

PRIVACY@WORK

FÜR DATENSCHUTZBEAUFTRAGTE



**Schnell erledigt: Diese Infos
müssen in das Verzeichnis von
Verarbeitungstätigkeiten**



ANDREAS WÜRTZ – IHR EXPERTE FÜR DATENSCHUTZ

ANDREAS WÜRTZ VERFÜGT ÜBER MEHR ALS 17 JAHRE BERUFERFAHRUNG ALS VOLLZEIT-DATENSCHÜTZER IM UNTERNEHMEN. ER ZEIGT IHNEN, WIE SICH DATENSCHUTZ PRAGMATISCH UMSETZEN LÄSST.

Das Verzeichnis ist kein Hexenwerk

Liebe Leserin, lieber Leser,

es gibt Themen im Datenschutz, die sind weder bei Unternehmen noch bei Beschäftigten beliebt. Und wahrscheinlich löst das Verzeichnis von Verarbeitungstätigkeiten auch bei Ihnen keine Begeisterungstürme aus. Das ist nachvollziehbar. Schließlich leuchtet der Nutzwert einer solchen formellen Verarbeitungsliste nicht sofort ein.

Doch glauben Sie mir: Das Verzeichnis ist besser als sein Ruf. Es hilft Ihrem Unternehmen und Ihnen, den Datenschutz für Ihr Unternehmen passgenau umzusetzen. Und die Sache mit dem Verzeichnis ist gar nicht so kompliziert, wenn Sie die Hinweise und Tipps in dieser Ausgabe umsetzen.

Viele Grüße

*Andreas Würtz, Rechtsanwalt und Chefredakteur
des Ratgebers „Datenschutz aktuell“*

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN: KENNEN SIE SICH AUS?

Es gibt Themen im Datenschutz, mit denen sich so niemand wirklich anfreunden will. So ist es beispielsweise mit dem Thema Verzeichnis von Verarbeitungstätigkeiten. Weil niemand um diese Dokumentationspflicht aus Art. 30 Datenschutz-Grundverordnung (DSGVO) herumkommt, ist es unerlässlich, sich des Themas anzunehmen. Klar, dass es viele Fragen gibt. So können Sie auf typische Fragen antworten:

Wo ist das Verzeichnis von Verarbeitungstätigkeiten geregelt?

Beim Verzeichnis von Verarbeitungstätigkeiten handelt es sich um eine gesetzliche Dokumentationspflicht. Die einschlägigen Vorgaben finden Sie in Art. 30 DSGVO. Prinzipiell sind Verantwortliche und Auftragsverarbeiter verpflichtet, ein solches Verzeichnis im Zusammenhang mit der Verarbeitung personenbezogener Daten zu erstellen und aktuell zu halten.

Muss jedes Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten haben?

Das lässt sich meist mit einem „mindestens ein Verzeichnis“ beantworten. So sind Verantwortliche verpflichtet, ein Verzeichnis nach Art. 30 Abs. 1 DSGVO zu führen. Das enthält die eigenen Verarbeitungstätigkeiten, bezüglich derer man Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist. Typisches Beispiel ist etwa eine von der Personalabteilung geführte elektronische Personalakte. Auch wenn man hier die Software einkauft, etwa online als „Software-as-a-Service-Lösung“, muss Ihr Unternehmen als Verantwortlicher die Verarbeitungstätigkeit dokumentieren.

Daneben gibt es noch ein Verzeichnis von Verarbeitungstätigkeiten speziell für Auftragsverarbeiter. Das könnte im Beispiel zuvor der Anbieter der Software für die elektronische Personalakte sein. Die inhaltlichen Anforderungen an dieses Verzeichnis ergeben sich aus Art. 30 Abs. 2 DSGVO. Folglich müssen Auftragsverarbeiter ein weiteres Verzeichnis führen, eben neben den Verarbeitungen, die das betreffende Unternehmen für sich selbst verantwortet.

Es gibt doch bestimmt eine Ausnahme von der Verzeichnispflicht, oder?

An sich gibt es tatsächlich einen Fall, in dem auf ein Verzeichnis verzichtet werden könnte. Die Betonung liegt hier auf „könnte“. Zwar sieht Art. 30 Abs. 5 DSGVO vor, dass ein Unternehmen mit weniger als 250 Mitarbeitern kein Verzeichnis von Verarbeitungstätigkeiten führen muss. Allerdings kommt es nicht nur auf die Mitarbeiterzahl an.

Auch wenn Ihr Unternehmen weniger als 250 Mitarbeiter hat, ist ein Verzeichnis dennoch erforderlich, wenn eine der folgenden Voraussetzungen erfüllt ist:

- Es gibt eine Verarbeitung, die ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt,
- die Verarbeitung erfolgt nicht nur gelegentlich, also nicht nur ab und an und somit regelmäßig oder
- es werden besondere Datenarten gemäß Art. 9 Abs. 1 DSGVO verarbeitet, beispielsweise Gesundheitsdaten oder personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DSGVO.

Es liegt auf der Hand, dass es eigentlich keine Verarbeitungen geben dürfte, die ohne jedes Risiko sind. Selbst unscheinbare Verarbeitungstätigkeiten, wie eine Liste mit Geburtstagen der Mitarbeiter, birgt Risiken. Solche Dokumente können etwa durch unsachgemäße Entsorgung in falsche Hände geraten. Fazit also: Es braucht immer ein Verzeichnis!

Für wen ist das Verzeichnis gedacht?

Ein solches Verzeichnis dient einerseits der Dokumentation und andererseits der Kontrolle. So kann

- ein Verantwortlicher oder Auftragsverarbeiter leichter einen Überblick erhalten, wie mit personenbezogenen Daten im Unternehmen gearbeitet wird,
- ein solches Verzeichnis Ihnen als Datenschutzbeauftragtem die Arbeit erleichtern. Sie können leichter identifizieren, wo besondere Risiken bestehen können. Das kann wichtig sein, damit Sie Ihre Ressourcen risikoorientiert einsetzen, und

- die zuständige Datenschutzaufsichtsbehörde die Vorlage des ganzen Verzeichnisses oder der Angaben zu einzelnen Verarbeitungstätigkeiten fordern. Dieses Recht ergibt sich aus Art. 30 Abs. 4 DSGVO. Einen besonderen Anlass braucht die Aufsichtsbehörde dafür nicht. Schließlich kann sie generell kontrollieren, ob sich ein Unternehmen an die gesetzlichen Vorgaben der DSGVO hält. Danach besteht ebendiese Dokumentationspflicht.

Was kann passieren, wenn unser Unternehmen kein Verzeichnis hat?

Hier sollten Sie auf zwei Aspekte verweisen: Erstens: Verzichtet ein Unternehmen auf das Führen eines Verzeichnisses, kann das die Datenschutzarbeit erschweren. So können Sie sich als Datenschutzbeauftragter nur schwer einen Überblick über die stattfindenden Verarbeitungstätigkeiten verschaffen. Unter Umständen wird es so auch schwierig, geltend gemachte Betroffenenrechte umzusetzen. Ist etwa nicht bekannt, wo überall personenbezogene Daten verarbeitet werden, kann das Löschen von Daten oder eine geforderte Auskunft ggf. nur unvollständig umgesetzt werden. Wird den Betroffenenrechten nicht ordnungsgemäß entsprochen, kann das zu einem Bußgeld führen.


Und zweitens: Ein Bußgeld kann es auch dafür geben, dass Ihr Unternehmen seiner Dokumentationspflicht aus Art. 30 DSGVO nicht nachkommt. So sind hier Strafen von bis zu 10 Mio. € möglich. Im Fall eines Unternehmens können es alternativ bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs sein, je nachdem, welcher der Beträge höher ist. Dabei ist klar: Wie hoch das Risiko ist, dass eine Datenschutzaufsichtsbehörde ein Verzeichnis prüft, dieses beanstandet und diesbezüglich ein Bußgeldverfahren einleitet, lässt sich nicht vorhersagen.

Wer muss sich um das Verzeichnis kümmern?

Das ist Sache des Verantwortlichen. Generell handelt es sich nicht um eine Aufgabe des Datenschutzbeauftragten. Das erkennen Sie bereits daran, dass die Pflicht, ein Verzeichnis zu erstellen, an den Verantwortlichen bzw. an den Auftragsverarbeiter adressiert ist. Außerdem finden Sie nichts dazu in Ihren gesetzlichen Aufgaben (Art. 39 Abs. 1 DSGVO). Ob ein Unternehmen das Führen des Verzeichnisses an den Datenschutzbeauftragten übertragen kann, ist umstritten. Es ist auf jeden Fall dann nicht möglich, wenn es zu einem Interessenskonflikt kommt. Das kann sein, wenn Sie selbst die Informationen bereitstellen sollen.

Welche Informationen müssen im Verzeichnis enthalten sein?

Was enthalten sein muss, ergibt sich aus Art. 30 DSGVO. Die Unterschiede erkennen Sie leicht in dieser Übersicht.



Übersicht: Mindestinformationen im Verzeichnis von Verarbeitungstätigkeiten	
Verzeichnis von Verarbeitungstätigkeiten für	
Verantwortliche (Art. 30 Abs. 1 DSGVO)	Auftragsverarbeiter (Art. 30 Abs. 2 DSGVO)
Name 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)	Name und 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)	–
wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 Buchst. f 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, 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)

VERARBEITUNGSTÄTIGKEIT: ERKLÄREN SIE, WAS DAMIT GEMEINT IST

Der Herausforderung eines Verzeichnisses von Verarbeitungstätigkeiten müssen sich Ihr Unternehmen und dessen Mitarbeiter stellen. Schließlich handelt es sich um eine gesetzlich geforderte Dokumentation. Als Datenschutzbeauftragter haben Sie es in der Hand, dass das Befüllen reibungslos klappt. Dazu zählt auch, dass Sie erklären, was ins Verzeichnis muss.

Die DSGVO hilft nicht wirklich weiter

Schauen Sie in die Datenschutz-Grundverordnung (DSGVO), finden Sie weder in Art. 30 noch in Art. 4 DSGVO eine Erklärung, was mit „Verarbeitungstätigkeit“ gemeint ist. Auch die Erwägungsgründe bieten nichts Erhellendes. Nur in Art. 4 Nr. 2 DSGVO wird der Begriff „Verarbeitung“ definiert. Hierbei handelt es sich um jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten.

Weil in der Verarbeitungsdefinition auch Vorgangsreihen erwähnt sind, wird jedoch deutlich, dass mit Verarbeitung eben nicht jeder einzelne Ver-

arbeitungsschritt gemeint sein dürfte. Vielmehr ist auch eine Aneinanderreihung von Teilschritten erfasst. Also können Sie die Ansicht vertreten, dass ebenso die „Verarbeitungstätigkeit“ als weiter Begriff zu verstehen ist, der auch Vorgangsreihen der Datenverarbeitung umfasst. Im Ergebnis wäre die Verarbeitungstätigkeit mit dem Begriff der Verarbeitung identisch.



Werden Sie zum „Historiker“

Die DSGVO ist die Fortführung und Weiterentwicklung der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG). Auf der Richtlinie basierte beispielsweise das frühere Bundesdatenschutzgesetz. Schon damals gab es Diskussionen zum ehemals erforderlichen Verzeichnissesverzeichnis. Hier war nämlich auch nicht so ganz klar, was mit einem „Verfahren“ gemeint ist. Schließlich konnte man dabei auch an Verarbeitungen auf Dateiebene denken, sodass etwa jede Datei als einzelne Verarbeitung im Verzeichnis hätte aufgeführt werden müssen.

Allerdings leuchtete auch damals jedem pragmatischen Datenschutzbeauftragten ein, dass ein Verzeichnis auf Dateiebene nicht gemeint sein konnte. Die Begründung lief folgendermaßen: Nach Art. 18 EU-Datenschutzrichtlinie und dessen Begründung ließ sich der Begriff „Verfahren“ als ein Bündel von Verarbeitungen interpretieren. In einem Verfahren waren also mehrere Verarbeitungen zusammengefasst, bei denen es über eine gemeinsame Zweckbestimmung und einen einheitlichen Sachverhalt zu einer Verarbeitung personenbezogener Daten kommt. Diese Sichtweise lässt sich auch auf die heutige Zeit und damit den Begriff „Verarbeitungstätigkeit“ übertragen.

Sprechen Sie lieber von Prozessen, Abläufen oder Vorgängen

Damit es mit den Inhalten für das Verzeichnis klappt, müssen Sie den Mitarbeitern und zuständigen Personen erklären, was in das Verzeichnis aufzunehmen ist. Machen Sie es hier nicht zu kompliziert. Anstatt von Verarbeitungstätigkeiten können Sie auch von einem Verarbeitungs- oder Geschäftsprozess, von einem Ablauf oder Vorgang sprechen. Das ist für viele leichter verständlich, nachvollziehbar und abgrenzbar. Dabei ist wichtig: Zeigen Sie auf, was Sie im Verzeichnis haben wollen. Das sind Verarbeitungstätigkeiten, sprich Verarbeitungsprozesse, die

- sich unter einen sinnvollen Oberbegriff zusammenfassen lassen,
- die von einem gemeinsamen Zweck getragen sind bzw. miteinander zusammenhängen und
- die sich nicht aufgrund ihrer Prägung als etwas Eigenständiges darstellen.



Machen Sie es passend

Bei der Abgrenzung einer Verarbeitungstätigkeit sollten Sie mit gesundem Menschenverstand vorgehen und Ihr Know-how als Datenschutzspezialist einfließen lassen. Sind Sie sich unsicher, wie „grob“ eine Verarbeitungstätigkeit zu einer anderen Verarbeitungstätigkeit abgegrenzt werden kann, können Sie mit anderen Datenschutzbeauftragten darüber sprechen, ob das aus deren Sicht noch passt.

Dabei ist wichtig: Eine Abgrenzung, die für alle Unternehmen und für jeden Fall gilt, gibt es nicht. Schließlich kann es auch auf die Unternehmensgröße ankommen, ob in einem Bereich noch von einer Verarbeitungstätigkeit gesprochen werden kann oder mehrere Verarbeitungstätigkeiten vorliegen. Im Kleinunternehmen kann es eine Verarbeitungstätigkeit „Kundenkommunikation“ geben, weil man nur einen Newsletter anbietet. Im Konzern können viele Formen des Kundenmarketings existieren, die so unterschiedlich sind, dass man von grundlegend anderen Verarbeitungsprozessen ausgehen kann.

Fürs Verständnis: Beispiele sind wichtig

Damit die Sache für die Kollegen greifbarer wird, sollten Sie auf Beispiele setzen. Wie wäre es beispielsweise mit Folgendem: Verkauft Ihr Unternehmen über einen Onlineshop Produkte, wird es hierfür eines Eintrags im Verzeichnis bedürfen. Eine Registrierung im Shop und das Abwickeln der Bestellung können als Prozessschritte Teil dieser Verarbeitungstätigkeit sein. Wird daneben auch ein Onlineshop auf einer Verkaufsplattform (z. B. Amazon Marketplace oder eBay) betrieben, bedarf es eines weiteren Eintrags. Es handelt sich hier um einen eigenständigen Vertriebskanal, für den andere Rahmenbedingungen gelten, etwa auch hinsichtlich Zwecke oder eingesetzter Technik.

SCHNELL ERLEDIGT: DIESE INFOS MÜSSEN IN DAS VERZEICHNIS

Das Thema Verzeichnis von Verarbeitungstätigkeiten ist nicht selbst-erklärend. Will Ihr Unternehmen ein Verzeichnis neu erstellen oder ein Bestehendes verbessern, sind vor allem Ihr Rat und Ihre Unterstützung gefragt. Sie haben es in der Hand, die Sache so zu gestalten, dass sie zügig erledigt wird und niemand gefrustet ist.

Sehen Sie die Sache realistisch

Als Datenschutzprofi wissen Sie: Wahrscheinlich dürfte wohl jedes Unternehmen ein Verzeichnis von Verarbeitungstätigkeiten brauchen, wenn es mit personenbezogenen Daten zu tun hat. Die Regelung des Art. 30 Abs. 5 Datenschutz-Grundverordnung (DSGVO), die von der Pflicht zur Führung eines Verzeichnisses entbindet, wird eher nie greifen. Denn: Es dürfte keine Verarbeitungen geben, die ohne jedes Risiko für die Rechte und Freiheiten der Betroffenen sind.

Weil kein Weg an einem Verzeichnis vorbeiführt, heißt es: geschickt damit umgehen, was nicht zu ändern ist. Und das meint insbesondere, dass Ihr Unternehmen einerseits den Anforderungen gerecht wird und andererseits die Anforderungen möglichst pragmatisch handhabt. Zugleich sollten Sie als Datenschutzbeauftragter berücksichtigen: Auch wenn die Pflicht zur Erstellung und Führung des Verzeichnisses nicht bei Ihnen liegt, sollte das Verzeichnis für Ihre Arbeit brauchbar sein. Dazu ist besonders wichtig, dass die Inhalte vollständig, informativ und aktuell sind.



Über die Umsetzung müssen nicht Sie entscheiden

Die DSGVO schreibt nicht vor, wie das Verzeichnis zu führen ist. In Art. 30 Abs. 3 DSGVO finden Sie lediglich die Festlegung, dass das Verzeichnis schriftlich geführt werden muss, wobei das auch in einem elektronischen Format passieren kann. Das heißt also für Sie: Ihr Unternehmen muss keine spezielle Software für das Verzeichnis einsetzen. Ein Verzeichnis beispielsweise auf Basis von Microsoft Word oder Excel kann ebenfalls

ausreichen. Selbst das meist etwas unpraktische manuelle Führen ist drin, also das händische Ausfüllen eines entsprechenden Formulars. Dabei ist wichtig für Ihre Beratung: Schriftlich bedeutet nur, dass etwas so festgehalten wird, dass es wiedergegeben werden kann, etwa in einer Datei, als Ausdruck oder abgeheftet in einem Ordner.

Geben Sie geschickt Hilfestellung


Egal, welche Software oder welche Lösungen Ihr Unternehmen für das Verzeichnis einsetzen will, vor allem eines erledigt sich nie von selbst: So sind die Verantwortlichen bzw. die zuständigen Ansprechpartner in Ihrem Unternehmen auszumachen. Diese Personen müssen alle relevanten Informationen zusammentragen.

Damit das klappt, sind Sie als Datenschutzbeauftragter gefragt. Eine gute Idee ist es, wenn Sie Gesprächstermine anbieten, um den Kollegen die Rahmenbedingungen, den Handlungsbedarf und das Vorgehen zu erläutern. So können Sie unterbinden, dass man sich querstellt, weil man das Verzeichnis nur als unnötigen bürokratischen Aufwand versteht. Zeigen Sie auf, dass das Verzeichnis eine gesetzliche Anforderung ist und darüber hinaus auch dazu beiträgt, den Datenschutz im Unternehmen besser umzusetzen.

Je einfacher, desto besser

Machen Sie stets klar: Es geht nicht darum, mit dem Verzeichnis einen Wettbewerb zu gewinnen. Dennoch müssen Sie es denjenigen so einfach wie möglich machen, die die Informationen für das Verzeichnis zusammenstellen sollen. Eine Möglichkeit ist, dass Sie sich an folgendem Muster orientieren. Das Muster dient der Erstellung eines Verzeichnisses für Verantwortliche und setzt sich aus einem Teil A und einem Teil B zusammen. Teil A enthält diejenigen Informationen, die bei wohl allen Verarbeitungen identisch sein dürften. Diesen Teil können Sie vorab befüllen. Sie bitten dann die Kollegen, nur Teil B für jede Verarbeitungstätigkeit zu befüllen.

Das von Ihnen verteilte Muster enthält idealerweise ein praxisnahes Beispiel, um die Inhalte möglichst selbsterklärend zu machen. Daneben kann es sinnvoll sein, dass Sie eine „Ausfüllanleitung“ beifügen. Hilfreich sind auch einige Termine, etwa virtuell, in denen Sie das Vorgehen erklären können. So haben Sie zugleich die Möglichkeit, konkrete Fragen zu beantworten und im Hinblick auf das Befüllen manchem Fehler vorzubeugen.



Bei der Auftragsverarbeitung gelten andere Anforderungen

Ist Ihr Unternehmen Auftragsverarbeiter, muss es meist ein zweites Verzeichnis führen, eben für die Auftragsverarbeitungen. Die Struktur ist zwar ähnlich, jedoch müssen Sie die nötigen Informationen nach Art. 30 Abs. 2 DSGVO abfragen und Ihr Muster für die Kollegen entsprechend abändern.

Muster: Verzeichnis von Verarbeitungstätigkeiten

Teil A) Allgemeine Angaben für alle Verarbeitungen

Art. 30 Abs. 1 Satz 2 Buchst. a DSGVO	Eintragungen
Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen	Neue Muster Vertriebs ABC GmbH
	Martin S. Gans (Geschäftsführer)
	Musterweg 1234 12345 Musterstadt Tel. 01234/56789-0 info@muster-vertrieb-abc.xyz
Name und die Kontaktdaten des Datenschutzbeauftragten	Hans Dampf Tel. 01234/56789-123 h.dampf@muster-vertrieb-abc.xyz

Teil B) Verzeichnis der Verarbeitungstätigkeiten

Verarbeitungstätigkeit	Bezeichnung der Verarbeitungstätigkeit	Onlineshop
	Verantwortliche Person/Abteilung	Fred Heinz (Vertrieb)
Angabe entsprechend Art. 30 Abs.1 Satz 2 DSGVO	Erläuterung	Informationen zur Verarbeitungstätigkeit

<p>Art. 30 Abs. 1 Satz 2 Buchst. b DSGVO: die Zwecke der Verarbeitung</p>	<p>Geben Sie das Ziel an, für das Ihr Unternehmen personenbezogene Daten verarbeitet. Sollte Ihnen eine Rechtsgrundlage (z. B. Paragraf im Gesetz, Vertrag, Einwilligung, Betriebsvereinbarung) bekannt sein, geben Sie diese bitte an.</p>	<p>Verkauf von Waren über den Onlineshop:</p> <ul style="list-style-type: none"> • Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO (Verarbeitung für die Erfüllung eines Vertrags mit dem Betroffenen bzw. vorvertragliche Maßnahmen auf Anfrage eines Betroffenen). • Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO (Einwilligung) bezüglich Weitergabe der Telefonnummer oder E-Mail-Adresse an Logistikpartner (Zustellungsankündigung) <p>Newsletter zu Rabattaktionen:</p> <ul style="list-style-type: none"> • Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO (Einwilligung) bezüglich Shop-Newsletter • Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO (überwiegendes berechtigtes Interesse) bezüglich Wahrnehmung Interessen und Durchsetzung von Rechtsansprüchen
<p>Art. 30 Abs. 1 Satz 2 Buchst. c DSGVO: Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten</p>	<p>Geben Sie grob an, auf welche Personen sich die Daten beziehen und um welche Daten es sich handelt.</p>	<p>Interessenten und Kunden: Anrede, Vorname und Name, Anschrift, Telefonnummer, E-Mail-Adresse, Bestellinformationen, Lieferinformationen, Informationen zur Zahlungsabwicklung</p>

<p>Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO:</p> <p>Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen</p>	<p>Führen Sie auf, wer die Daten erhält oder wem diese mitgeteilt werden können.</p>	<p>Interne Empfänger:</p> <ul style="list-style-type: none"> • Mitarbeiter Vertrieb • Mitarbeiter Logistik • Mitarbeiter Kundenservice <p>Externe Empfänger:</p> <ul style="list-style-type: none"> • Speditionen und Lieferdienste: Adressdaten, Telefonnummer, E-Mail-Adresse • Zahlungsdienstleister XYZ-pay: Bestell- und Rechnungsinformationen • Rechtsanwalt und Inkassounternehmen
<p>Art. 30 Abs. 1 Satz 2 Buchst. e DSGVO:</p> <p>Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabs. 2 DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien</p>	<p>Geben Sie bitte an, ob es zu einer Übermittlung an Stellen außerhalb der EU oder des Europäischen Wirtschaftsraums kommt.</p>	<p>Entsprechende Übermittlungen sind nicht vorgesehen; eingebundene Dienstleister sind in der EU ansässig.</p>

<p>Art. 30 Abs. 1 Satz 2 Buchst. f DSGVO:</p> <p>die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien</p>	<p>Wann Daten zu löschen sind, ergibt sich insbesondere aus Art. 17 DSGVO. Bei diesem Punkt geben Sie die entsprechende Frist oder die Rahmenbedingungen an.</p>	<ul style="list-style-type: none"> • Rechnungen: 10 Jahre (§ 147 Abs. 3 Satz 1, Abs. 1 Nr. 4a Abgabenordnung (AO)); Fristbeginn nach § 147 Abs. 4 AO) • Bestellinformationen: bis Löschung des Kontos durch den Kunden • Kundenkonto: auf Anforderung des Kunden bzw. 5 Jahre nach letzter Nutzung des Kundenkontos • E-Mail-Adresse für Newsletter: Löschung bei Widerruf der Einwilligung bzw. Löschaufforderung durch Betroffenen
<p>Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO:</p> <p>eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen, gemäß Art. 32 Abs. 1 DSGVO</p>	<p>Erläutern Sie bitte kurz, welche technischen und organisatorischen Schutzmaßnahmen (Art. 32 DSGVO) ergriffen wurden. Zu nennen sind technische Maßnahmen, wie etwa Zugriffsschutz, Verschlüsselung und Back-up-Lösungen. Aber auch organisatorische Regelungen wie Arbeitsanweisungen oder betriebliche Regelungen sind von Bedeutung. Ggf. können bzw. sollten Sie auch ein vorhandenes Sicherheitskonzept beifügen.</p>	<ul style="list-style-type: none"> • Zugriff auf die Daten nur durch die Mitarbeiter der zuständigen Abteilung im Rahmen ihrer Aufgaben (Umsetzung Berechtigungskonzept) • verschlüsselte Datenspeicherung und -übertragung • kein Kontakt zu Zahlungsdaten (Bank-/Kreditkartendaten) → getrennte Abwicklung durch Zahlungsdienstleister • Prozesse in Prozesshandbuch „Onlinevertrieb“ festgelegt • Durchführung regelmäßiger Sicherheitstests und Update von Schutzmaßnahmen • weitere Maßnahmen aus dem Sicherheitskonzept „Onlineshop“ vom 11.3.2024

ALLE VERARBEITUNGSTÄTIGKEITEN AUFGEFÜHRT?

Schritt 1: Starten Sie mit einem Brainstorming

Mit einem Brainstorming sammeln Sie spontane Einfälle und Gedankenblitze. Achten Sie darauf, dass Sie zu Oberbegriffen oder Fragen alles notieren, was Ihnen in den Sinn kommt. Filtern Sie nicht und lassen Sie nichts unnotiert, weil Sie es für unpassend oder nicht relevant halten.

Schritt 2: Gehen Sie gezielt auf die Suche

Bei einem Brainstorming allein sollten Sie es nicht belassen. Setzen Sie auch auf Gespräche, beispielsweise mit Bereichen, die oft in das Verarbeiten personenbezogener Daten involviert sind etwa die IT-Abteilung oder der Betriebsrat.

Schritt 3: Adressieren Sie den Handlungsbedarf

Haben Sie Verarbeitungstätigkeiten oder Bereiche mit Handlungsbedarf identifiziert, sollten Sie den zuständigen bzw. verantwortlichen Kollegen klarmachen, dass dies deren To-do ist.

Impressum:



PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 – 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: <https://www.privacyxperts.de>, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autor: Andreas Würtz, Freiberg am Neckar, Produktmanagement: Lisa Greiling, Bonn,

Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte S. 1: VZ_Art, S. 5 thataroth, S. 8 La Famiglia – alle Adobe.Stock.com, Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim Erscheinungsweise: 16 mal im Jahr; im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work 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. Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau