten national und grenzüberschreitend in allen Bereichen des Gesellschafts-, Steuer- und Arbeitsrechts sowie des IT- und Datenschutzrechts. Dr. Simon ist als Fachanwalt für Handels- und Gesellschaftsrecht unter anderem auf die Compliance- und Strukturierungsberatung mittelständischer Unternehmen spezialisiert, insbesondere auf die Schnittstellen zum Datenschutz- und Technikrecht.

Heike Schulze Brandhoff ist Rechtsanwältin und Fachanwältin für Arbeitsrecht der SPITZWEG Partnerschaft mbB. Sie ist eine versierte Beraterin in der Ausgestaltung datenschutzrechtlicher Instrumente und Prozesse an der Schnittstelle des Arbeits- und Datenschutzrechts.

www.spitzweg.com

Die EU-Datenschutz-Grundverordnung hält für den deutschen Unternehmer ohne Zweifel komplexe Aufgaben bereit. Sie werden sicherlich anspruchsvoller dadurch, dass der deutsche Gesetzgeber das Bundesdatenschutzgesetz zur Anpassung an die neuen EU-Vorgaben geändert hat. In der Technik ebenso wie im Recht wird sich erst in den nächsten Jahren zeigen, ob die „Schnittstellen" der beiden Regelungswerke so optimiert sind, dass kein rechtsfreier Raum besteht und der Aufwand für den Unternehmer nicht größer wird.

Ist die EU-Grundverordnung ein Monster?

Der Unternehmer als Teilnehmer am Wirtschaftsleben und zugleich auch als Arbeitgeber hat für den Umgang von personenbezogenen Daten einen neuen Ansatz zu wählen. Gesetzlich gefordert ist in der Tat ein Datenschutzmanagement, das nicht nur den Ist-Zustand im Unternehmen dokumentiert und überwacht, sondern als zentrales Element der Verantwortungskontrolle und der Haftungsabsicherung für die Unternehmensleitung dient. Nur auf diesem Weg kann der wesentliche Schritt gelingen, dass den gesetzlichen Dokumentationspflichten, den Auskunftspflichten gegenüber Betroffenen, der notwendigen Anpassung und ständigen Überprüfung von Datenschutzinstrumenten (Betriebsvereinbarungen, Einwilligungserklärungen, Datenschutzverpflichtungen und so weiter) nachgekommen sowie das Risiko der deutlich erhöhten Bußgelder vermieden wird.

In der Sache hat der Gesetzgeber (nur) das nachvollzogen, was notwendig ist, um den Schutz von Verbraucherdaten (vor allem als Kunde, als Arbeitnehmer und als Geschäftspartner) gegen unbefugte Nutzung und insbesondere Missbrauch zu schützen. Je mehr versucht wird, Fertigungsprozesse zu optimieren, Kostenpositionen zu identifizieren und zu reduzieren sowie insgesamt die Skalierbarkeit in der Wertschöpfungskette zu erhöhen, desto mehr benötigen wir das „Datum" als Informationsträger, um diese Ziele zu erreichen. Auf diesem Weg werden jedoch nicht nur die Prozesse in der Wertschöpfungskette transparenter, sondern auch die an der Wertschöpfungskette beteiligten Kunden, Arbeitnehmer und Geschäftspartner gläserner. In diesem Sinn ist der Datenschutz des 21. Jahrhunderts schlicht „der Geist, den wir riefen".

Datenschutz „by design of judges“

Mit dem neuen gesetzlichen Rahmen ist es jedoch noch nicht getan. Auch in der Rechtsprechung zum Arbeitsrecht hat sich in den letzten Jahren ein Wertewandel im Umgang mit personenbezogenen Daten von Arbeitnehmern vollzogen. Es ist zwischenzeitlich gefestigte Rechtsprechung des Bundesarbeitsgerichts, dass Sachverhalte, die Grundlage für eine (in der Praxis meist fristlose) Kündigung des Arbeitsverhältnisses sind, jedoch unter Verstoß gegen datenschutzrechtliche Bestimmungen gewonnen wurden, einem sogenannten Beweisverwertungsverbot unterliegen. In der Praxis bedeutet dies regelmäßig, dass die Sachverhalte nicht mehr geeignet sind, einen Kündigungsgrund darzustellen, die Kündigung also unwirksam ist. Auch auf diese geänderte gesellschaftspolitische Wertentscheidung hat sich längst noch nicht jeder Unternehmer in Deutschland eingestellt. Sie erfordert jedoch Kenntnisse und Sensibilisierung der Personalverantwortlichen, einen klaren Umgang mit klassisch kündigungsrelevanten Sachverhalten und einen ebenso klaren, vorausschauenden Prozess in der Personalabteilung für die Beendigung von Arbeitsverhältnissen.

Datentransfer außerhalb der EU – it works?

Auch über Europas Grenzen hinweg sind die Dinge im Fluss. Nach dem Urteil des EuGH in der Rechtssache Max Schrems im Jahr 2015 war das sogenannte Safe-Habor-Abkommen zwischen der EU und den USA als Grundlage für einen Datentransfer in die USA untauglich geworden. Der EuGH sprach diesem Abkommen die notwendigen Garantien ab, die das EU-Datenschutzrecht für den Umgang mit personenbezogenen Daten von EU-Bürgern auch im Ausland fordert. Für Brüsseler Verhältnisse sehr schnell traf sodann die EU-Kommission einen Beschluss über den sogenannten EU-US Privacy Shield als neue Rechtsgrundlage für einen transatlantischen Datentransfer. Ob dieser europäische Beschluss (allein) eine Grundlage für einen solchen Transfer bilden kann, ist juristisch nach wie vor offen. Ebenso offen sind die weiteren in der Praxis gerne beworbenen Instrumente für einen angeblich rechtssicheren Datentransfer außerhalb der EU beziehungsweise des EWR. Diese sind derzeit ebenfalls Gegenstand von Verfahren vor dem EuGH. Der Unternehmer muss sich also auch hier Gedanken darüber machen, ob und wie die drohende Wertentscheidung europäischer Gerichte bei der Gestaltung seiner unternehmensbezogenen IT-Prozesse berücksichtigt werden sollen. Tröstlich bleibt bei diesen schwierigen Rahmenbedingungen allein, dass die Themen nach wie vor im Fluss sind und die Entwicklungen auch zugunsten des Unternehmers aufgehen können.

Wenn nichts mehr hilft, hilft die Versicherung

Die Quintessenz ist offensichtlich: Das Thema Datenschutz hat in den letzten Jahren – und nicht erst mit der EU-Datenschutz-Grundverordnung – einen Wandel in seiner Bedeutung und damit auch in seinem Handlingsaufwand innerhalb unternehmerischer Prozesse gewonnen. Er hebt es auf eine Stufe mit dem Arbeitsschutz oder der Produkthaftung. Das bedeutet für den Unternehmer nicht nur einen grundlegend anderen Ansatz dieses Themas, einen deutlich höheren Organisations- und Kostenaufwand und die Notwendigkeit von Investitionen in IT-Hardware- und Software. Ebenso klar ist: Auch in diesem Bereich wird eine vollständige Risikoabsicherung nicht möglich sein. Es wird Datenpannen, Hacker-Angriffe/Cyber-Kriminalität und infolgedessen Verlust von Betriebs-Know-how, Störungen im Betriebsablauf bis hin zu Betriebsunterbrechungen, Image-Schaden und Ähnliches geben, die sich – je nach Einzelfall – selbstverständlich auch im Jahresabschluss oder der persönlichen Verantwortung der Geschäftsleitung niederschlagen können.

Umso mehr ist der Unternehmer gehalten, zu prüfen, ob und in welchem Umfang Versicherungslösungen für das Unternehmen und die handelnden Personen ein Restrisiko auffangen können. Auch hier ist der Versicherungsmarkt noch im Fluss, muss der Unternehmer also sorgsam seine maßgeschneiderte Lösung wählen.

FAZIT

Im Ergebnis zeigt sich, dass Datenschutz im 21. Jahrhundert eine vollständige Neupositionierung der Unternehmensleitung erfordert. Die DSGVO fordert vor diesem Hintergrund ein umfassendes Datenschutzmanagement, das von der Dokumentation und Kontrolle bis hin zur Haftungsabsicherung reicht. An dem damit verbundenen Aufwand führt nicht zuletzt angesichts des Risikos von Datenpannen und deutlich erhöhter Bußgelder kein Weg vorbei. ■