Umsetzung des neuen Datenschutzrechts im Unternehmen

5 Schritte, mit denen Sie dem Datenschutz Rechnung tragen

PRIVACYXPERTS

Die „Scharfschaltung“ der EU-Datenschutzgrundverordnung (DSGVO) am 25.05.2018 ist nun schon einige Zeit her – trotzdem haben noch nicht alle Unternehmen das neue Datenschutzrecht in die Praxis umgesetzt. Zum einen liegt das an den umfangreichen Informations- und Dokumentationspflichten, zum anderen bestehen nach wie vor noch zahlreiche Unsicherheiten.

Ziel dieses Beitrags ist es daher, Ihnen eine Hilfestellung für die effiziente Umsetzung der zentralen DSGVO-Vorgaben in Ihrem Unternehmen an die Hand zu geben – Schritt für Schritt und möglichst in der richtigen Reihenfolge, nämlich risikoorientiert – getreu dem Motto: „First things first“, also die wichtigen Dinge zuerst. Anhand des folgenden Maßnahmenplans können Sie in fünf Schritten einzelne Handlungsfelder ausfindig machen und deren unterschiedliche Prioritäten erkennen, einordnen sowie die zur Umsetzung erforderlichen Maßnahmen in die Tat umsetzen. Außerdem finden Sie am Ende dieser Broschüre eine Checkliste, anhand derer Sie schnell und übersichtlich den Fortschritt Ihres Unternehmens in Sachen Datenschutz beurteilen können.

Nehmen Sie den Datenschutz ernst – denn andernfalls drohen Sanktionen der Datenschutz-Aufsichtsbehörden und/oder Abmahnungen von Konkurrenten bzw. Verbraucherschutzinstitutionen.

Michael Rohrlich

1. Zuallererst: Verschaffen Sie sich einen Überblick

In einem ersten Schritt ist es sinnvoll, sich zumindest das wichtigste Grundlagenwissen im Bereich Datenschutz anzueignen – denn auch wenn Sie einen besonders qualifizierten Berater hinzuziehen, muss Ihnen eines klar sein: Die Haftung für etwaige Datenschutzverstöße liegt stets bei der Unternehmensführung – ganz gleich ob Sie einen Datenschutzbeauftragten, Datenschutzberater oder sonstigen Experten engagiert haben. Daher ist es unerlässlich, dass Sie die zentralen Begrifflichkeiten und Grundsätze kennen.

Generell dient das Datenschutzrecht dem Schutz von Daten natürlicher Personen, also Menschen.

Es dreht sich im Kern alles um die sogenannten personenbezogenen Daten und deren Verarbeitung. Die entscheidenden Begriffe, nämlich „personenbezogen" und „Verarbeitung", sind jeweils sehr weitgehend zu verstehen. Ein Personenbezug besteht bereits dann, wenn eine natürliche Person identifizierbar ist. Im Zweifel sollten Sie daher davon ausgehen, dass die Daten, die typischerweise in einem Unternehmen vorhanden sind, Personenbezug haben. Lediglich reine Statistik- bzw. Maschinendaten sind ausgeschlossen – etwa Programmcodes oder Alterspyramiden.

Zu den personenbezogenen Daten gehören u.a.

- persönliche Daten (Name, Anschrift, Geburtsdatum ...)
- äußerliche Merkmale (Größe, Haar- und Augenfarbe, Gewicht ...)
- Kontaktdaten (Telefonnummer, Faxnummer, E-Mail-Adresse ...)
- Finanzdaten (Bankverbindung, Gehaltsabrechnung ...)
- Gesundheitsdaten (Krankmeldung, Diagnose, Überweisung ...)
- Fotos mit einer erkennbar abgebildeten Person
- Kfz-Kennzeichen
- IP-Adressen

Dabei wird auch nicht unterschieden, ob die Daten von Kunden, Beschäftigten oder Vertragspartnern stammen – alle müssen gleichermaßen durch das im Datenschutzrecht verankerte Recht auf informationelle Selbstbestimmung geschützt werden.

Nach Maßgabe der DSGVO ist unter dem Begriff „Verarbeitung“ jeder Vorgang im Zusammenhang mit personenbezogenen Daten zu verstehen.

Dabei spielt es keine Rolle, ob dieser Vorgang manuell oder automatisch ausgeführt wird. Es geht hierbei im Grunde um alle möglichen Einzeltätigkeiten, beispielsweise Erheben, Ordnen, Speichern, Verändern, Verwenden, Übertragen oder auch Löschen.

Also sollten Sie auch in Bezug auf den Verarbeitungs-Begriff im Zweifel davon ausgehen, dass eine Verarbeitung im Sinne der DSGVO vorliegt. Allerdings sind rein private Tätigkeiten, wie etwa die Geburtstagsliste in Excel für die Familie und Freunde, vom Anwendungsbereich der DSGVO ausgenommen.

Einer der Grundsätze des Datenschutzrechts besagt, dass es als sogenanntes Verbot mit Erlaubnisvorbehalt konzipiert ist. Daraus folgt, dass jede Verarbeitung personenbezogener Daten erst einmal untersagt ist – es sei denn, sie ist ausnahmsweise erlaubt. Sie benötigen also für jeden Verarbeitungsvorgang eine entsprechende Rechtsgrundlage.

Rechtsgrundlagen für Verarbeitungsvorgänge:
- Einwilligung der Person, deren Daten verarbeitet werden
- gesetzliche Erlaubnisnorm
- überwiegende berechtigte Interessen

Wenn Ihnen also ein gesetzlicher Erlaubnistatbestand zur Seite steht, dann benötigen Sie nicht noch zusätzlich eine Einwilligung. Wenn Sie Daten aufgrund Ihrer überwiegenden Interessen verarbeiten, muss nicht auch noch ein Gesetz Ihnen diese Verarbeitung gestatten. Und so weiter …

Die Einwilligung einer Person für die Verarbeitung ihrer Daten zu haben, klingt erst einmal natürlich optimal. Allerdings zeigen sich in der Praxis hierbei zwei Hürden, die Sie meistern müssen. Einerseits sind die Anforderungen an eine korrekte Einwilligungserklärung u. a. wegen der erweiterten Informationspflichten mit Inkrafttreten der DSGVO gestiegen. Andererseits kann eine Einwilligung jederzeit widerrufen werden, so dass dann mit Wirkung für die Zukunft die Rechtsgrundlage für die Datenverarbeitung wegfällt.

Wenn Sie Ihre berechtigten Interessen als Rechtsgrundlage wählen, müssen Sie diese mit den Interessen der Personen, deren Daten Sie verarbeiten (die sog. Betroffenen), abwägen. Zudem müssen Sie das Ganze dokumentieren und im Zweifel auch nachweisen können, dass Ihre Interessen die der Betroffenen überwiegen – und warum. Dabei besteht stets das Risiko, dass eine Datenschutz-Aufsichtsbehörde oder ein Gericht die Sachlage anders bewertet.

Ideal ist folglich, wenn man eine gesetzliche Erlaubnis als Rechtsgrundlage heranziehen kann. Die DSGVO hat die wichtigsten sozusagen mit „an Bord".

Eine Datenverarbeitung ist insbesondere zulässig...
- zur Erfüllung eines Vertrages,
- zur Durchführung vorvertraglicher Maßnahmen oder
- aufgrund einer rechtlichen Verpflichtung.

Im Rahmen der klassischerweise anfallenden Tätigkeiten in Unternehmen, wie etwa der Bearbeitung von Aufträgen, der Verwaltung von Beschäftigtendaten oder auch der Buchhaltung, bestehen oftmals gesetzliche Erlaubnistatbestände, weshalb hier nicht noch zusätzlich berechtigte Interessen oder Einwilligungen vorliegen müssen. Die Daten Ihrer Kunden benötigen Sie in aller Regel zur Durchführung (vor-)vertraglicher Maßnahmen, die Daten Ihrer Mitarbeiter zur Zahlung von Löhnen oder auch zur Leistung von Sozialabgaben usw.

Auf Einwilligungen oder berechtigte Interessen sollten Sie nur dann zurückgreifen, wenn es für eine bestimme Tätigkeit keine passende Vorschrift in der DSGVO, im BDSG oder in Spezialgesetzen gibt. So benötigen Sie beispielsweise regelmäßig eine vorab erteilte Einwilligung für den Versand elektronischer Werbung, also beispielsweise für Ihren Newsletter.

DSGVO: Aktuelles Basiswissen

Ein Drittel der EU Unternehmen arbeiten nicht DSGVO konform. Wie steht es um Ihr Unternehmen? Für wen genau gilt die DSGVO? Und was müssen Sie wirklich tun? Dieser Spezial-Report liefert die Antworten.

Jetzt brandaktuelles Wissen zum Thema Datenschutz sichern

DSGVO: Was Sie jetzt noch umsetzen sollten...

Arbeiten Sie schon datenschutzkonform?

Seit dem 25.05.2018 sind die neuen Datenschutzregeln verbindlich, und zwar nicht nur die **DSGVO,** sondern auch das **neue Bundesdatenschutzgesetz. Das ist nun schon einige Tage her...**

Wenn Sie bisher noch relativ entspannt abgewartet haben oder die Unternehmensleitung vielleicht die Bedeutung dieser Wände im Datenschutz noch nicht erkannt hat, dann wird es jetzt **höchste Zeit loszulegen und sich ins Zeug zulegen.**

Wir klären die drängendsten Fragen!

Die DSGVO und das neue Bundesdatenschutzgesetz haben viele Änderungen mit sich gebracht, aber so manches bleibt auch beim Alten. Die ersten Monate sind rum und die ersten Gerichte fällen Urteile über Bußgelder von DGSVO Verstößen.
Hier trifft es nicht nur die großen Unternehmen. Auch kleinere Unternehmen werden von den Aufsichtsbehörden geprüft...

Manche wichtige Frage lässt sich gleich beantworten. Etwa die nach der Haftung und den zukünftigen Aufgaben des Datenschutzbeauftragten. Auch zum schwierigen Thema Auftragsverarbeitung können wir Ihnen einige Tipps an die Hand geben.

Für Aufregung sorgt das Thema Rekord-Bußgelder, die die DSGVO vorsieht. Und wir sehen, dass diese Extrem-Bußgelder gar nicht so unwahrscheinlich sind. Kann es Sie auch treffen?

Bei diesen und vielen weiteren Fragen unterstützt Sie der **kostenlose Spezialreport „DSGVO: Aktuelles Basiswissen".**

Dank zahlreicher Tipps, Musterformulierungen, Checklisten und konkreten Empfehlungen ist der kostenlose Spezialreport "DSGVO: Aktuelles Basiswissen" eine **wertvolle Lektüre für Datenschutzbeauftragte und andere Datenschutzverantwortliche!**

Das Beste daran ist: Den Spezialreport können Sie jetzt gleich hier völlig kostenlos zum Download anfordern.

Jetzt gleich kostenlos anfordern

2. Sofort handeln: Maßnahmen, die jeder wahrnimmt

Die nächsten Schritte zur DSGVO-Compliance sollten darin bestehen, solche Maßnahmen umzusetzen, die besonders große Außenwirkung haben. Denn diese sind von Datenschutz-Aufsichtsbehörden oder Konkurrenten sehr einfach nachzuvollziehen.

Besonders wichtig sind daher zwei Aspekte:
- Erfüllung der Informationspflichten
- ggf. Benennung und Meldung eines Datenschutzbeauftragten (DSB)

Die Informationspflichten aus der DSGVO müssen Sie, unabhängig von Ihrer Mitarbeiteranzahl, in jedem Fall erfüllen. Sie müssen sowohl für Ihre alltäglichen Aufgaben als auch speziell für Ihre Tätigkeit im Internet – also etwa auf Ihrer Website, in Ihrem Webshop oder auch in Ihren Social-Media-Profilen – Datenschutzhinweise bereitstellen.

Sie benötigen also zumindest zwei Dokumente:
- allgemeine Datenschutzhinweise für Ihre „Offline-Geschäftstätigkeiten“
- Datenschutzerklärung für Ihre Webseite etc.

Verpflichtende Informationen für Ihre Datenschutzerklärungen:
- Name und Kontaktdaten Ihres Unternehmens
- Kontaktdaten eines etwaigen Datenschutzbeauftragten
- Zwecke der Datenverarbeitung
- Rechtsgrundlagen der Datenverarbeitung
- ggf. die Empfänger oder die Kategorien von Empfängern, denen Sie personenbezogene Daten übermitteln
- Dauer der Datenspeicherung bzw. Kriterien für die Festlegung dieser Dauer
- Hinweis auf die Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung, Widerruf, Widerspruch, Beschwerde und Datenportabilität, d. h. Datenübertragbarkeit)
- ggf. Hinweis auf gesetzliche oder vertragliche Pflichten zur Bereitstellung der Daten und die Folgen der Nichtbereitstellung

Die Online-Präsenz hat oberste Priorität!

In Ihren Online-Präsenzen müssen Sie über die dort eingesetzten Technologien informieren, mit denen Sie personenbezogene Daten verarbeiten (insbesondere die IP-Adresse). Es geht hier also beispielsweise um Google Analytics, Kontaktformulare, Newsletter, Social Plugins oder SSL-Verschlüsselung.

Um diese Datenschutzhinweise zu erstellen, sollte idealerweise ein Fachmann beauftragt werden. Alternativ können Sie auch einen der im Internet angebotenen Generatoren nutzen, wie z. B. unter www.wbs-law.de/it-recht/datenschutzrecht/datenschutzerklaerung-generator oder auch www.datenschutz-generator.de. Um diese Tools zu nutzen, benötigen Sie allerdings diverse Informationen juristischer wie technischer Natur.

In jedem Fall sollte Ihre Online-Datenschutzerklärung oberste Priorität haben, denn sie kann jederzeit von überall auf der Welt abgerufen werden.

Hinweis: Achten Sie darauf, dass diese Erklärung auf allen Endgeräten, insbesondere auf Tablet-PCs oder Handys, gleichermaßen gut lesbar dargestellt wird. Der Einsatz von „responsive design“ ist hier das Zauberwort, denn dadurch passt sich die Darstellung z. B. einer Internetseite oder eine App automatisch der Größe des Bildschirms des jeweiligen Endgerätes an.

Gleich danach sollten Sie Ihre allgemeinen Datenschutzhinweise erstellen (lassen)

Die allgemeinen Datenschutzhinweise müssen jedem neuen Kunden, jedem neuen Mitarbeiter, jedem neuen Vertragspartner usw. zur Verfügung gestellt werden. Wer sie bereits erhalten hat, muss kein weiteres Mal informiert werden.

Die allgemeinen Datenschutzhinweise müssen prinzipiell jederzeit mitgeteilt werden können – sei es per E-Mail, in Briefen oder auch am Telefon bzw. im persönlichen Gespräch. Die DSGVO macht hier keinen Unterschied zwischen einem kurzen Gespräch am Messestand, dem Austausch von Visitenkarten, einem Telefonat oder einer E-Mail etc. Zumindest ein kurzer Hinweis auf die eigenen Datenschutzhinweise ist Pflicht.

TIPP: Idealerweise sollten Sie Ihre allgemeinen Datenschutzhinweise also als PDF-Datei auf eine Webseite laden, die unter einer aussagekräftigen, nicht allzu komplizierten Adresse erreichbar ist (z. B. „www.mustermann.de/datenschutz“).

Darauf können Sie dann per sprechendem Link, wie etwa „Datenschutzhinweise unter www.mustermann.de/datenschutz“, auf verschiedenen Kanälen hinweisen.

Beispiel für einen „sprechenden Link“:
„Hier finden Sie unsere Datenschutzhinweise: www.xyz.de/datenschutz“

Sie können diesen Hinweis auf Ihrem Briefkopf platzieren, auf Briefumschläge drucken lassen, in Ihre E-Mail-Signatur integrieren und/oder auf Ihrem Anrufbeantworter hinterlassen. Auch ein Aushang im Ladenlokal oder ein Aufsteller am Empfang ist möglich.

Sie sollten so viele Hinweise wie möglich platzieren, damit alle Ihre Kunden, Vertragspartner oder Beschäftigten sie zur Kenntnis nehmen können.

Sowohl die allgemeinen Datenschutzhinweise als auch die Online-Datenschutzerklärung müssen jeweils
- präzise,
- transparent,
- verständlich und
- leicht zugänglich

erfolgen.

Darüber hinaus müssen sie in einer klaren und einfachen Sprache formuliert sein.

Da die Inhalte recht umfangreich ausfallen können, sollten sie gut strukturiert bzw. „leicht verdaulich“ aufbereitet werden. Dazu bietet sich etwa eine vorangestellte Gliederung oder auch eine Präsentation in einer Frage-Antwort-Form an. Jedenfalls sollte der Text nicht mit Fachausdrücken oder „Behördendeutsch“ überfrachtet werden.

+++ Rekordbußgelder wegen Datenschutz-Verstößen: 35 Mio. € Strafe gegen Handelskette, 14,5 Millionen gegen Immobilienkonzern … Druck auf Datenschutzbeauftragte steigt! +++ Alle Bereiche im Unternehmen jetzt systematisch prüfen +++

Mit welcher dieser 57 Checklisten wollen Sie bei der Umsetzung von DSGVO, BDSG & Co. jetzt alles richtig machen?

Das gab's noch nie: Datenschutz-Experten veröffentlichen die wichtigsten Datenschutz-Checklisten in einem Paket. Mit den Checklisten sichern Sie sich diese Vorteile:

- Sie **prüfen jeden Bereich** Ihres Unternehmens gründlich und fachmännisch (weil in den 57 Checklisten genau erklärt ist, worauf es bei jedem Prüfschritt ankommt)
- Sie **decken Datenschutz-Lücken auf** – auch in Bereichen, wo man es normalerweise nicht erwartet (weil die Checklisten auch Bereiche wie private Handy-Nutzung, Home-Office und Datenvernichtung nach DIN 6399 abdecken)
- Sie erhalten **Sicherheit auch bei schwammigen Vorgaben** von DSGVO und BDSG (z.B. wenn Sie die „Verhältnismäßigkeit" prüfen sollen)
- Sie kommen Ihrer **Beratungsfunktion** spielend leicht nach (weil Sie durch die Prüfpunkte das perfekte Grundschema für jede Stellungnahme haben)

GRATIS Download

Hier als Gratis-Geschenk erhalten

Ihre Prämie für den Test von "Datenschutz aktuell" - seit über 15 Jahren geprüfte Informationen für interne und externe Datenschutzbeauftragte.

„JA! Ich möchte mit den 57 Checklisten jetzt JEDEN Bereich im Unternehmen auf DSGVO, BDSG & Co. überprüfen.

Enthält Geschenke im Wert von 219,83 €

Benötigt Ihr Unternehmen einen Datenschutzbeauftragten?

Bei der Frage müssen sowohl die DSGVO als auch das BDSG zu Rate gezogen werden. Unterm Strich läuft es in den meisten Fällen wohl auf die Frage hinaus, wie viele Beschäftigte es im Unternehmen gibt. Sind mehr als neun Beschäftigte vorhanden, besteht in aller Regel die Pflicht zur Benennung eines DSB.

Achtung: Bei der Beschäftigtenanzahl zählt jeder Kopf, also z. B. auch Teilzeit- oder Aushilfskräfte, Leiharbeiter, Studenten, Azubis etc.!

Unternehmen mit weniger als zehn Beschäftigten brauchen nur dann einen DSB, wenn sie in Branchen tätig sind, die besonders sensible Daten verarbeiten – z. B. Markt- und Meinungsforschung, Detektei, Adresshandel oder Online-Werbenetzwerk.

WICHTIG: Wenn Ihr Unternehmen zu denjenigen gehört, die einen DSB benennen müssen (oder dies freiwillig tun), müssen Sie diesen der Aufsichtsbehörde melden, die für Sie zuständig ist.

Wenn Ihr Unternehmen z. B. in NRW ansässig ist, dann ist die NRW-Datenschutzaufsicht für Sie zuständig, wenn es in Bayern seinen Sitz hat, ist es die bayerische etc.

LINK-TIPP: Im Internet finden Sie unter www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html eine Liste mit den Anschriften der Datenschutz-Aufsichtsbehörden und außerdem Online-Formulare, über die Sie Ihren DSB melden können.

NEU: Das große 99-teilige Präventions-Paket für Datenschutzbeauftragte

Mit diesem umfangreichen Paket zu DSGVO, BDSG, TMG und IT-Sicherheit erhalten Sie 99 wichtige Vorlagen, Urteile und Checklisten für Ihre Arbeit als Datenschutzbeauftragter zum Sofort-Einsatz:

GRATIS
Download

- Mit diesen 34 Checklisten **prüfen Sie JEDEN Anwendungsfall rechtlich sicher** ... und verfassen professionelle Stellungnahmen
- Ihr Verarbeitungsverzeichnis und andere **Dokumentationen genügen im Prüfungsfall den hohen Ansprüchen der Behörden.**
- Sie **schließen** zusammen mit der IT eventuell vorhandene **Lücken bei der Datensicherheit** (weil Sie einen Überblick haben „was die IT da eigentlich macht").
- Sie kennen **aktuelle Urteile** und wissen, was Sie daraus für Schlüsse für Ihr Unternehmen ziehen
- **Datenschutz in der Personalabteilung:** Was der Chef darf und welche Rechte die Mitarbeiter haben
- Wie Sie Datenschutz in Ihrem Unternehmen **strategisch aufbauen**

„JA! Ich will beim Datenschutz von Anfang an alles richtig machen!"
GRATIS-Präventions-Paket hier herunterladen

Insgesamt 5 Geschenke im Wert von 239,38 € erhalten

3. Ebenfalls wichtig: Vorgänge, die Ihre Geschäftsbeziehungen betreffen

Weiterhin relevant sind solche Maßnahmen, die zwar keine weltweite Außenwirkung haben, aber dennoch gegenüber Dritten wirken. Hierzu gehören u. a. Verträge mit Dienstleistern oder auch Einwilligungserklärungen für den Versand elektronischer Werbung. Sofern Sie vor dem 25. Mai 2018 Einwilligungen nach alter Rechtslage korrekt eingeholt haben, gelten diese in der Regel weiterhin. Zukünftig sind natürlich die entsprechenden DSGVO-Vorgaben zu beachten.

Wenn Sie Dritte mit Tätigkeiten beauftragen, bei denen diese mit personenbezogenen Daten Ihres Unternehmens, z. B. von Ihren Kunden oder Mitarbeitern, in Berührung kommen, muss neben dem eigentlichen Dienst- oder Werkvertrag auch noch ein sog. Auftragsverarbeitungsvertrag (AV-Vertrag) geschlossen werden. Allerdings ist es diesbezüglich momentan leider so, dass es noch nicht abschließend geklärt ist, wann welche Tätigkeit als AV-Verhältnis im Sinne der DSGVO einzustufen ist.

Typische Auftragsverarbeiter sind etwa

- Werbeagenturen,
- Newsletter-Versender,
- Hosting-Dienstleister (z. B. Webseite, E-Mail),
- IT-Dienstleister,
- Cloud-Dienstleister,
- Entsorgungsunternehmen oder auch
- Anbieter von Online-Analyse-Tools (z. B. Google Analytics).

Tätigkeiten von Angehörigen freier Berufe, wie z. B. Anwälte, Ärzte oder Steuerberater, zählen regelmäßig nicht als Auftragsverarbeitung. Das Gleiche gilt für Versandunternehmen wie die Deutsche Post, DPD etc. und auch für Banken. Bei der Beurteilung, ob ein AV-Verhältnis vorliegt oder nicht, stellt sich wohl letztlich die Frage, wie die Hauptaufgabe des betreffenden Dienstleisters genau aussieht. Es geht darum, ob er besonders die Verarbeitung bestimmter (personenbezogener) Daten als Ihr „verlängerter Arm“ durchführen soll oder ob dies nur „nebenbei“ geschieht.

WICHTIG: Fertigen Sie eine Aufstellung der von Ihnen beauftragten Dienstleister und die fachliche Einstufung an, ob und in welchem Fall ein AV-Verhältnis gegeben ist!

In diesen Fällen liegt typischerweise ein Auftragsverarbeitungsverhältnis vor:

- EDV-technische Arbeiten für Lohn-und Gehaltsabrechnung
- Cloud-Computing
- Werbeadressenverarbeitung in sog. Lettershops
- Verarbeitung von Kundendaten durch Callcenter ohne wesentliche eigene Entscheidungsspielräume
- Newsletter-Dienstleister
- Datenerfassung, Datenkonvertierung oder Einscannen von Dokumenten
- Auslagerung der Backup-Sicherheitsspeicherung und anderer Archivierungen
- Datenträgerentsorgung durch Dienstleister
- Zentralisierung bestimmter „SharedServices-Dienstleistungen“ innerhalb eines Konzerns, wie Dienstreisen-Planungen oder Reisekostenabrechnungen
- ärztliche/zahnärztliche Verrechnungsstellen
- Sicherheitsdienste, die an der Pforte Besucher- und Anliefererdaten erheben

In diesen Fällen muss ein AV-Vertrag geschlossen werden.

LINK-TIPP: Ein Vertragsmuster inklusive weiterführender Anmerkungen finden Sie online z. B. unter www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo.

DSGVO: Aktuelles Basiswissen

**Ein Drittel der EU Unternehmen arbeiten nicht DSGVO konform. Wie steht es um Ihr Unternehmen?
Für wen genau gilt die DSGVO? Und was müssen Sie wirklich tun? Dieser Spezial-Report liefert die Antworten.**

Jetzt brandaktuelles Wissen zum Thema Datenschutz sichern

DSGVO: Was Sie jetzt noch umsetzen sollten...

Arbeiten Sie schon datenschutzkonform?

Seit dem 25.05.2018 sind die neuen Datenschutzregeln verbindlich, und zwar nicht nur die **DSGVO,** sondern auch das **neue Bundesdatenschutzgesetz. Das ist nun schon einige Tage her...**

Wenn Sie bisher noch relativ entspannt abgewartet haben oder die Unternehmensleitung vielleicht die Bedeutung dieser Wände im Datenschutz noch nicht erkannt hat, dann wird es jetzt **höchste Zeit loszulegen und sich ins Zeug zulegen.**

Wir klären die drängendsten Fragen!

Die DSGVO und das neue Bundesdatenschutzgesetz haben viele Änderungen mit sich gebracht, aber so manches bleibt auch beim Alten. Die ersten Monate sind rum und die ersten Gerichte fällen Urteile über Bußgelder von DGSVO Verstößen.
Hier trifft es nicht nur die großen Unternehmen. Auch kleinere Unternehmen werden von den Aufsichtsbehörden geprüft...

Manche wichtige Frage lässt sich gleich beantworten. Etwa die nach der Haftung und
den zukünftigen Aufgaben des Datenschutzbeauftragten. Auch zum schwierigen Thema Auftragsverarbeitung können wir Ihnen einige Tipps an die Hand geben.

Für Aufregung sorgt das Thema Rekord-Bußgelder, die die DSGVO vorsieht. Und wir sehen, dass diese Extrem-Bußgelder gar nicht so unwahrscheinlich sind. Kann es Sie auch treffen?

Bei diesen und vielen weiteren Fragen unterstützt Sie der **kostenlose Spezialreport „DSGVO: Aktuelles Basiswissen".**

Dank zahlreicher Tipps, Musterformulierungen, Checklisten und konkreten Empfehlungen ist der kostenlose Spezialreport "DSGVO: Aktuelles Basiswissen" eine **wertvolle Lektüre für Datenschutzbeauftragte und andere Datenschutzverantwortliche!**

Das Beste daran ist: Den Spezialreport können Sie jetzt gleich hier völlig kostenlos zum Download anfordern.

Jetzt gleich kostenlos anfordern

4. Lästig, aber unumgänglich: Dokumentation

Es gibt Maßnahmen, die nur intern ablaufen, die Sie aber gleichwohl nicht vernachlässigen dürfen. Hier ist in erster Linie das sogenannte Verzeichnis von Verarbeitungstätigkeiten, oder kurz Verarbeitungsverzeichnis, zu nennen. Dieses dient Ihnen als Nachweis Ihrer Datenschutzmaßnahmen. Einsicht nehmen darf hier jedoch nur die Datenschutz-Aufsichtsbehörde auf Anfrage.

Das Verarbeitungsverzeichnis besteht aus diesen drei Teilen:

- Teil 1: „Deckblatt“
- Teil 2: Beschreibung der Verarbeitungstätigkeiten (Hauptteil)
- Teil 3: Auflistung der technischen und organisatorischen Maßnahmen (TOM) zum Datenschutz

Alle Teile zusammengenommen – inklusive verschiedener Anlagen (z. B. das Löschkonzept, die Passwortrichtlinie, die Benutzerrechteregelung oder das Backup-Konzept) – bilden das Verarbeitungsverzeichnis. Ob Sie es auf Papier oder in Dateiform führen, bleibt Ihnen überlassen.

Wichtig: Die Unterlagen müssen aus sich heraus verständlich sein und den Status quo Ihrer Datenschutzorganisation abbilden! Die Behörde muss daraus also beispielsweise ablesen können, zu welchen Zwecken und auf welcher Rechtsgrundlage Sie welche Daten verarbeiten, wann und wieso Sie welche Daten löschen, welche technischen und organisatorischen Maßnahmen Sie zum Schutz der Daten ergriffen haben usw.

Teil 1: „Deckblatt“

Im Wesentlichen führen Sie hier Namen und Kontaktdaten Ihres Unternehmens sowie – falls vorhanden – die Daten Ihres Datenschutzbeauftragten auf.

Leider gibt die DSGVO für die praktische Umsetzung keine wirklich brauchbare Hilfestellung, so dass insbesondere die Erstellung des zweiten Teils nicht ganz trivial ist. So ist u. a. nicht vorgegeben, wie grob oder feingliedrig die einzelnen Verarbeitungstätigkeiten aufgelistet werden müssen.

Teil 2: Beschreibung der Verarbeitungstätigkeiten

Diese vorgegebenen Mindestangaben müssen in jedem Fall enthalten sein:

- der Zweck der Verarbeitungstätigkeit (z. B. Kundenbetreuung, Personalverwaltung oder Werbezwecke)
- die Kategorien der betroffenen Personen (z. B. Kunden, Beschäftigte, Lieferanten)
- die Kategorien der verarbeiteten Daten (z. B. Name, Adressdaten, Kontaktdaten, Vertragsdaten)
- eventuell auch Kategorien von besonders sensiblen Daten (z. B. Gesundheitsdaten, Gewerkschaftszugehörigkeit, Religion)
- die Kategorien von Empfängern der Daten (z. B. Bank, Finanzamt, Krankenkasse, Dienstleister)
- eine eventuell geplante Übermittlung der Daten in Länder außerhalb der EU
- einschlägige Lösch- bzw. Aufbewahrungsfristen

Schwierigkeiten bestehen oftmals dabei, erst einmal zu identifizieren, welche Verarbeitungsvorgänge überhaupt im Unternehmen bestehen. Hier kann man sich zunächst an der Organisationsstruktur des Unternehmens orientieren.

Es gibt Bereiche, deren Aufgaben regelmäßig durchgeführt werden müssen:

- Unternehmensführung
- Buchhaltung
- Personalabteilung
- IT
- Marketing

Diese Fachbereiche im Unternehmen entsprechen einzelnen Verarbeitungstätigkeiten, zumindest bei einer sehr groben Aufteilung. Um den datenschutzrechtlichen Anforderungen zu genügen, sollten diese jedoch noch etwas mehr aufgegliedert werden. So können etwa die Aufgaben der Personalabteilung mit verschiedenen Einzelaufgaben umrissen werden, wie z. B. Bewerbermanagement, Urlaubsplanung, Lohnzahlung usw.

TIPP: Wenn Sie diese Einzeltätigkeiten aller Fachbereiche beispielsweise in einer Excel-Liste untereinander aufführen und die Spalten daneben jeweils mit den oben genannten Pflichtangaben befüllen, haben Sie zumindest schon mal das Grundgerüst für Ihr Verarbeitungsverzeichnis.

HINWEIS: Vergessen Sie nicht Ihren Internetauftritt, gegebenenfalls den Versand Ihres Newsletters und/oder die Durchführung von Events, denn auch dies sind Verarbeitungstätigkeiten, die im Verarbeitungsverzeichnis zu erfassen sind.

Teil 3: Auflistung der technischen und organisatorischen Maßnahmen zum Datenschutz

Dazu gehören u. a. Aspekte der IT-Sicherheit wie beispielsweise:
- die Sicherung des Serverraums
- der Einsatz von Nutzernamen und Passwort
- der Betrieb einer Firewall
- Antiviren-Programme
- usw.

Datenschutz umfasst aber nicht nur die IT-Sicherheit, sondern reicht auch in den analogen Bereich. Hier gibt es Maßnahmen wie z. B.
- die Absicherung des Zugangs zum Gebäude durch Alarmanlagen
- den Einsatz von Sicherheitsschlössern o. Ä.

Sie dürfen aber auch die organisatorischen Maßnahmen nicht vergessen, denn
- Arbeitsanweisungen oder
- Betriebsvereinbarungen, z. B. ein Verbot der privaten Internet- oder E-Mail-Nutzung am Arbeitsplatz oder eine sog. „Clean-Desk-Policy“,

sind ebenfalls wichtige Datenschutzmaßnahmen. Durch Letztere zum Beispiel wird sichergestellt, dass alle Beschäftigten die Unterlagen, die personenbezogene Daten enthalten, in eine Schublade oder in einen Schrank räumen, bevor sie Feierabend machen, und dadurch dann ein sauberer Schreibtisch (engl.: „clean desk“) entsteht.

Ebenso sollte der Zugriff auf Computer gesperrt werden, wenn ein Mitarbeiter in die Pause geht.

Vorlagen für Verarbeitungsverzeichnisse finden Sie auch online, beispielsweise auf der Webseite des Bayerischen Landesamtes für Datenschutz (www.lda.bayern.de/de/kleine-unternehmen.html).

5. Dranbleiben: Schulen Sie Ihre Mitarbeiter

Mit den Schritten 1 bis 4 erfüllen Sie die Mindestanforderungen gemäß der DSGVO. Darüber hinaus müssen Sie auch darauf eingestellt sein, dass betroffene Personen ihre Rechte ausüben und z. B. Auskunft über die von ihnen verarbeiteten Daten verlangen. Sie müssen in jedem Fall reagieren.

Das bedeutet: Alle Ihre Mitarbeiter müssen zumindest die Grundlagen des Datenschutzrechts kennen.

Zum einen fordert dies das Gesetz und zum anderen kann effektiver Datenschutz nur so funktionieren – indem alle ihn befolgen. Das bedeutet letztlich aber auch, dass sämtliche Beschäftigten regelmäßig geschult werden müssen, um nicht nur die Grundkenntnisse zu haben, sondern auch die aktuellen Entwicklungen im Bereich Datenschutz kennenzulernen.

Ebenfalls wichtig ist, dass Sie sich nicht auf der einmal erlangten DSGVO-Compliance „ausruhen". Sie müssen sich regelmäßig selbst überprüfen, ob sich z. B. Ihre Verarbeitungsvorgänge geändert haben, zum Beispiel bei Einführung eines neuen Zeiterfassungssystems, oder ob die technische Entwicklung Neuerungen mit sich bringt, die für das eigene Unternehmen relevant sind.

TIPP: Zumindest einmal pro Jahr ist eine solche Selbst-Prüfung erforderlich.

Checkliste DSGVO-Umsetzung	
Maßnahmen zur DSGVO-Umsetzung	**Bitte abhaken, wenn erledigt**
Online-Datenschutzerklärung vorhanden und DSGVO-konform?	
Allgemeine Datenschutzhinweise vorhanden und DSGVO-konform?	
Prozess zur Bereitstellung der allgemeinen Datenschutz-hinweise an alle neuen Kunden, Mitarbeiter etc. im Unter-nehmen vorhanden?	
Pflicht zur Benennung eines DSB? Falls ja: DSB der Auf-sichtsbehörde gemeldet?	
Aufstellung aller Dienstleister erstellt?	
Eventuell Auftragsverarbeitungsverhältnisse identifiziert? AV-Verträge abgeschlossen bzw. an die DSGVO angepasst?	
Liste mit Einwilligungserklärungen erstellt? Einwilligungen aktuell? Falls nein: Einwilligungstext aktualisiert?	
Gegebenenfalls Arbeitsanweisungen, Betriebsvereinbarun-gen o. Ä. an die DSGVO angepasst?	
Verarbeitungsverzeichnis erstellt?	
Wichtige Anlagen zum Verarbeitungsverzeichnis vorhanden (z. B. Löschkonzept, Benutzerrechteregelung, Backup-Konzept usw.)?	
Prozess zur Reaktion auf Ausübung von Betroffenenrechten im Unternehmen vorhanden? Alle Mitarbeiter geschult/ informiert?	
Prozess zur regelmäßigen Überprüfung der eigenen DSGVO-Compliance im Unternehmen vorhanden?	

PRIVACYXPERTS

ein Unternehmensbereich des VNR Verlag für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 0228/9 55 01 50
Fax: 0228/3 69 64 80
Internet: www.privacyxperts.de
E-Mail: kundendienst@privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Vorstand: Richard Rentrop, Bonn

Herausgeberin: Denise vom Hoff, Bonn

Redaktion: Rechtsanwalt Michael Rohrlich

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.

© 2019 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Bukarest, Manchester, Warschau