© photovs – AdobeStock.com

Technische und organisatorische Maßnahmen

PRIVACYXPERTS

Inhaltsverzeichnis

Sicherheit der Verarbeitung: Kennen Sie sich aus? 1

Schutzmaßnahmen Fehlanzeige? Hier können Sie fündig werden 7

Ruckzuck erledigt: Risiken ausmachen und bewerten 10

Schnell geprüft: Checken Sie die technisch-organisatorischen Maßnahmen 15

Passen die Sicherheitsmaßnahmen? In 7 Schritten finden Sie es heraus 20

Sicherheit der Verarbeitung: Kennen Sie sich aus?

Datenschutzrechtliche Anforderungen umzusetzen ist eine ganz schöne Herausforderung, gerade seit die Datenschutz-Grundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG) anzuwenden sind. Die Sicherheit der Verarbeitung personenbezogener Daten ist ein wichtiger Bestandteil des risikoorientierten Datenschutzes. Kennen Sie sich hier aus?

1. Welche Rahmenbedingungen gelten?

Wichtigste Vorschrift zur Sicherheit der Verarbeitung personenbezogener Daten ist Art. 32 DSGVO. Wenn Sie sich diese Regelung anschauen, sehen Sie sofort: Das Risiko für die Rechte und Freiheiten spielt eine große Rolle bei der Auswahl der Schutzmaßnahmen.

Durch das Verarbeiten personenbezogener Daten an sich bzw. durch die technische Ausführung der Verarbeitung bestehen mehr oder weniger große Risiken für eine Beeinträchtigung der Rechte und Freiheiten der Betroffenen. Diesen Risiken muss der Verantwortliche in Ihrem Unternehmen mit einem angemessenen Schutzniveau entgegenwirken. Daher ist klar: Ohne eine Analyse der Risiken geht es nicht, sprich, der Verantwortliche bzw. Sie müssen in Ihrem Unternehmen vor jeder Datenverarbeitung die folgende Frage stellen:

Welche Risiken bestehen für die Rechte und Freiheiten der Betroffenen, und zwar auf (datenschutz)rechtlicher, organisatorischer und technischer Ebene?

Nach Art. 32 Abs. 1 DSGVO müssen Sie in die Bewertung der Risiken verschiedene Aspekte einfließen lassen. Dazu zählen:

- Stand der Technik
- Art, Umfang, Umstände und Zwecke der Verarbeitung
- unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Stehen die Risiken und ihre Bedeutung fest, kann der nächste Schritt folgen: die Auswahl von technischen und organisatorischen Maßnahmen, um so die Risiken auf ein vertretbares Maß zu reduzieren.

2.Wer ist für die Auswahl und Umsetzung der Maßnahmen verantwortlich?

Generell ist die Umsetzung der Anforderungen aus der DSGVO Sache des Verantwortlichen. Art. 24 Abs. 1 DSGVO legt ähnlich wie Art. 32 DSGVO fest, dass der Verantwortliche unter Berücksichtigung

- derArt, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie
- der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten

geeignete technische und organisatorische Maßnahmen umsetzen muss. Damit muss er sicherstellen und den Nachweis dafür erbringen können, dass die Verarbeitung in Einklang mit der DSGVO erfolgt.

Wer Verantwortlicher ist, ergibt sich aus Art. 4 Nr. 7 DSGVO. Auf den Punkt gebracht: Das ist, wer über die Zwecke und Mittel, sprich das Ob und Wie, einer Verarbeitung personenbezogener Daten entscheidet. Das ist zunächst die Unternehmensleitung. Diese Verantwortung kann diese aber auch auf nachgeordnete Hierarchiestufen (z. B. Bereichs- und Abteilungsleiter) übertragen.

3. Welche Rolle spielen Sie als Datenschutzbeauftragter?

Als Datenschutzbeauftragter gelten Sie nicht als Verantwortlicher für die Verarbeitungen personenbezogener Daten Ihres Unternehmens. Sie trifft auch nicht die Umsetzungsverantwortung für die sich etwa aus Art. 32 DSGVO ergebenden Anforderungen an den technisch-organisatorischen Datenschutz.

Welche Rolle Sie spielen, ergibtsich in erster Linie aus Art. 39 Abs. 1 DSGVO. ImWesentlichen beraten Sie das Unternehmen und die Beschäftigten in Fragen des Datenschutzes. Sie unterstützen beratend bei der Durchführung der Datenschutz-Folgenabschätzung durch den Verantwortlichen. Ferner kontrollieren Sie die Umsetzung der geltenden gesetzlichen oder betrieblichen Festlegungen (z. B. Betriebsvereinbarungen) zum Datenschutz.

Inhalte Verzeichnis von Verarbeitungstätigkeiten	
Verantwortlicher (Art. 30 Abs. 1 DSGVO)	**Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO)**
den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten (Art. 30 Abs. 1 Buchst. a DSGVO)	den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie ggf. des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten (Art. 30 Abs. 2 Buchst. a DSGVO)
Zwecke der Verarbeitung (Art. 30 Abs. 1 Buchst. b DSGVO)	—
Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 Buchst. c DSGVO)	Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden (Art. 30 Abs. 2 Buchst. b DSGVO)
Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen (Art. 30 Abs. 1 Buchst. d DSGVO)	—
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation; geeignete Garantien bei einer Übermittlung im Sinne von Art. 49 Abs. 1 Unterabs. 2 DSGVO (Art. 30 Abs. 1 Buchst. e DSGVO)	ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation; geeignete Garantien bei einer Übermittlung im Sinne von Art. 49 Abs. 1 Unterabs. 2 DSGVO (Art. 30 Abs. 2 Buchst. c DSGVO)
wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 Buchst. f DSGVO)	—
wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO (Art. 30 Abs. 1 Buchst. g DSGVO)	wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 DSGVO (Art. 30 Abs. 2 Buchst. d DSGVO)

4. Welche Maßnahmenschwerpunkte sind nach Art. 32 DSGVO zu betrachten?

Die DSGVO zeigt in Art. 32 Abs. 1 auf, welche Maßnahmen typischerweise in Betracht zu ziehen sind. Dazu zählen:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität,Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheitder Verarbeitung

5. Was versteht man unter dem Stand der Technik?

Auch wenn dieser Begriff sehr verbindlich klingt und den Eindruck erweckt, dass die richtige Technik leicht auszumachen wäre, ist dem nicht so. Der Stand der Technik muss in Bezug auf die jeweilige Technik immer individuell bestimmt werden. Mit einfließen müssen hier vor allem folgende Aspekte:

- Welche Technik ist am Markt verfügbar?
- Ist die Technik aktuell, sprich, werden neue Entwicklungen und gefestigte Forschungsergebnisse berücksichtigt?
- Ist die Technik ausgereift und für den verfolgten Zweck zuverlässig einsetzbar?
- Ist der Einsatz der Technik im Hinblick auf das zu erreichende Ziel wirtschaftlich vertretbar?

Beachten Sie dabei unbedingt: Der sogenannte Stand der Technik darf nicht mit dem Stand der Wissenschaft verwechselt werden. Die Wissenschaft kann schon längst fortschrittlichere Techniken und Maßnahmen entwickelt haben. Diese Weiterentwicklungen müssen jedoch noch lange nicht in der Praxis einsetzbar oder überhaupt für die Nutzung im Unternehmen verfügbar sein.

6. Welche Bedeutung haben die Schutzmaßnahmen aus § 64 BDSG?

Gerade wer schon viele Jahre im Datenschutz tätig ist, kennt noch den Maßnahmenkatalog zum technisch-organisatorischen Datenschutz in der Anlage zu § 9 Satz 1 des alten BDSG. Suchen Sie nach diesen Maßnahmen, finden Sie sie auch im aktuellen BDSG. Wer sich nun freut, dass doch alles beim Alten geblieben ist, dürfte jedoch schnell enttäuscht sein. Das aktuelle BDSG enthält auch Regelungen für öffentliche Stellen, die auf die Richtlinie (EU) 2016/680 zurückgehen. Diese Richtlinie und die darauf basierenden Regelungen im BDSG haben für Unternehmen grundsätzlich keine Bedeutung.

Aus diesem Grund ist § 64 BDSG, der ebenfalls Anforderungen an die Sicherheit der Datenverarbeitung regelt und insgesamt 14Maßnahmenschwerpunkte definiert, für Unternehmen nicht anzuwenden. Das lässt sich nicht bezweifeln. So ergibt sich aus §45 Abs. 1 Satz 1 BDSG, dass die Regelungen des Teils 3 des BDSG nur für öffentliche Stellen gelten, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständig sind.

ACHTUNG: Indirekte Anwendung ist dennoch denkbar. Wird Ihr Unternehmen für eine öffentliche Stelle tätig, kann es passieren, dass man es im Rahmen einer Auftragsverarbeitung verpflichtet, entsprechende Maßnahmen im Sinne von § 64 BDSG vorzusehen. Dabei ist ferner wichtig: Handelt es sich um eine Stelle, die dem Landesrecht unterliegt, beispielsweise Städte und Gemeinden, gilt das Landesdatenschutzgesetz des jeweiligen Bundeslands.

7. Was passiert, wenn man sich technische Schutzmaßnahmen nicht leisten kann?

Technische Maßnahmen haben oft einen entscheidenden Vorteil: Sind sie richtig umgesetzt, funktioniert die Maßnahme quasi automatisch. Anders sieht es bei organisatorischen Maßnahmen aus, etwa Festlegungen, Arbeitsanweisungen oder Richtlinien zum Umgang mit personenbezogenen Daten. Hier spielen eben Menschen, sprich die Beschäftigten, eine wesentliche Rolle. Nur wenn sie gewillt sind, die Festlegung umzusetzen, entfaltet die Schutzmaßnahme auch wirklich ihre Wirkung und kann zur Risikominimierung beitragen.

„Hände in den Schoß legen“ geht nicht

Überhaupt keine Maßnahmen ergreifen, weil das zu teuer wäre, dürfte wohl keine Datenschutzaufsichtsbehörde akzeptieren. Das kommt schon einem „Die Hände in den Schoß legen und hoffen, dass alles gut geht“ gleich. Schlimmstenfalls kann ein schmerzhaftes Bußgeld drohen.

Kann sich Ihr Unternehmen eine bestimmte technische Maßnahme nicht leisten, sollte es stets prüfen, ob es nicht eine kostengünstigere Maßnahme gibt, deren Wirkung beispielsweise durch eine organisatorische Maßnahme ergänzt wird, damit sie die erforderliche Wirkung entfaltet.

Schutzmaßnahmen Fehlanzeige? Hier können Sie fündig werden

Möglicherweise kennen Sie diese Situation: Sie fragen als Datenschutzbeauftragter nach, wie es um diese oder jene Verarbeitung stehe, etwa die Webseite. Ganz schnell erhalten Sie die Antwort, dass alles im grünen Bereich sei. Können Sie dem Glauben schenken? Oft liegt bei den technischen und organisatorischen Schutzmaßnahmen einiges im Argen.

Klar ist: Wer es mit der Sicherheit der Verarbeitung personenbezogener Daten nach Art. 32 Datenschutz-Grundverordnung (DSGVO) nicht so genau nimmt, riskiert nicht nur Ärger mit Betroffenen oder Negativschlagzeilen. Umso wichtiger ist, dass keine Verarbeitung durch das Raster fällt.

Gehen Sie wie folgt Schritt für Schritt vor, um Defizite bei Schutzmaßnahmen zu vermeiden:

1. Schritt: Schauen Sie ins Verzeichnis

Nahezu alle Unternehmen müssen es führen: das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO). Das Verzeichnis mag zwar für manchen in erster Linie eine bürokratische Maßnahme sein. Allerdings ist es gerade für Sie als Datenschutzbeauftragten ein wichtiges Arbeitsmittel. Eine solche Übersicht ermöglicht Ihnen mehr Durchblick. Dennoch sollten Sie sich unbedingt nicht allein darauf verlassen, was Sie vorfinden. Besser ist es, wenn Sie mit offenen Augen durch die Welt gehen.

2. Schritt: Beseitigen Sie weiße Flecken auf der Landkarte

Das Verzeichnis von Verarbeitungstätigkeiten können Sie auch wie eine Datenschutzlandkarte verstehen. Wenn die Inhalte stimmen und alles „kartografiert“ ist, ist alles gut. Gibt es jedoch weiße Flecken auf der Landkarte, heißt es, die Ärmel hochkrempeln. Schließlich sollte es keine Verarbeitungen im Unternehmen geben, die Ihnen unbekannt sind oder die man vor Ihnen versteckt. Gerade die ggf. vor Ihnen versteckten oder auf den ersten Blick weniger bedeutenden Verarbeitungen können für richtig viel Ärger sorgen.

3. Schritt: Gehen Sie auf die Suche

Wenn Sie sich auf die Suche nach unbekannten bzw. ungeprüften Datenverarbeitungsverfahren machen, sollten Sie sich einige Fragen stellen. Diese helfen Ihnen dabei zu bewerten, wie risikobehaftet eine Datenverarbeitung ist und wie sehr es auf passende technische und organisatorische Schutzmaßnahmen ankommt.

Hat die Verarbeitung Außenwirkung?
Darunter fallen alle Datenverarbeitungen, die auf eine Beziehung nach draußen gerichtet und die für andere sichtbar sind. So z. B. ein Online-Shop, das Online-Bewerbungsportal oder das System zur Pflege von Kundenbeziehungen (Customer Relationship Management). Der Außenbezug an sich sorgt schon allein für ein gewisses Risiko. Denken Sie an die Betroffenen, aber auch an Ärger für Ihr Unternehmen, zum Beispiel:

- Schadensersatz
- Bußgeld
- Imageschaden

Gerade Aufsichtsbehörden, Medien und Konkurrenten können problemlos alles unter die Lupe nehmen, was nach außen hin sichtbar ist.

Werden Informationen verarbeitet, die besonders schützenswert sind oder Meldepflichten auslösen?
Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, muss Ihr Unternehmen bei entsprechendem Risiko für die Betroffenen die Aufsichtsbehörde (Art. 33 DSGVO) und ggf. auch die Betroffenen (Art. 34 DSGVO) informieren. Spielen bei einer Verarbeitung besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) eine Rolle, etwa Gesundheitsdaten, ist erhöhter Schutzbedarf angesagt. Bei Betroffenenprofilen, Bank- und Kreditkartendaten sieht das nicht anders aus.

Die Erfahrung zeigt, dass Sie beispielsweise in den folgenden Bereichen auf unbekannte Verarbeitungen stoßen können: Online, Personal, Marketing, IT-Abteilung.

CHECKLISTE: Typische Fundorte für Defzite bei Schutzmaßnahmen			
Bereich	**Hintergrundinformation**	**Geprüft?**	
Online	Schauen Sie sich etwa die Webseite oder den Online-Shop an. Kommt hier Verschlüsselung bei der Datenübertragung zum Einsatz? Wie werden Passwörter gespeichert? Wo liegen Zahlungsinformationen? Wie aktuell sind die eingesetzten Module?	❑ ja	❑ nein
Personal	Gerade Personalbereiche führen manchmal ein gewisses Eigenleben. Denken Sie an Bewerbungsportale, Mitarbeiterumfragen oder Trainingsangebote (z. B. Web-based Trainings). Hier werden Systeme auch gerne selbst „gebastelt", oder es kommen externe Dienstleister zum Einsatz, manchmal mit fragwürdigem Datenschutzverständnis	❑ ja	❑ nein
Marketing	Marketingaktionen können es in sich haben: Schauen Sie einfach einmal danach, wie der Newsletter-Versand organisiert ist, welche Technik oder welche Dienstleister zum Einsatz kommen.	❑ ja	❑ nein
IT-Abteilung	Die IT-Abteilung sorgt dafür, dass die Datenverarbeitung funktioniert, und unterliegt einem hohen Kostendruck. Gern wird da auf günstigere Dienstleister zurückgegriffen. Doch auch bei solchen Konstellationen muss der Schutz der Daten gewährleistet sein und sogar vertraglich vereinbart werden.	❑ ja	❑ nein

Ruckzuck erledigt: Risiken ausmachen und bewerten

Ähnlich wie auch sonst im Leben besteht bei allem, was das Unternehmen macht, ein gewisses Risiko. Das ist auch der Fall, wenn man mit personenbezogenen Daten arbeitet. Egal, ob zufälliger Verstoß gegen gesetzliche Bestimmungen oder leichtsinnige Mitarbeiter, es ist immer möglich, dass etwas schiefgeht. Solche Risiken sind aber nicht gottgegeben. Man kann etwas dagegen tun. Das geht am besten nach einer Risikoanalyse.

Kernelement der DSGVO: Risikobasierter Ansatz

Eine der wesentlichen Besonderheiten der Datenschutz-Grundverordnung (DSGVO) ist der risikobasierte Ansatz. Diesen finden Sie beispielsweise in Art. 24 DSGVO. So müssen Unternehmen zur Umsetzung der DSGVO nicht einfach nur geeignete technische und organisatorische Maßnahmen ergreifen. Wenn die Verantwortlichen diese Maßnahmen festlegen, müssen sie auch die Risiken für die Rechte und Freiheiten natürlicher Personen im Hinblick auf deren Eintrittswahrscheinlichkeit und Schwere berücksichtigen.

Aber auch wenn es um die Sicherheit der Verarbeitung personenbezogener Daten (Art. 32 DSGVO) geht, muss Ihr Unternehmen die Risiken ausmachen, bewerten und mittels geeigneter Maßnahmen die Risiken so behandeln, dass sie weitestgehend minimiert sind.

Risikoanalyse: Eigentlich nicht Ihr Job!

Vielleicht kennen Sie das auch:„Ah, es geht um personenbezogene Daten. Dann kümmert sich der Datenschutzbeauftragte darum.“ Doch diese Aussage ist absoluter Quatsch. Denn: Sie beraten und unterstützen in Datenschutzfragen. Die Durchführungs- und Umsetzungsverantwortung liegt jedoch beim Verantwortlichen, sprich: bei der Unternehmensleitung. Will man also die mitunter aufwendige Risikoanalyse zur Festlegung der erforderlichen technischen und organisatorischen Maßnahmen komplett auf Sie abwälzen, sollten Sie das zurückweisen. Sie können gerne unterstützen und Hilfe leisten. Allerdings müssen andere liefern.

Um im Zusammenhang mit der Risikoanalyse besser beraten zu können, können Sie wie folgt vorgehen:

1. Schritt: Fordern Sie Fakten zur Verarbeitung ein

Einfach ins Blaue hinein lassen sich Risiken nicht annähernd zutreffend ausmachen und bewerten. Sie brauchen eine Faktenlage, auf der alles Weitere basiert. Mit Faktenlage sind die Informationen gemeint, die eine beabsichtigte Datenverarbeitung beschreiben. Darüber, welche Informationen das mindestens sind, brauchen Sie nicht lange grübeln. Schauen Sie in die Vorgaben zum Verzeichnis der Verarbeitungstätigkeiten (Art. 30 Abs. 1 DSGVO).

Doch bei z. B. Zweck, Datenkategorien, technisch-organisatorischen Maßnahmen und Löschfristen sollten Sie es nicht belassen. Lassen Sie sich auch beschreiben, auf welcher Rechtsgrundlage die Verarbeitung personenbezogener Daten stattfinden soll. Idealerweise können Sie sich zusätzlich mit einem Datenflussmodell einen Überblick darüber verschaffen, welche Daten wound wie verarbeitet werden.

Schon in diesem Schritt sollten Sie fragen: Wie wird die Sicherheit der Verarbeitung personenbezogener Daten technisch und organisatorisch sichergestellt? Fragen Sie nach einem Sicherheitskonzept, das etwa die technischen Schutzmaßnahmen zumindest grob beschreibt. Auch ein Betriebskonzept können Sie fordern, das etwa auch die organisatorischen Rahmenbedingungen (Festlegungen, Regeln, Maßnahmen) beschreibt.

2. Schritt: Stellen Sie die Schutzwürdigkeit fest

Wie immer im Datenschutzrecht braucht es für die Verarbeitung von personenbezogenen Daten eine Rechtsgrundlage (Art. 6 Abs. 1 DSGVO). Dabei müssen die Voraussetzungen der Rechtsgrundlage, aber auch die Grundprinzipien aus Art. 5 DSGVO beachtet werden, etwa die Prinzipien der Datenminimierung, Zweckbindung und Vertraulichkeit.

Doch selbst wenn die Voraussetzungen einer Rechtsgrundlage erfüllt sind, bestehen Risiken für die Daten selbst. Um die Risiken zutreffend bewerten zu können, müssen Sie eine entscheidende Bezugsgröße kennen: Sie müssen wissen, wie schutzwürdig die betreffenden personenbezogenen Daten sind.

Um die Zuordnung zu erleichtern und auch zu standardisieren, setzen Unternehmen auf sogenannte Schutzstufen oder Schutzklassen. Dies kann ein Buchstabensystem von A bis E sein, wie es etwa die Landesbeauftragte für den Datenschutz Niedersachsen vorschlägt. Dabei steht A für Daten, die frei zugänglich sind und keinen Schutzbedarf haben. Mit E werden Daten gekennzeichnet, deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit eines Betroffenen beeinträchtigen können.

Ihr Link: https://lfd.niedersachsen.de/startseite/technik_und_organisation/schutzstufen/schutzstufen-56140.html

Andere setzen lieber auf ein Zahlensystem von 0 = Daten ohne Schutzbedarf bis 3 = Daten, die bei falscher Handhabung den Betroffenen erheblich schädigen und in seiner Existenz bedrohen können.

WICHTIG: Die Schadenshöhe sollte zur Geschäftstätigkeit passen. Außerdem: Der Schutzbedarf kann verschiedene Ausprägungen haben. Denken Sie nicht nur an die Vertraulichkeit von Daten. Vielmehr können auch die Verfügbarkeit und Integrität (Unveränderbarkeit) von Daten unterschiedlich ausgeprägt sein. Daher können auch hier entsprechende Stufen oder Klassen vergeben werden.

Schutzstufen, Schutzklassen			
Schutzstufe, Schutzklasse	**Beeinträchtigung/Schadenshöhe für Betroffene bei unsachgemäßem Umgang**	**Schutzbedarf**	**Beispiele für Daten**
0	Keine Beeinträchtigung Gesamtschaden: 0 €	kein	Informationen im Internet, Telefonbucheintrag, Zeitungsbericht
1	Geringe Beeinträchtigung Gesamtschaden: < 5.000 €	niedrig	E-Mail-Adressen für Newsletter, Kfz-Kennzeichen
2	Mittlere Beeinträchtigung Gesamtschaden: < 50.000 €	mittel	Gehaltsabrechnungen, Steuerbescheid; Zahlungsinformationen Kunde
3	Hohe Beeinträchtigung Gesamtschaden: > 50.000 €	hoch	Gesundheitsinformationen, Kundenprofile

3. Schritt: Identifizieren Sie Gefahren

Wenn es darum geht, mögliche Gefahren für den Schutz personenbezogener Daten auszumachen, sollten Sie nicht so vorgehen, dass Sie sich nur am Naheliegenden oder an dem, was alle erwarten, orientieren. Denken Sie auch das Undenkbare. Stellen Sie sich am besten mit Mitarbeitern anderer Bereiche, z. B. IT-Abteilung, nicht die Frage, was getan werden muss, damit der Datenschutz gewährleistet wird. Viel besser ist es zu fragen, was passieren muss, damit es mit dem Datenschutz schiefgeht. So kommen Sie vielleicht bei der Datenverarbeitung „Online-Shop" auch auf Gefahren wie:

- nicht ausreichend qualifizierte Mitarbeiter
- Hacker, die den Online-Shop angreifen
- unzureichende Datensicherungsmaßnahmen

4. Schritt: Machen Sie aus Gefahren Risiken und geben Sie ihnen einen Wert

Haben Sie eine Gefahr identifiziert, müssen Sie einschätzen, wie wahrscheinlich sich diese Gefahr realisiert und der Schaden eintritt. Für die Eintrittswahrscheinlichkeit nutzen Sie ebenfalls ein Zahlensystem, das Sie individuell gestalten können. So z. B.:

1 = niedrig: Schadenseintritt einmal oder innerhalb von fünf Jahren denkbar
2 = mittel: Schadenseintritt mehrmals oder innerhalb von zwei Jahren denkbar
3 = hoch: Schadenseintritt kurzfristig möglich

5. Schritt: Lassen Sie Risiken behandeln

Einfach Risiken durch Multiplikation von Schutzstufe (oder Schadenshöhe) und Eintrittswahrscheinlichkeit einzustufen, reicht nicht. Risiken müssen behandelt werden, um sie auf ein vertretbares Maß zu reduzieren. Dies kann geschehen durch:

- **Risiko minimieren:** Gegenmaßnahmen werden ergriffen, sodass gemäß deren Wirksamkeit das Risiko reduziert wird.
- **Risiko akzeptieren:** Unter Umständen lässt sich das Risiko nicht mit verhältnismäßigem Aufwand (weiter) reduzieren. Dann muss das Risiko getragen werden, und zwar von der Unternehmensleitung.

- **Risiko übertragen:** Es wäre denkbar, sich gegen Risiken etwa zu versichern und das Risiko auf eine Versicherung zu übertragen. In der Praxis dürfte diese Möglichkeit jedoch in der Regel ausscheiden.
- **Risiko vermeiden:** Kommt es nicht zur Verarbeitung oder wird diese anders ausgestaltet, kann ein Risiko ggf. gar nicht erst entstehen.

WICHTIG: Es kann durchaus vorkommen, dass etwa ein Manager mit Ihnen Risiken und Gegenmaßnahmen bewertet und meint, dass die verbleibenden Risiken tragbar seien. Hinterfragen Sie stets, ob er überhaupt dazu befugt ist, diese Einschätzung zu treffen. Gehen Sie im Zweifel lieber auf Nummer sicher: Risiken, Gegenmaßnahmen und Restrisiken stellen Sie der Unternehmensleitung vor, damit diese entscheidet.

6. Schritt: Bewerten Sie auch die Gegenmaßnahmen

Generell können Sie auch standardisiert bewerten, wie gut Gegenmaßnahmen wirken und das Risiko reduzieren. So können Sie die Wirkung im Hinblick auf die Eintrittswahrscheinlichkeit oder Schadenshöhe mit 1 = niedrig, 2 = mittel, 3 = hoch einordnen und die Zahl vom jeweiligen Risikowert in Abzug bringen. Allerdings sollte dabei klar sein: Auch wenn Sie rechnerisch das Risiko auf null bringen, verbleibt meist ein gewisses Restrisiko.

BEISPIEL: ONLINE-SHOP WIRD IN EIGENREGIE BETRIEBEN			
Gefahr/Risiko	**Eintrittswahrscheinlichkeit**	**Schutz-stufe**	**Risikowert (Multiplikation)**
Mitarbeiter macht Konfigurationsfehler und Daten sind für Unbefugte zugänglich.	1 (Grund: Betreuung erfolgt nebenbei durch Mitarbeiter ohne einschlägige Qualifikation.)	2	2
Hacker greifen Online-Shop an.	3 (Grund: Allgemeine Lebenserfahrung zeigt, dass Hacker jede greifbare Sicherheitslücke ausnutzen.)	2	6
Kundendaten gehen aufgrund Serverausfalls verloren.	3 (Grund: kein Datensicherungskonzept vorhanden; Sicherung findet nicht statt; Server und eingesetzte Technik relativ alt und störanfällig)	3	9

Schnell geprüft: Checken Sie die technisch-organisatorischen Maßnahmen

Die technisch-organisatorischen Maßnahmen zu überprüfen ist eine zeitintensive Herausforderung. Nutzen Sie für die Kontrolle der technisch-organisatorischen Maßnahmen eine praxiserprobte Checkliste, die Ihnen hilft, zielorientiert und zeitsparend Ihre Prüfung vorzunehmen. Los geht's!

Sind Sie auf der Suche nach den Regelungen zur Sicherheit der Datenverarbeitung, werden Sie in Art. 32 Datenschutz-Grundverordnung (DSGVO) fündig. Allerdings sind die Anforderungen (z. B. Vertraulichkeit, Integrität) zur Sicherstellung eines angemessenen Schutzniveaus ziemlich abstrakt gehalten. Wollen Sie in diesem Zusammenhang beraten, müssen Sie die einzelnen Anforderungen mit Leben füllen.

Ebenfalls wichtig im Zusammenhang mit den Schutzmaßnahmen: Risikoorientierung ist ein Muss. Alle Maßnahmen zur Sicherheit der Verarbeitung personenbezogener Daten müssen dem Risiko angemessen sein. Das bedeutet, die technisch-organisatorischen Maßnahmen sind in erster Linie an den Risiken zu orientieren, die bei der Verarbeitung für die personenbezogenen Daten entstehen, so z. B. durch Vernichtung,Verlust oder Veränderung, unbefugte Offenlegung von oder unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden (vgl. Art. 32 Abs. 2 DSGVO).

Checkliste vielfältig einsetzbar

Als Datenschutzbeauftragter haben Sie insbesondere Ihrem Beratungs- und Kontrollauftrag nachzukommen (Art. 39 Abs. 1 Buchst.a und b DSGVO). Wollen Sie dem im Zusammenhang mit der Sicherheit der Verarbeitung personenbezogener Daten entsprechen, stellen Sie sich vielleicht sofort die Frage, wie Sie das nur anstellen sollen. Setzen Sie auf die folgende Checkliste. Diese enthält typische Prüfpunkte im Zusammenhang mit dem technisch-organisatorischen Datenschutz. Dabei hat die Checkliste gleich meh-

rere Vorteile: Einerseits ist sichergestellt, dass Sie etwa bei einer Beratung nichts Wichtiges vergessen.Andererseits können Sie die Checkliste auch für eine Kontrolle oder ein Audit einsetzen und so Ihre Prüfmaßnahme bzw. Ihren Prüfkatalog und Ihre Feststellung dokumentieren.

Die Checkliste können Sie aber auch als Fragebogen einsetzen, wenn etwa die zuständige Person beschreiben soll, wie die Maßnahmen konkret umgesetzt werden. In diesem Fall brauchen Sie die Checkliste nur etwas umzubauen: Spalte 2 versehen Sie mit der Überschrift „Umsetzungsbeispiele“ und Spalte 3 mit „Vorgesehene Umsetzung“.

WICHTIG: Es gibt keinen gesetzlich vorgegebenen Prüfrahmen. Insofern können Sie die Checkliste um passende Maßnahmen zur Umsetzung der Anforderungen aus Art. 32 DSGVO ergänzen. Hier können Sie auch auf betriebliche Besonderheiten Rücksicht nehmen.

CHECKLISTE: Maßnahmen zur Sicherheit der Verarbeitung (Art. 32 DSGVO)				
Maßnahme	**Konkrete Umsetzung**	**Ihre Feststellungen**	**Ingesamt in Ordnung?**	
Anforderung: Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)				
Zutritts-kontrolle	Unbefugte haben keinen Zutritt; Einsatz von Chipkarten, Video-überwachung und Alarmanlage	Inaugen-scheinnahme bestätigt Umsetzung.	❑ ja	❑ nein
Zugangskon-trolle	Verwendung eines sicheren Anmeldeverfahrens (Umsetzung Passwortrichtlinie); Entzug von Berechtigungen bei Aufgaben-wechsel und Austritt aus Unter-nehmen		❑ ja	❑ nein
Zugriffs-kontrolle	Berechtigungskonzept regelt Zugriffsrechte; Umsetzung Mini-malprinzip: Vergabe und Entzug von Berechtigungen gemäß Richtli-nie; gegebenenfalls Protokollierung von Zugriffen; Auswertung von Protokollen		❑ ja	❑ nein

(Fortsetzung)

Maßnahme	Konkrete Umsetzung	Ihre Feststellungen	Ingesamt in Ordnung?	
Datentrennung	Speicherung in getrennten physischen oder virtuellen Systemen oder Datenbanken; keine Vermischung von personenbezogenen Daten; Umsetzung Zweckbindung durch Arbeitsanweisung		❑ ja	❑ nein
Pseudonymisierung	gesonderte Aufbewahrung der Referenztabelle; Zugriff auf Tabelle nur im Vieraugenprinzip		❑ ja	❑ nein
Verschlüsselung	Verschlüsselung von Datenträgern mit besonders schutzwürdigen Daten mit Verfahren nach dem Stand der Technik		❑ ja	❑ nein
Anonymisierung	unwiederbringliche Entfernung identifizierbarer Merkmale, sobald möglich und sinnvoll		❑ ja	❑ nein
Löschung (Speicherbegrenzung)	Vernichtung nicht mehr erforderlicher Informationen; Nutzung unterschiedlicher Löschverfahren nach Schutzbedürftigkeit der Informationen; Dokumentation der erfolgreichen Löschung		❑ ja	❑ nein
Anforderung: Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)				
Weitergabekontrolle	Unbefugte Verwendung wird unterbunden durch Verschlüsselung der zu transportierenden Daten.		❑ ja	❑ nein
Eingabekontrolle	Protokollierung der Eingabe und Änderung von Datensätzen; Auswertung der Protokolle		❑ ja	❑ nein

(Fortsetzung)

Anforderung: Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)				
Maßnahme	**Konkrete Umsetzung**	**Ihre Feststellungen**	**Ingesamt in Ordnung?**	
Verfügbarkeitskontrolle	Redundante Datenspeicherung; Durchführung von Back-ups; Notfallmanagement; abgesicherte Stromversorgung		❑ ja	❑ nein
Belastbarkeit der Systeme	regelmäßige Systemtests; Auswertung von Fehlermeldungen; Vorhalten eines Redundanzsystems		❑ ja	❑ nein
Anforderung: Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. c DSGVO)				
Datensicherung	Sicherung der Daten auf anderem System/Datenträger sowie sichere Aufbewahrung in anderem Brandabschnitt; regelmäßiger Test der Datenwiederherstellung (Recovery-Test)		❑ ja	❑ nein
Notfallmanagement	Festlegung von Notfallplänen; Stellvertreter- und Urlaubsregelungen; regelmäßige Übung des „Ernstfalls“		❑ ja	❑ nein
Schnelle Ersatz beschaffung	Systemtechnik kann innerhalb 24 Stunden ausgetauscht werden.		❑ ja	❑ nein
Anforderung: Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen				
Datenschutzmanagement	Erstellung und Einhaltung von einschlägigen Arbeitsanweisungen; Sensibilisierung von Mitarbeitern; Kontrolle durch Datenschutzbeauftragten; Bewertung durch unabhängige externe Stelle		❑ ja	❑ nein
Zwischenfallmanagement	Pläne und Teams für Notfall- und Krisenmanagement		❑ ja	❑ nein
Update-Management	regelmäßige Überprüfung der ergriffenen Maßnahmen auf Eignung, Umsetzung und Wirksamkeit		❑ ja	❑ nein

(Fortsetzung)

Maßnahme	Konkrete Umsetzung	Ihre Feststellungen	Ingesamt in Ordnung?	
Auftrags-kontrolle	Dienstleister werden nach vorgegebenen Kriterien sorgfältig ausgewählt; Datenschutzvereinbarungen bzw. Auftragsverarbeitungsverträge regeln die Zusammenarbeit. Kontrolle der Umsetzung vereinbarter Maßnahmen		❑ ja	❑ nein
Auditierung	Regelmäßige Überprüfung der Umsetzung durch unabhängige Stelle (z. B. Unternehmensrevision); Überprüfung der Zertifizierung des externen Dienstleisters (Auftragsverarbeiter)		❑ ja	❑ nein

Passen die Sicherheitsmaßnahmen? In 7 Schritten finden Sie es heraus

Die Datenschutz-Grundverordnung (DSGVO) ist eine ganz schöne Herausforderung. Und wo man auch hinschaut: Bei jeder Verarbeitung personenbezogener Daten lauern größere oder kleinere Risiken. Diesen muss Ihr Unternehmen mit Schutzmaßnahmen begegnen.

Teil Ihrer Aufgaben ist es, zu Fragen des Datenschutzes zu beraten. Wichtig ist hierbei, dass Sie strukturiert und nachvollziehbar arbeiten. Das sorgt für Transparenz und Verständnis. Falls Sie ein Konzept mit Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (Art. 32 DSGVO) bewerten sollen, setzen Sie auf die folgende praxiserprobte Vorgehensweise:

CHECKLISTE: Prüfung risikoorientierter Schutzmaßnahmen			
	Ihre Aktivität	**Erledigt?**	
1. Schritt	Machen Sie sich schlau Lassen Sie sich Konzepte und Dokumentationen zur betreffenden Verarbeitung vorlegen und schauen Sie insbesondere nach den festgelegten technischen und organisatorischen Schutzmaßnahmen. Versuchen Sie auch, sich selbst ein Bild zu machen, indem Sie etwa bei Webseiten die Kundensicht einnehmen. Prüfen Sie im Bedarfsfall auch, ob die theoretischen Festlegungen mit der praktischen Handhabung übereinstimmen.	❑ ja	❑ nein
2. Schritt	Identifizieren Sie denkbare Risiken. Orientieren Sie sich dabei an Menge und Schutzwürdigkeit der verarbeiteten Daten sowie der technischen Umsetzung. Notieren Sie alle Risiken, die Ihnen in den Sinn kommen. In der Regel bestehen diese Risiken tatsächlich. Allerdings ist es eine Frage der Wahrscheinlichkeit, ob und, wenn ja, welcher Schaden eintritt. Wichtig: Beziehen Sie in die Prüfung unbedingt die in Art. 32 Abs. 2 DSGVO erwähnten Risiken mit ein. So z. B. die unbeabsichtigte oder unrechtmäßige Offenlegung von Daten sowie den unbefugten Zugang zu personenbezogenen Daten.	❑ ja	❑ nein
3. Schritt	Bewerten Sie die identifizierten Risiken Analysieren und bewerten Sie die Risiken nach möglichst objektiven Maßstäben. Schönen Sie auf keinen Fall Ihre Bewertung, weil Ihnen ein Risikowert zu hoch vorkommt.	❑ ja	❑ nein

(Fortsetzung)

	Ihre Aktivität	Erledigt?	
4. Schritt	Ordnen Sie Maßnahmen zur Risikoreduzierung zu Prüfen Sie nun, welche Schutzmaßnahmen geplant sind oder ergriffen wurden und wie diese dazu beitragen, das bestehende Risiko zu reduzieren. Dabei sollten Sie bedenken: dass eine Gegenmaßnahme die Schadensauswirkung oder aber die Wahrscheinlichkeit beeinflussen kann. Auch weniger wirksame Maßnahmen können in der Gesamtschau eine erhebliche Reduzierung bewirken. Welche Aspekte zur Schaffung eines angemessenen Datenschutzniveaus abgedeckt werden müssen, ergibt sich aus Art. 32 Abs. 1 DSGVO.	❑ ja	❑ nein
5. Schritt	Beurteilen Sie, ob mit den Maßnahmen ein angemessenes Schutzniveau erreicht wird Fragen Sie sich, ob bei der Umsetzung der Schutzmaßnahmen davon auszugehen ist, dass die Rechte und Freiheiten der Betroffenen nur so weit beeinträchtigt sind, wie dies unbedingt erforderlich ist. Wichtiger Bestandteil ist hier, dass die Daten auch sicher sind. Auch wenn üblicherweise Restrisiken verbleiben: Bei verständiger Würdigung aller Umstände müssen diese Restrisiken gerade mit Blick auf die Schutzwürdigkeit der Daten und den verfolgten Verarbeitungszweck akzeptabel sein.	❑ ja	❑ nein
	Ihre Aktivität	**Erledigt?**	
6. Schritt	Klären Sie den Prozess zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen Einfach nur Schutzmaßnahmen aufs Papier zu bringen, reicht nicht. Auch mit der Umsetzung ist es nicht getan. Hinterfragen Sie, wie man der Anforderung aus Art. 32 Abs. 1 Buchst. d DSGVO gerecht wird. Eine regelmäßige Wirksamkeitsprüfung und die Dokumentation der Prüfung sind unerlässlich. Klar ist aber auch: Hier muss der Verantwortliche bzw. die für die Verarbeitung verantwortliche Abteilung aktiv werden. Das ist nicht Ihre Aufgabe als Datenschutzbeauftragter.	❑ ja	❑ nein
7. Schritt	Informieren Sie über Ihr (vorläufiges) Ergebnis Bevor Sie lange Berichte schreiben, sollten Sie bedenken: Halten Sie Ihr Resultat fest, allerdings nur als vorläufiges Ergebnis. Laden Sie zum Gespräch ein und diskutieren Sie Ihre Feststellungen. Aufgrund Ihrer Hinweise werden unter Umständen noch umfassende Änderungen vorgenommen.	❑ ja	❑ nein

© Egor – AdobeStock.com

PRIVACYXPERTS

ein Unternehmensbereich des VNR Verlags für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28/9 55 01 50, Fax: 02 28/3 69 64 80
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de

Vorstand: Richard Rentrop

Verantwortlicher i.S.d.P: Michael Jodda, Theodor-Heuss-Str. 2-4, 53095 Bonn

Autor: Andreas Würtz

Satz: Holger Hellendahl, Neuss

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

© 2020 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest, Manchester, Warschau