LINDA LIESUM
SACHVERSTÄNDIGE FÜR
WIRTSCHAFTSKRIMINALITÄT
& COMPLIANCE

Gerade mal ein Drittel der betroffenen Unternehmen hat sich mit dem neuen Bundesdatenschutzgesetz und der damit verbundenen Anpassung an die EU-Datenschutzgrundverordnung auseinandergesetzt.

Fit für DSGVO und BDSG-Neu?

@Jakub Jirsák / Fotolia

Ab 25.05.2018 muss die DSGVO verbindlich angewendet werden. Bei Nicht-Erfüllung der DSGVO Kriterien, müssen Unternehmen mit extrem hohen Bußgeldern und Geldstrafen rechnen. Nutzen Sie den Schnelltest, um zu erkennen ob bei der Umsetzung der Vorgaben der DSVGO und des BDSG-neu noch Vorkehrungen zu treffen sind.

Am 05.07.2017 ist das BDSG-Neu im Bundesgesetzblatt veröffentlicht worden. Damit wurde das geltende Bundesdatenschutzgesetz an die neue EU-Datenschutzgrundverordnung (nachfolgend DSGVO) angepasst, die ab 25.05.2018 verbindlich anzuwenden ist. Die DSGVO hat zum Ziel, insgesamt das Datenschutzniveau in Europa zu optimieren und soweit als möglich grenzüberschreitend in Europa einheitlich zu implementieren. Dennoch lässt die DSGVO auch Spielraum für nationale Gesetzgeber in Auslegungsfragen. Deutschland hat von diesen Spielräumen, u.a. im Beschäftigtendatenschutz, Gebrauch gemacht, um bisher bestehende höhere Standards im Vergleich zu DSGVO weiterhin sicherzustellen.

Aber was bedeutet dies für Unternehmen konkret? Mit welchen Konsequenzen müssen Unternehmen bei Verstößen rechnen und wie können Unternehmensverantwortliche mittels einiger kleinerer Fragen testen, ob und inwieweit bei den derzeitigen Prozessen, Systemen Mitarbeitern ihres Unternehmens die neuen Datenschutzbestimmungen bekannt und umgesetzt sind:

Verstöße gegen die DSVGO können Unternehmen zukünftig teuer zu stehen kommen

Bei Bußgeldern galt bislang nach dem BDSG der Begriff des Unternehmens, d.h. jede juristische Person eines Konzerns wurde als verantwortliche Stelle angesehen, es gab damit auch keine Konzernhaftung. Nach den neuen Regelungen der DSGVO ändert sich diese Sichtweise. Art 104 und Art 105 beschreiben ein Unternehmen als jede eine wirtschaftliche Tätigkeit ausübende Einheit, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung. Dies hat damit zur Folge, dass gegebenenfalls auch eine Konzernhaftung in einer Unternehmensgruppe auftreten kann. Demzufolge sind auch die Sanktionsmaßnahmen neuerdings anders zu bewerten:

1. Neben der erheblichen Erhöhung der Bußgelder von derzeit maximal EUR 300.000,- können zukünftig Beträge von bis zu EUR 20.000.000,- auf Unternehmen zukommen.

2. Es können Geldstrafen bis zu 4 % des weltweit erzielten Umsatzes für ein Unternehmen veranschlagt werden, sofern dieser Wert das Bußgeld von EUR 20.000.000,- übersteigt.

Wonach richtet sich die Sanktionshöhe und gibt es noch weitere Sanktionsmaßnahmen?

Bei der Festlegung der Strafen fallen u.a. die nachfolgenden Kriterien ins Gewicht:

- Art, Schwere und Dauer des Verstoßes
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes
- die getroffenen Kriterien zur Risikominderung
- die getroffenen Maßnahmen zur Minderung des entstandenen Schadens
- etwaige bekannte frühere Verstöße
- Mitwirkung bei Aufklärung und Kooperation mit den Aufsichtsbehörden
- Art der personenbezogenen Daten, die von dem Verstoß betroffen sind
- Etc.

Je nach Schwere des Vergehens und der Häufigkeit von Verstößen in Unternehmen sowie der damit einhergehenden Sorgfalt können auch Unternehmen noch weitere Sanktionsmaßnahmen treffen:

- Rüge
- Zeitliches oder endgültiges Verbot der Datenverarbeitung
- Gewinnabschöpfung
- Etc.

setzung der Vorgaben der DSGVO und des BDSG-neu empfiehlt es sich, die nachfolgenden Fragen als einen kurzen Test zur Selbstüberprüfung zu nutzen, um zu sehen, ob und inwieweit noch Verbesserungen in den bestehenden Vorkehrungen zum Schutz von personenbezogenen Daten getroffen werden müssen.

1. Beschäftigtendatenschutz

Mit der Einführung des BDSG-neu wurde im Bereich des Beschäftigtendatenschutzes von einer der Öffnungsklauseln, die die DSGVO den Mitgliedstaaten ermöglicht hat, Gebrauch gemacht. Die deutsche Bundesregierung hat Wert darauf gelegt, dass die bisherigen Schutzmaßnahmen übernommen und auf weitere Beschäftigtengruppen ausgedehnt wurden.

Demzufolge sind zukünftig auch Leiharbeiter dem BDSG-neu zu unterziehen. Daraus ergeben sich Fragestellungen, wie z.B.:

Projizieren bestehende Betriebsvereinbarungen grundsätzlich auch auf Leiharbeiter/innen sofern datenschutzrechtliche Belange betroffen sind? Liegen bei allen Mitarbeiter/innen und Leiharbeiter/innen schriftliche Einwilligungserklärungen und Widerrufsbelehrungen zur Nutzung personenbezogener Daten vor?

2. Pflichten für Unternehmen

Mit der DSGVO ergibt sich für Unternehmen neuerdings auch die Verpflichtung zur Datenschutz-Folgenabschätzung. Was genau heißt dies und wie stellen Unternehmen sicher, dass die wesentlichen Folgen erfasst, ausreichend bewertet und bei Verstößen den zuständigen Aufsichtsbehörden berichtet werden?

Darüber hinaus kommt auf Unternehmen, die zwar selber keine Niederlassung in der EU unterhalten, aber u.a. Waren oder Dienstleistungen durch Repräsentanten anbieten, die Verpflichtung zu, einen EU-Vertreter für den Datenschutz zu bestellen. Daraus ergibt sich die Frage: Ergibt sich für das Unternehmen die Verpflichtung zur Bestimmung eines EU-Vertreters und wie wird sichergestellt, dass dieser die notwendige Einbindung in die Prozesse hat, um seinen Aufgaben nachkommen zu können?

Die Erweiterung der Haftung auf den gesamten Konzern für Verstöße gegen die DSGVO kann Bußgelder bis 20 Mio. EUR bzw. Geldstrafen bis zu 4 % des weltweit erzielten Umsatzes betragen.

Wie können Unternehmen feststellen, ob sie fit sind für die DSGVO und BDSG-neu?

Damit Unternehmensverantwortliche schnell und pragmatisch feststellen können, ob ihre Unternehmung „sattelfest" ist im Umgang mit der Um-

Linda Liesum

Sachverständige für Wirtschaftskriminalität und Compliance

DIN EN ISO/iEC 17024 zertifizierte Sachverständige für Wirtschaftskriminaität und Compliance der Akkreditierungsstelle des European Committee for Quality Assurance GEIE in Brüssel Zertifizierungsnr. 1-16-1041

Tel.-Nr. 06126 9513 343
linda.liesum@forensic-sv.de

Wiesbadener Str. 7
65510 Idstein

Auch wurden die Bestimmungen hinsichtlich der Bestellung für einen Datenschutzbeauftragten verschärft. Sofern Versicherungsunternehmen darüber hinaus den MaGo (Mindestanforderungen an die Geschäftsorganisation), die zum 01.02.2017 in Kraft getreten sind) unterliegen, ist zukünftig die gesamte Geschäftsleitung für Schlüsselfunktionen – zu denen auch der Datenschutzbeauftragte zählt – verantwortlich. Dies bedeutet, es hat eine regelmäßige Unterrichtung der Geschäftsführung zu erfolgen und Maßnahmen sind gesamtheitlich zu entscheiden und demzufolge auch zu dokumentieren. Hier ergibt sich die Frage: Sind die Prozesse im Unternehmen so ausgelegt, dass grundsätzlich die gesamte Geschäftsleitung gleichermaßen über die Tätigkeiten und Empfehlungen der Beauftragten unterrichtet werden und die jeweiligen Umsetzungsmaßnahmen gesamtheitlich entschieden und dokumentiert werden?

3. Internationale Datentransfers ins Ausland

Der Transfer von personenbezogenen Daten in Staaten außerhalb der EU war nach dem alten BDSG problematisch und bleibt es auch weiterhin, unabhängig von der Einführung der DSGVO als auch des BDSG-neu. Aber was heißt dies im Zusammenhang mit der steigenden Zahl von Auslagerungen von standardisierten Vorgängen. Wie oft werden Schadenabwicklungen, Standardabfragen wie z.B. KYC-Abfragen an Stellen nach Indien oder ein anderes Drittland gegeben. Daraus ergibt sich die Frage: Reichen die implementierten Sicherheitsmechanismen aus, um ein angemessenes Datenschutzniveau zu gewährleisten und inwieweit sind die Prozesse in den regelmäßigen Überwachungen? Entsprechen die bestehenden vertraglichen Bestimmungen mit Dienstleistern den gesetzlichen Bestimmungen im Hinblick auf eine mögliche Auftragsdatenverarbeitung? Ist dem Kunden bekannt, dass seine Daten im Rahmen einer möglichen Auftragsdatenverarbeitung an Dritte weitergegeben werden und hat er hierzu seine Einwilligung erteilt?

4. Digitalisierung

Aber auch die zunehmende Digitalisierung stellt Firmen vor neue Herausforderungen: Was ist zum Beispiel mit Kundendaten, die in der sogenannten Cloud liegen und von einem Rechenzentrum in Europa betrieben werden. Gelten ausnahmslos die gleichen Regelungen in allen Ländern auf Basis der DSGVO oder haben einzelne Länder wie z.B. Deutschland von den möglichen Öffnungsklauseln Gebrauch gemacht? Wie sehen die Sicherheitsmaßnahmen, z.B. Verschlüsselung, Pseudonymisierung und Berechtigungskonzepte aus und wer verwaltet und überprüft diese regelmäßig?

Wie kann ich Sie unterstützen und welche Expertise bringe ich mit?

Wenn Sie als Unternehmensverantwortlicher bei der Beantwortung der oben gestellten Fragen festgestellt haben, dass Ihre Unternehmung noch den ein oder anderen Optimierungsbedarf hat, unterstütze ich Sie gerne.

Im Laufe meiner beruflichen Karriere war ich selber neben meinen Complianceaufgaben für mehr als 11 Jahre Datenschutzbeauftragte für einen großen, international tätigen Versicherungsmakler. Dadurch bin ich vertraut mit den Bestimmungen und Anforderungen im Umgang mit personenbezogenen Daten und kann aus der Praxis heraus häufig gestellte Fragen beantworten und mögliche Risiken erkennen, analysieren und in Form einer Risikomatrix auch bewerten.

Bei der Erstellung einer Gap-Analyse zwischen implementierten datenschutzrechtlichen Maßnahmen und neuen Anforderungen, der Analyse und Bewertung von sich daraus ergebenen Risiken und der Bestimmung und Entwicklung eines Maßnahmenplans unterstütze ich Sie gerne. Daran anschließend begleite ich Sie bei der Umsetzung der Maßnahmenpläne und stehe gerne beratend zur Seite.

Wenn Sie weitere Informationen benötigen, kontaktieren Sie mich.

Zusammenfassung

Ab 25.05.2018 gilt die neue EU-Datenschutzgrundverordnung (DSGVO)

Der Schnelltest für Unternehmen beschäftigt sich mit diesen Themen:

- Beschäftigungsdatenschutz
- Pflichten für Unternehmen
- Internationale Datentransfers ins Ausland
- Digitalisierung

Verstöße gegen die DSVGO können Unternehmen zukünftig teuer zu stehen kommen:

Die bisherige Obergrenze von Bußgeldern von 300.000 EUR kann nun bis zu 20. Mio. EUR betragen. Des weiteren gibt es Geldstrafen bis zu 4 % des weltweit erzielten Umsatzes, sofern der Wert des Bußgeldes den Wert von 20 Mio. EUR übersteigt. Unabhängig von der geprüften Konzerneinheit wird beim Verstoß der komplette Konzern bei der Festlegung der Strafen herangezogen.

Es lohnt sich jetzt ins Handeln zu kommen.