RINK

Praxisleitfaden Datenschutzgrundverordnung (DSGVO)

Nützliche Hilfestellungen und Informationen
für Ihr Unternehmen

Herausgegeben von:

Rink Rechtsanwaltsgesellschaft mbH
Expo Plaza 1
30539 Hannover

Tel: 0511 51 53 53 - 00
Fax: 0511 51 53 53 - 49

RINK

Inhalt

RINK

Einleitung

Die Datenschutzgrundverordnung (DSGVO) kommt und wird ab dem 25. Mai 2018 die bestehenden Regelungen zum Datenschutz in Europa ersetzen. Sie ist jedoch nicht nur eine Vereinheitlichung alter Regelungen, sondern bringt im Vergleich zum bisher geltenden Datenschutzrecht erhebliche Neuerungen mit sich.

Unternehmen bleibt für die Umsetzung nur eine knapp bemessene Zeit. Sie müssen die umfangreichen Anforderungen der DSGVO umsetzen und entsprechende Prozesse im Unternehmen etablieren oder ändern.

Mit dieser Broschüre geben wir Ihnen einen Überblick über die geänderten Vorschriften und erste Anhaltspunkte, wie Sie ein effektives Datenschutz-Management-System in Ihrem Unternehmen einführen können.

Sollten Sie Fragen oder Anregungen haben, treten Sie gerne in Kontakt mit uns.

RINK

Warum handeln?

Erweiterte Rechenschaftspflicht, Art. 5 Abs. 2

Gerade in klein- und mittelständischen Unternehmen fristete das Datenschutzrecht bis heute häufig ein Schattendasein. Dies ist nicht zuletzt dem Umstand geschuldet, dass Bußgelder durch die Aufsichtsbehörden selten verhängt wurden.

Es ist aber zu erwarten, dass sich dies Praxis ändern wird. Die Prüfung von Unternehmen wird sich künftig einfacher gestalten, da die DSGVO als einen neuen, zentralen Grundsatz eine sehr weitgehende Rechenschaftspflicht für Unternehmen vorsieht. Jedes Unternehmen, welches personenbezogene Daten verarbeitet ist verpflichtet, alle erforderlichen Prozesse und einzelne Schritte zu dokumentieren. Diese Dokumentation ist insbesondere für Überprüfungen durch Aufsichtsbehörden nachweisbar vorzuhalten. Hierzu zählt nicht nur, dass Einwilligungen der betroffenen Personen protokolliert werden, sondern sämtliche Datenverarbeitungsprozesse und entsprechende Prüfroutinen sind zu dokumentieren. Eine unzureichende Dokumentation wird sich maßgeblich auf die Höhe des Bußgeldes auswirken.

Hohe Bußgeldandrohung und Erweiterung der Bußgeldtatbestände

Der Bußgeldrahmen wird durch die DSGVO deutlich ausgeweitet. Der Verordnungstext legt den Aufsichtsbehörden die Verpflichtung auf, künftig „abschreckende“ Bußgeldhöhen zu verhängen. Anders als das BDSG mit seinem Bußgeldrahmen von bis zu 300.000 € können nach der DSGVO bereits bei „einfachen“ Verstößen Bußgelder in einer Höhe von bis zu 10.000.000 € bzw. 2 % des gesamten weltweiten Jahresumsatzes des vorgelagerten Geschäftsjahres verhängt werden, je nachdem, welcher Wert höher ist. Bei schwerwiegenden Verstößen können die Geldbußen sogar verdoppelt werden.

Verbandsklagerecht

Auch durch das neue Verbandsklagerecht laufen Unternehmen Gefahr in Bezug auf datenschutzrechtliche Verstöße stärker in Anspruch genommen zu werden als bisher. Nach den bisherigen Regelungen konnten Verbraucherschutzorganisationen nur dann gegen Unternehmen vorgehen, wenn sie fehlerhafte Datenschutzregelungen in ihren Allgemeinen Geschäftsbedingungen veröffentlichten. Diese Befugnis wird durch das „Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts“ erweitert. Ein Unterlassungsanspruch besteht nun auch bei gesetzwidrigen Praktiken von Gesetzen, welche die Zulässigkeit der Erhebung personenbezogener Daten eines Verbrauchers durch einen Unternehmer regeln, sowie sämtliche Vorschriften, welche die Verarbeitung oder Nutzung personenbezogener Daten, die über einen Verbraucher erhoben wurden, wenn die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhoben, verarbeitet oder genutzt werden.

Damit hat der deutsche Gesetzgeber die Öffnungsklausel in Art. 80 Abs. 2 DSGVO genutzt. Dieses Gesetz räumt einer Vielzahl von Verbänden ein Klagerecht zur abstrakten Durchsetzung datenschutzrechtlicher Vorschriften ein. Es ist damit nicht erforderlich, dass der Betroffene selbst beschwert sein muss.

RINK

Wen in den Veränderungsprozess einbeziehen?

Die DSGVO bringt zahlreiche neue Anforderungen mit sich, die sich auf eine Vielzahl von Unternehmensbereichen auswirken wird. Die jeweiligen Leiter der Abteilungen sollten Sie bei der Einführung der DSGVO möglichst von Anfang miteinbeziehen und informieren:

» Geschäftsführung: Sie sollte über die Gesetzesänderung und dessen Auswirkungen informiert werden. Zu informieren ist über die bestehenden Risiken, sowie die nicht unerheblichen Kosten bei der Einführung eines Datenschutz-Managementsystems.

» Informationssicherheitsbeauftragter: Die von der DSGVO geforderte Risikoanalyse zur Identifizierung von Schwachstellen sollte nicht ohne Einbeziehung des Informationssi- cherheitsbeauftragten durchgeführt werden, um festzustellen, inwieweit auf die bereits vorhandenen Risikoanalysen aufgebaut werden kann.

» Rechtsabteilung: Eine Vielzahl von Verträgen müssen geprüft und ggf. angepasst werden.

» Personalabteilung und Betriebsrat: Alle Betriebsvereinbarungen zur Regelung des Beschäftigtendatenschutzes müssen überprüft, verhandelt und ggf. angepasst werden. Hierbei muss gem. § 87 Abs. 1 Nr. 6 BetrVG mit dem Betriebsrat zusammengewirkt werden. Auch sind Mitarbeiterschulungen über die neuen gesetzlichen Anforderungen erforderlich.

RINK

Welche Prozesse, Richtlinien und Anweisungen muss ich in meinem Unternehmen überprüfen?

- Vollständige Dokumentation aller Verarbeitungsprozesse von personenbezogenen Daten im Unternehmen
- Einführung einer Risiko-Analyse zur Festlegung geeigneter technisch-organisatorischer Maßnahmen
- Überarbeitung der Einwilligungserklärungen, sowie der Protokollierung.
- Überarbeitung des Prozesses für den Widerruf der Einwilligung
- Prozess zur Verarbeitung von Widersprüchen
- Etablierung eines Prozesses zur Einbeziehung einer datenschutzrechtlichen Prüfung bei der Einführung von neuen Prozessen. Hier sind die rechtlichen Anforderungen – insbesondere ob eine Datenschutzfolgenabschätzung notwendig ist oder nicht, zu prüfen.
- Prozess bei Datenpannen (Notfallmanagement)
- Überprüfung und ggf. Anpassung bestehender Betriebsvereinbarungen
- Entwicklung einer Schnittstelle, um Daten in gängigem elektronischen Format übertragen zu können
- Durchführung von Schulungen zu den Neuerungen der DSGVO und der neuen Prozesse
- Prozess zur Überwachung von Änderungen der Gesetzgebung und entsprechender Fortbildung

RINK

Referentenentwurf des ABDSG-E

Die DSGVO ersetzt die Regelungen des BDSG. Als Verordnung gilt sie ohne nationalen Umsetzungsakt in allen Mitgliedsstaaten. Allerdings werden die jeweiligen nationalen Gesetzgeber in einigen Bereichen durch sog. Öffnungsklauseln ermächtigt, Regelungen der Verordnung zu konkretisieren oder bestimmte Bereiche selbstständig zu regeln. Der deutsche Gesetzgeber ist derzeitig dabei, ein entsprechendes Gesetz zu erlassen.

Beispielsweise ist zu erwarten, dass die BDSG-Regelung zum Erfordernis eines Datenschutzbeauftragten bestehen bleiben wird und damit Deutschland über die Mindestanforderungen hinausgeht, und eine Pflicht bei mehr als 9 Angestellten zur Bestellung besteht.

Der gesamte Beschäftigtendatenschutz unterliegt andererseits gemäß Art. 88 Abs. 1 DSGVO einer Öffnungsklausel. Allerdings sind keine weitreichenden Änderungen durch den nationalen Gesetzgeber zu erwarten, sondern eine dem § 32 BDSG entsprechende Regelung. Betriebsvereinbarungen zum Datenschutz im Arbeitsverhältnis bleiben nach wie vor zulässig. Allerdings müssen sie den Vorgaben der DSGVO entsprechen, sodass sie überprüft werden sollten.

RINK

Datenschutzgrundsätze

Mehr Transparenz und Informationspflichten, Art. 12 f.

Die in der DSGVO enthaltenen Informationspflichten, wenn personenbezogene Daten beim Betroffenen erhoben werden, sind umfangreicher als im BDSG. Der Verantwortliche muss nun neben seiner Identität, der Zweckbestimmung und der Kategorien von Empfängern folgende Informationen bereitstellen:

- seine Kontaktdaten
- Kontaktdaten des Datenschutzbeauftragten
- ggf. berechtigte Interessen des Verantwortlichen
- Rechtsgrundlage
- Beabsichtigen einer Übermittlung an ein Drittland oder eine internationale Organisation
- Dauer der Speicherung
- Rechte des Betroffenen (insbesondere Auskunft, Löschung, Berichtigung, Einschränkung und Widerrufsrecht, sowie sein Beschwerderecht bei der Aufsichtsbehörde)
- für den Fall des Profilings eine Information über Logik und Tragweite der angestrebten Auswirkung

Erforderlich sind daher Unternehmensprozesse, welche sicherstellen, dass die Informationspflichten bei der Erhebung vorhanden und aktuell gehalten werden. Häufig werden Unternehmen nicht jeder Datenverarbeitung bereits einer Rechtsgrundlage zugeordnet haben. Mit Einführung der DSGVO besteht aber eine Informationspflicht gegenüber den betroffenen Personen über die Rechtsgrundlage und wenn die Verarbeitung auf einer Abwägung der Interessen beruht, müssen darüber hinaus auch die eigenen berechtigten Interessen aufgeführt werden.

Weitreichende Nachweispflichten, Art. 5, 24

Art. 24 legt dem Verantwortlichen die Pflicht auf, geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen, dass personenbezogene Daten in Übereinstimmung mit der DSGVO verarbeitet werden. Es handelt sich mithin nicht um Maßnahmen zur Sicherheit der Verarbeitung. Diese sind gesondert in Art. 32 DSGVO geregelt. Auf den ersten Blick ergibt sich diese Pflicht schon aus der Gesamtheit der Normen der DSGVO. Jedoch fordert die Norm, dass der Verarbeiter im Vorfeld unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung, sowie der Eintrittswahrscheinlichkeit und Schwere die Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen analysieren und festhalten soll. Hierbei handelt es sich um eine klassische Risikoanalyse, welche laufend verbessert und aktuell gehalten werden muss. Diese Norm wird flankiert von Art. 5 Abs. 2, der dem Verantwortlichen eine sog. „Rechenschaftspflicht“ in Bezug auf die Grundzüge, welche in Abs. 1 genannt sind, auferlegt.

Aus dem Zusammenhang von Art. 5 Abs. 2 und Art. 24 ergibt sich eine vollständige Dokumentationspflicht aller Verarbeitungsvorgänge, sowie einer Risikoanalyse der hieraus entstehenden Gefahren. Dies bedeutet einen erheblichen Mehraufwand. Achten Sie bei der Dokumentation auch darauf, dass - je nach Erlaubnistatbestand - die betroffene Person unterschiedliche Rechte haben kann. So kann die betroffene Person ihre Einwilligung jederzeit widerrufen, wohingegen ein Widerspruch nur unter bestimmten Voraussetzungen erfolgen kann.

Privacy by Design / Privacy by Default

Neu eingeführt wird die Verpflichtung, dass Unternehmen für ihre Datenverarbeitungsprozesse technisch und organisatorisch Maßnahmen treffen müssen, welche die Erhebung von personenbezogenen Maßnahmen auf die erforderlichen Daten begrenzt, die für den Verarbeitungszweck notwendig sind. Gemeint ist nicht nur die quantitative Menge, sondern auch der Umfang ihrer Verarbeitung, deren Zugänglichkeit und Speicherfristen.

Auch wenn der Verordnungsgeber hier Facebook, Google und Co. im Hinterkopf hatte, betrifft es insbesondere auch andere Anbieter von Anwendungen und Apps, welche auf ihre Datenschutzkonformität geprüft werden müssen.

Datenschutz-Folgenabschätzung, Art. 35

Die aus dem BDSG bekannte Vorabkontrolle wird in der DSGVO durch die Datenschutz-Folgenabschätzung ersetzt und inhaltlich neu gefasst, grundsätzlich aber nichts Anderes.

Eine Datenschutz-Folgenabschätzung ist immer dann durchzuführen, wenn eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen zur Folge haben kann.

Aufgrund der in Art. 35 Abs. 3 DSGVO genannten Regelbeispiele, bei denen eine Durchführungspflicht besteht, ist im Vergleich zum BDSG ein größerer Anwendungsbereich für die Datenschutz-Folgeabschätzung zu erwarten.

Die Aufsichtsbehörden sind gemäß Art. 35 Abs. 4 DSGVO ermächtigt im Rahmen ihres jeweiligen Zuständigkeitsbereichs eine Liste der Verarbeitungsvorgänge zu veröffentlichen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist.

Künftig sollten Sie die Liste der für Sie zuständigen Aufsichtsbehörde im Blick haben und eine Erstprüfung ihrer Prozesse, bei denen personenbezogene Daten erhoben werden, etablieren. Auch sollten vorhandene Prozesse mit der Liste abgeglichen werden. Für den Fall, dass Sie keine Maßnahmen treffen oder treffen können, um ein hohes Risiko einer Datenverarbeitung einzuschränken, müssen Sie die zuständige Aufsichtsbehörde miteinbeziehen.

RINK

Rechtmäßigkeit der Verarbeitung

Der aus dem BDSG bekannte Grundsatz des Verbotes mit Erlaubnisvorbehalt, also das grundsätzliche Verbot personenbezogene Daten zu verarbeiten, es sei denn, eine Erlaubnis liegt vor, bleibt auch unter der DSGVO erhalten. Nach wie vor muss die betroffene Person eine Einwilligung erteilen, die Verarbeitung aufgrund eines Vertrages erfolgen oder eine Ermächtigung durch gesetzliche Bestimmung vorliegen.

Einwilligung

Anforderungen bleiben weitgehend erhalten

An den hohen Anforderungen, die bisher für eine Einwilligung galten (Freiwilligkeit und einfache und verständliche Sprache) hat sich durch die Einführung der DSGVO nicht viel geändert. Auch hat die betroffene Person weiterhin ein jederzeitiges Recht auf Widerruf seiner Einwilligung. Dieser Widerruf muss einfach, jederzeit und ohne Begründung möglich sein.

Auch gilt gemäß Art. 7 Abs. 4 DSGVO in Verbindung mit Erwägungsgrund 34 das Kopplungsverbot auch nach der DSGVO fort und wird verschärft: der Vertragsschluss oder die Erbringung einer Dienstleistung darf nicht von der Einwilligung der betroffenen Person abhängig gemacht werden, es sei denn, die personenbezogenen Daten sind für die Erfüllung des Vertrages erforderlich. Die Verarbeitung von sensiblen Daten ist grundsätzlich untersagt, es sei denn, es liegt eine Einwilligung vor.

Erwägungsgrund 32 sieht eine graduelle Erhöhung der Anforderungen an die Einwilligungshandlung vor: Es ist eine eindeutige Handlung, beispielsweise durch Anklicken eines Kästchens auf der Webseite erforderlich. Ein stillschweigendes Einverständnis, durch ein standardmäßig angekreuztes Kästchen oder die bloße Untätigkeit der betroffenen Personen ist nicht ausreichend. Auch muss in jeden Datenverarbeitungsvorgang gesondert eingewilligt werden.

Denken Sie auch daran, dass Sie den Nachweis einer rechtskonformen Einwilligung erbringen können müssen.

Kein Schriftformerfordernis

Neu ist, dass die Schriftform nicht mehr ausdrücklich gefordert wird, sodass die Einwilligung auch in einer anderen Form erteilt werden kann. Bedenken Sie jedoch, dass die DSGVO die Protokollierung der Einwilligung verpflichtend vorschreibt. Damit dürfte zumindest der schriftliche Nachweis für die Praxis weiterhin Bestand haben.

Stellen Sie sicher, dass die Einwilligungen protokolliert werden.

Einwilligung durch Minderjährige

Die DSGVO hat erstmals Voraussetzungen für die Einwilligungsfähigkeit von Minderjährigen aufgenommen. Diese können nur wirksam eine Einwilligung erteilen, wenn sie das 16. Lebensjahr vollendet haben oder die Eltern der Verarbeitung zugestimmt haben.

Zu beachten ist, dass Sie die Beweislast für die rechtskonforme Einwilligung tragen und insofern ein nachweisbarer Prozess etabliert werden sollte, wie Sie das Alter im Rahmen der Einwilligungserklärung verifizieren können.

Zulässigkeit von Zweckänderungen, Art. 6

Auch wenn der Grundsatz der Zweckbindung in der DSGVO Einzug gefunden hat, so wird er im Rahmen der Weiterverarbeitung aufgeweicht. Die Verordnung unterscheidet zwischen

Erst- und Weiterverarbeitung. Eine Weiterverarbeitung ist auch dann rechtmäßig, wenn sie mit dem ursprünglich festgelegten, eindeutigen und rechtmäßigen Zweck vereinbar ist (sog. „Kompatibilitätsprüfung“).

Neben der Kompatibilitätsprüfung ist erforderlich, dass die Zweckänderung für die betroffene Person vorhersehbar war, der Verantwortliche angemessene Maßnahmen zur Datensicherheit ergriffen hat und mögliche Folgen für die betroffenen Personen mitberücksichtigen wurden. Insoweit unterscheidet sich die DSGVO vom BDSG, welche die Nutzung für einen anderen Zweck nach § 28 Abs. 2 BDSG Nr. 1 als zulässig erachtet, wenn es zur „Wahrung berechtigter Interessen“ der verantwortlichen Stelle erforderlich ist und „kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.“ Auch wenn der Wortlaut „mit dem ursprünglichen Zweck vereinbar“ bereits in der EU-Datenschutzrichtlinie enthalten war, ist unklar, wie diese Begrifflichkeit in Deutschland ausgelegt werden wird. Insoweit bleibt abzuwarten, wie eng oder weit künftige, weitere Verarbeitungszwecke definiert werden können.

Nicht zu vergessen ist, dass die betroffene Person gemäß Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 vorab über die Weiterverarbeitung zu einem anderen Zwecke zu informieren.

Auch wenn die Zweckänderung für Unternehmen ein interessantes Instrument sein kann, die bereits erhobenen personenbezogenen Daten weiterzuverarbeiten, so sind die Anforderungen hieran hoch.

Zweckänderungen sollte nur in Ausnahmefällen angedacht werden.

Profiling und Scoring, Art. 22

Die DSGVO führt den Begriff des „Profilings“ ein und versteht hierunter jede Art der automatisierten Verarbeitung personenbezogener Daten, die darauf abzielt, dass die Daten verwendet werden, um bestimmte persönliche Aspekte eines Betroffenen zu bewerten, analysieren oder vorherzusagen.

Der Anwendungsbereich der Norm scheint überschaubar. Zu nennen sind hier insbesondere Auskunfteien, welche Informationen über das Zahlungsverhalten von natürlichen Personen speichern, wie beispielsweise die SCHUFA Holding AG.

Die DSGVO untersagt jene Form der reinen automatisierten Entscheidungsfindung. Der betroffenen Person muss, wenn die Entscheidung rechtliche Wirkungen entfaltet oder den Betroffenen in einer ähnlichen Weise erheblich beeinträchtigen kann, das Recht eingeräumt werden, nicht ausschließlich einer solchen Entscheidung unterworfen zu werden. Als Mindestanforderungen nennt die DSGVO das Recht auf Eingreifen einer Person, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung.

Die Auswirkungen dürften aber gering sein, da es weiterhin möglich ist, eine automatisierte Entscheidung einzuholen, wenn dies für den Abschluss oder die Erfüllung eines Vertrages zwischen dem Verantwortlichen und der betroffenen Person erforderlich ist.

Werbliche Ansprache und Direktmarketing, Art. 6 Abs. 1f.

Wesentlich abgespeckt und weiter formuliert wurden die Erlaubnistatbestände für die werbliche Ansprache von Interessenten und Kunden. Anders als die engen Regelungen des BDSG (Listenprivileg oder rechtswirksame Einwilligung, sowie entsprechender Sondernormen für Telefon- und E-Mail-Werbung), sieht die DSGVO heute eine allgemeine Interessenabwägung zwischen den berechtigten Interessen des Unternehmens und den Interessen bzw. Grundrechten der betroffenen Personen vor. Von entscheidender Bedeutung ist, dass die DSGVO die Verarbeitung von personenbezogenen Daten zum Zwecke des Direktmarketings als ein berechtigtes Interesse eines Unternehmens betrachtet.

Durch diese Öffnung können sich für Unternehmen neue Potentiale für die Werbung ergeben. Insoweit sollten diese neuen Möglichkeiten im Rahmen der eigenen Werbestrategie berücksichtigt werden.

Neue Rechte der Betroffenen

Recht auf Vergessen werden

Personenbezogene Daten waren schon nach dem BDSG bei einem Zweckfortfall zu löschen. Neu ist, dass der Verarbeiter, der personenbezogene Daten öffentlich gemacht hat, künftig andere Unternehmen, an welche sie die Daten weitergegeben haben, darüber informieren müssen, dass die betroffene Person die Löschung seiner personenbezogenen Daten, Kopien, Replikationen der Daten, sowie entsprechender Links verlangt. Der Verordnungsgeber fordert aber nur Maßnahmen, die angemessen sind, d.h. unter Berücksichtigung der verfügbaren Technologien und Implementierungskosten.

Überprüfen Sie Ihre Löschkonzepte und passen Sie diese an. Sie sollten ihre internen Betriebsabläufe so organisieren, dass sie wissen, wo Sie welche personenbezogenen Daten gespeichert, veröffentlicht oder weitergeben haben. Denken Sie an den Fall, dass ihr Datenbestand nicht auf dem neusten Stand ist und Sie diese Informationen an Dritte weitergeben haben.

Recht auf Einschränkung der Verarbeitung, Art. 18

Das Recht auf Einschränkung der Verarbeitung tritt an die Stelle des Rechts auf Sperrung. Die betroffene Person kann unter bestimmten Voraussetzungen verlangen, dass sämtliche erhobenen personenbezogenen Daten nur mit individueller Einwilligung und zur Durchsetzung von Rechtsansprüchen verarbeitet werden dürfen.

Eine Einschränkung der Verarbeitung ist fortan dann vorzunehmen, wenn der Betroffene es verlangt und

» er die Richtigkeit der personenbezogenen Daten bestreitet, wobei die Einschränkung dann für die Dauer zu bewirken ist, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen oder

» die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt oder

» der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt oder

» Widerspruch gegen die Verarbeitung gemäß Artikel 21 Abs. 1 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen

Wird die Verarbeitung eingeschränkt, so ist die betroffene Person im Rahmen der Informationspflicht verpflichtet, die betroffene Person vor Aufhebung der Einschränkung zu informieren. Auch ist im Fall einer Übermittlung an Dritte der Verantwortliche verpflichtet, jene über die Einschränkung zu informieren, damit dieser seine Verarbeitungsprozesse einschränken kann. Diese Pflicht greift nur insoweit, wie die Unterrichtung möglich und dem Verantwortlichen nicht unzumutbar ist.

Recht auf Datenübertragbarkeit, Art. 20

Wenngleich der Verordnungsgeber Facebook und Google bei der Schaffung dieser Regelungen vor Augen gehabt hat, so verpflichtet der Verordnungsgeber alle Unternehmen, zukünftig, die personenbezogenen Daten, die eine Person dem Unternehmen zur Verfügung gestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zurückzugeben. Auf Wunsch des Betroffenen sollen diese Daten - sofern dies technisch möglich ist - auch direkt an ein anderes Unternehmen übermittelt werden. In Ermangelung von Standards bleibt abzuwarten, wie diese Reglung technisch umgesetzt wird.

Bereits bei Etablierung von neuen Verarbeitungsprozessen sollten Sie sich überlegen, wie Sie künftig sicherstellen können, dass die Daten der betroffenen Person in der geforderten Form ausgelesen und der betroffenen Person übermittelt werden können.

RINK

Sicherheit der Verarbeitung, Art. 32

Wie schon das BDSG, verpflichtet auch die DSGVO zur Umsetzung geeigneter technischer und organisatorischer Maßnahmen, mit denen ein angemessenes Schutzniveau hergestellt werden soll. Die DSGVO stellt allerdings ausdrücklich klar, dass ein risikobasierender Ansatz gefordert wird. Der Verantwortliche hat neben dem Stand der Technik, den Implementierungskosten, der Art, dem Umfang und Umständen, sowie dem Verarbeitungszweck auch die Eintrittswahrscheinlichkeit des Risikos und die Schwere des Eingriffs für die Rechte der betroffenen Person zu bewerten. Unternehmen müssen sich im Rahmen ihres Risikomanagements mit den potentiellen Gefahren und Auswirkungen, sowie den Eingriffsintensitäten ihrer Datenverarbeitungsprozesse auseinandersetzen.

Bei den möglichen Maßnahmen bleibt die DSGVO hinter den exemplarisch aufgezählten Möglichkeiten im BDSG zurück und stellt die aus der ISO 27001 bekannten Schutzziele der Informationssicherheit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme als Schutzziele in den Vordergrund.

Etablieren Sie ein spezifisches Risikomanagementsystem für ihre Datenschutzprozesse. Dieses System sollten Sie nach dem PDCA-Zyklus überwachen, verbessern und dokumentieren.

Auftragsverarbeitung, Art. 28

Neben der sprachlichen Änderung weg von der Auftragsdatenverarbeitung hin zur Auftrags- verarbeitung erhöht die DSGVO in einigen Bereichen die Anforderungen an die Auftragsver- arbeitung. Der Auftragsverarbeiter wird in seinem Verantwortungsbereich stärker in die Pflicht genommen. Der Verordnungsgeber fordert das Vorliegen von „Garantien“ auf Seiten des Auf- tragsverarbeiters hinsichtlich der technischen und organisatorischen Maßnahmen. Auch hat der Auftragsverarbeiter eigene Dokumentationspflichten und haftet gemäß Art. 82 Abs. 1, 4 bei Datenpannen gesamtschuldnerisch zusammen mit dem Verantwortlichen gegenüber der betroffenen Person. Insoweit kann es passieren, dass der Auftragsverarbeiter im Außenverhältnis den kompletten Schaden ersetzen muss und erst im Anschluss die anderen Beteiligten gemäß Art. 82 Abs. 5 in Regress nehmen kann. Auch kann die Aufsichtsbehörde Bußgelder direkt gegen den Auftragsverarbeiter verhängen, wenn die Auftragsverarbeitung nicht den Vorgaben der DSGVO entspricht.

Lediglich in Bezug auf die bisher erforderliche Schriftform bleibt die DSGVO hinter dem BDSG zurück und ermöglicht auch den elektronischen Abschluss einer solchen Vereinbarung.

Gemeinsame Verantwortliche, Art. 26

Die in Art. 4 Abs. 7 angelegte gemeinsame Verantwortung (auch „Joint Controllership“ genannt) ist in Art. 24 geregelt. Dieses in der BDSG nicht vorhandene Gebilde sieht vor, dass neben der alleinigen Verantwortung auch ein arbeitsteiliges Zusammenwirken möglich ist und zielt damit auf kleine und mittlere Unternehmen ab, für die ein derartiges Zusammenwirken essenziell notwendig ist, um wirtschaftlich erfolgreich zu sein. Von dem gemeinsamen Zusammenwirken ist die alleinige Verantwortung einer Stelle und die Auftragsverarbeitung abzugrenzen. Die Unternehmen müssen in diesem Fall eine „kleine Vereinbarung zur Auftragsverarbeitung“ schließen, welche folgende Bestimmungen enthält:

» Aufgabenverteilung der Pflichten nach der DSGVO,

» insbesondere, wie Betroffenenrechte gewahrt werden,

» wer die Informationspflichten nach Art. 13 f. DSGVO erfüllt,

» Festlegung einer Kontaktstelle für den Betroffenen,

» Beschreibung der Funktion und Beziehung zum Betroffenen;

Die Artikel-29 Datenschutzgruppe hat sich bereits 2010 mit diesem Modell auseinandergesetzt und Leitlinien entwickelt, wie die Abgrenzung zu erfolgen hat. Sollten Sie ein derartiges Konzept beabsichtigen, prüfen Sie anhand der Leitlinien, welche Voraussetzungen erfüllt sein müssen (Art. 29- Datenschutzgruppe, WP 169 vom 16.2.2010)

RINK

Meldepflichten bei Datenpannen, Art. 33

Die bisher in § 42a BDSG geregelten Informationspflichten bei Datenpannen von besonderen personenbezogenen Daten wurde in der DSGVO neu geregelt, weiter gefasst und verschärft.

Meldepflicht gegenüber der Aufsichtsbehörde

Art. 33 verpflichtete Verantwortliche, jede Verletzung des Schutzes von personenbezogenen Daten, insbesondere im Falle einer rechtswidrigen Zerstörung, Veränderung oder Verlust, der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden mit einer ausführlichen Beschreibung, den möglichen Auswirkungen und bereits ergriffener Gegenmaßnahmen, zu melden. Von der Meldepflicht erfasst ist auch die unbeabsichtigte Zerstörung oder Veränderung von personenbezogenen Daten. Sie ist nur dann entbehrlich, wenn die Risiken für die Rechte der betroffenen Personen unwahrscheinlich sind.

Meldepflicht gegenüber den Betroffenen

Gegenüber den betroffenen Personen besteht eine Benachrichtigungspflicht, wenn dessen personenbezogene Daten betroffen sind und die Panne voraussichtlich zu einem Risiko für die Rechte und Freiheiten des Betroffenen führt. Die Mitteilung muss ohne unangemessene Verzögerung und in klarer und einfacher Sprache über

» die Art der Verletzung,

» den Namen und die Kontaktdaten des Datenschutzbeauftragten oder eines sonstigen Ansprechpartners für weitere Informationen,

» eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten,

» eine Beschreibung der ergriffenen bzw. vorgeschlagenen Maßnahmen zur Eindämmung der Verletzung bzw. ihrer nachteiligen Auswirkungen

informieren.

Im Rahmen des Business Continuity Managements bzw. der Notfallplanung sollten Prozesse etabliert werden, wie mit Datenpannen umgegangen wird (Risikoanalyse in Form eines Audits, Anschreiben für die betroffenen Personen und Aufsichtsbehörde). Gerade die geforderte Risikoanalyse innerhalb von 72 Stunden wird KMU-Unternehmen ohne Vorbereitung schwerfallen. Auch sollten Sie Ihre Mitarbeiter schulen, dass sie in der Lage sind, Datenschutzverletzungen zu erkennen und zu melden.
Telekommunikationsunternehmen müssen darüber hinaus aufgrund von § 109a TKG Datenschutzverstöße an die Bundesnetzagentur und den Bundesdatenschutzbeauftragten melden. Insoweit unterliegen diese zwei Mitteilungsverpflichtungen. Es bleibt abzuwarten, ob § 109a TKG aufgehoben oder angepasst wird, da die EU-Kommission die e-Privacy Richtlinie, welche Grundlage der vorgenannten Vorschrift ist, derzeit überarbeitet und an die DSGVO anpasst.

RINK

Bestellungspflicht, Aufgaben und Pflichten des Datenschutzbeauftragten, Art. 37ff.

Bestellungspflicht

Die DSGVO bleibt bei der Bestellpflicht hinter dem BDSG zurück und schreibt die Bestellung eines Datenschutzbeauftragten verpflichtend nur vor, wenn die Hauptaktivität des Unternehmens dem Umfang oder seinem Zweck nach die massenhafte, regelmäßige und systematische Beobachtung von Betroffenen erfordert oder deren Kerngeschäft in der massenhaften Verarbeitung sensibler Daten besteht.

Da die Verordnung enthält im Rahmen der Bestellungspflicht eine Öffnungsklausel, welche der deutsche Gesetzgeber aller Wahrscheinlichkeit nach nutzen wird und die Bestellpflicht bereits bei 9+ Angestellten vorsehen wird.

Aufgaben und Pflichten

Neu ist die Pflicht zur Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften, sowie der Strategie des Unternehmens zum Schutz von personenbezogenen Da- ten. Damit wird sein Aufgabengebiet, die Unterrichtung und Beratung des Unternehmens deutlich ausgeweitet.

Als Datenschutzbeauftragter sollten Sie sich intensiv mit den neuen Aufgaben auseinandersetzen. Gerade die Überwachung der Einhaltung von gesetzlichen Bestimmungen und der entsprechenden Strategie erfordert einen kontinuierlichen und dokumentierten Überwachungsprozess. Hier bleibt abzuwarten, inwieweit der deutsche Gesetzgeber einen weiteren Haftungsrahmen auch für den Datenschutzbeauftragten schafft.

Internationale Datenübermittlung, Art 44

Im Bereich der internationalen Datenübermittlung gibt es für den deutschen Rechtsanwender keine großen Änderungen. Wie bisher auch darf eine Übermittlung von personenbezogenen Daten ins Ausland nur erfolgen, wenn die Kommission ein angemessenes Schutzniveau festgestellt hat. Liegt dieser Angemessenheitsbeschluss nicht vor, so müssen die bekannten Instrumente wie Standardvertragsklauseln, Binding-Corporate Rules (BCR) oder die Einwilligung des Betroffenen herangezogen werden. Hinsichtlich der BCR hat der Verordnungsgeber nunmehr die entsprechenden Voraussetzungen in die DSGVO aufgenommen.

Auch hier gilt: Überprüfen Sie alle Datenübermittlungen, ob personenbezogene Daten ins Ausland übermittelt werden, welche Rechtsgrundlage angewendet wird und wie Sie ein angemessenes Datenschutzniveau sicherstellen. Etablieren sie Prozesse, die sicherstellen, dass bei Übermittlungen von personenbezogenen Daten ins Ausland die rechtlichen Rahmenbedingungen geprüft werden. Prüfen Sie immer zuerst, ob die EU-Kommission eine Angemessenheitsentscheidung für das jeweilige Land, in das Sie beabsichtigten, Daten zu übermitteln, erlassen hat. Liegt diese Entscheidung nicht vor, müssen Sie andere Rechtsinstitute prüfen (Einwilligung, Standardvertragsklauseln, Bindung Corporate Rules etc.).

Zertifizierungen, Art. 42

Die meisten bisher am Markt erhältlichen Zertifikate haben meist nur am Rande etwas mit dem Datenschutz zu tun. Weder findet eine vollständige Prüfung aller datenschutzrechtlichen Belange statt noch ist das Zertifizierungsverfahren ausreichend transparent. Allerdings haben Datenschutzzertifizierungen ein großes Potential - insbesondere bei Auftragsverarbeitungen - künftig Klarheit darüber zu schaffen, ob die gesetzlichen Datenschutz-Anforderungen eingehalten werden. So können beispielsweise Cloud-Dienste entscheidend profitieren, da Kunden sich durch ein anerkanntes Zertifikat leichter ein Bild über das Datenschutzniveau eines Unternehmens machen können.

Es bleibt abzuwarten, wann hierfür neue, praxistaugliche Zertifizierungsverfahren entwickelt werden bzw. bestehende Zertifizierungen überarbeitet werden. Als Auftragsverarbeiter sollten Sie die Entwicklungen in diesem Bereich im Blick behalten und ihre Datenschutzorganisation frühzeitig DSGVO konform aufstellen, um von möglichen Zertifikate profitieren zu können.

Haftung, Bußgelder und Sanktionen

Haftungserstreckung auf ausländische Unternehmen, Art. 3

Auch ausländische Unternehmen treffen die Haftungsregelungen der DSGVO, wenn ihre Datenverarbeitung dazu dient, Bürgern der EU Waren oder Dienstleistungen anzubieten bzw. deren Verhalten zu beobachten.

Diese Verantwortlichkeit trifft Unternehmen jeder Größe, also nicht nur Facebook und Google, sondern jeden Anbieter, der sein Angebot auf Bürger der Europäischen Union ausrichtet.

Haftung auf Schadensersatz, Art. 82

Dies DSGVO erweitert die Haftungsverantwortlichkeit des Verantwortlichen deutlich.

Nach dem BDSG ist der Verantwortliche nur zum Ersatz eines Schadens verantwortlich, wenn der betroffenen Person ein materieller Schaden entstanden ist, welcher aus einer unzulässigen oder unrichtigen Datenverarbeitung entstanden ist und der Verantwortliche die nach den Umständen des Falles gebotene Sorgfalt nicht beachtet hat. Die DSGVO geht darüber hinaus und normiert Haftungsregelungen für rein moralische Schäden.

Bußgelder

Der Bußgeldrahmen wird durch die DSGVO deutlich ausgeweitet. Der Verordnungstext legt den Aufsichtsbehörden die Verpflichtung auf, künftig „abschreckende" Bußgeldhöhen zu verhängen. Anders als das BDSG mit seinem Bußgeldrahmen von bis zu 300.000 € können nach der DSGVO bereits bei „einfachen" Verstößen Bußgelder in einer Höhe von bis zu 10.000.000 € bzw. 2 % des gesamten weltweiten Jahresumsatzes des vorgelagerten Geschäftsjahres verhängt werden, je nachdem, welcher Wert höher ist. Bei schwerwiegenden Verstößen können die Geldbußen sogar verdoppelt werden.

Damit wird deutlich, dass die Bußgelder im Rahmen des Risikomanagements eines jeden Unternehmens nicht mehr als ein akzeptiertes Risiko hingenommen werden, sondern behandelt werden müssen.

Es ist angezeigt, alle Datenverarbeitungsprozesse auf den Prüfstand zu stellen. Einerseits nach den neuen Erlaubnisregelungen der DSGVO, andererseits unter Berücksichtigung des erweiterten Haftungstatbestandes.

Auch sollten Prozesse etabliert werden, wie sichergestellt wird, dass vor Einführung neuer Prozesse, die personenbezogene Daten verarbeiten, eine Überprüfung der Zulässigkeit stattfindet.


RINK