DSGVO-RETTUNGS-PAKET

Schritt-für-Schritt-Anleitung zur
DSGVO-konformen Dokumentation

digital pioneers

audatis
Datenschutz und Informationssicherheit | CONSULTING

Inhalt

EINSTIEG

1. Los geht‘s

Diese Schritt-für-Schritt-Anleitung zur DSGVO-konformen Dokumentation soll dir ermöglichen, dich mit den wesentlichen Dokumentationsanforderungen aus datenschutzrechtlicher Sicht vertraut zu machen und die für dein Unternehmen notwendigen Anpassungen unserer Vorlagen einfach und schnell umzusetzen.

Ziel unseres Datenschutzpakets ist es, dir so viel Arbeit wie möglich abzunehmen, damit du dich um die wesentlichen Themen im Unternehmen kümmern kannst.

Dazu haben wir zusammen mit Fachexperten aus den Bereichen Datenschutz(-recht) und Informationssicherheit zahlreiche Checklisten, Formulare und Richtlinien erstellt, die von dir in der Regel nur minimal angepasst werden müssen.

Diese Schritt-für-Schritt-Anleitung wird dich durch den gesamten Prozess und alle relevanten Dokumente führen und dir die notwendigen Stellen aufzeigen, an denen du Anpassungen vornehmen musst.

Fragen vor dem Start

Bevor du mit der Nutzung unseres Datenschutzpakets startest, hier noch ein paar Antworten auf wichtige Fragen, die du dir vielleicht stellst.

Sind die Dokumente rechtssicher?

Da die DSGVO vor dem 25.05.2018 noch nicht verbindlich ist, kann es auch noch keine entsprechenden rechtssicheren Aussagen in vielen Bereichen geben, die unklar oder nicht eindeutig festgelegt sind. Daher gibt es zwar bereits zahlreiche juristische Auslegungen und Interpretationen, diese basieren aber stets auf Annahmen und dem Vergleich mit Gesetzen und der Rechtsprechung der Vergangenheit. Wir haben die Dokumente nach bestem Wissen und Gewissen so verfasst, dass die kleinstmögliche Unsicherheit in der Auslegung der Vorgaben einbezogen wurde.

Unsere Dokumente ersetzen natürlich keine Rechtsberatung und auch keine Beratung durch Fachexperten im Bereich Datenschutz oder Informationssicherheit, soweit die konkrete Umsetzung und Ausgestaltung von Maßnahmen in der individuellen Praxis betroffen ist.

Wir können mangels individueller Kenntnis deines Unternehmens hier nur bestmögliche Beispiele und Vorlagen liefern. Deren Anpassung und Einsatz liegt am Ende in deinem Verantwortungs- und Haftungsbereich. Zum Vergleich ein Beispiel aus einem anderen Lebensbereich: Du kaufst ein schnelles Auto. Jetzt fährst du damit in einer 30er Zone zu schnell und bekommst ein Bußgeld. Der Hersteller übernimmt natürlich keine Haftung dafür, dass man sich auch an die Verkehrsregeln hält, das ist Sache des Fahrers. Wir liefern also das Auto in Form von Dokumenten und du kannst diese mit „angepasster Geschwindigkeit“ sicher einsetzen, sofern die individuellen Rahmenparameter dazu passen.

Was bedeutet anwaltlich geprüft?

Einige unserer Dokumente tragen den Vermerk „anwaltlich geprüft“. Diese wurden durch einen Rechtsanwalt geprüft und freigegeben. Damit kannst du nach aktuellem Stand die Einhaltung des Gesetzes sicherstellen, sofern es nicht zu individuellen Abweichungen oder im Rahmen der Rechtsprechung zukünftig zu Änderungen kommt. Sofern die Praxis in deinem Unternehmen von der dargestellten Situation im Dokument abweicht, kann dies natürlich nicht gewährleistet werden. Auch hier gilt, die Dokumente ersetzen keine individuelle Rechtsberatung.

Weitere Fragen und Antworten findest du in unserem FAQ-Bereich auf t3n.de.

Risikomanagement

Um die für alle Unternehmen, Behörden und sonstigen Organisationen nun europaweit völlig neue Rechts- und Risikolage im Datenschutz bestmöglich zu bewältigen, raten wir dir dazu, dich nachfolgend mit den wichtigsten Risiken aus Sicht des Datenschutzes vertraut zu machen und diese bei deiner Umsetzung zu berücksichtigen.

Bußgeld und Schadenersatz

In den Medien werden die Bußgelder aus Art. 83 der DSGVO viel zitiert und es wird von Strafen bis zu 20 Millionen Euro oder sogar 4 Prozent des weltweiten Umsatzes bei Konzernen gesprochen. Das ist grundsätzlich richtig, allerdings wird selten erwähnt, dass im gleichen Artikel auch eine ganze Liste von Umständen im Einzelfall zu berücksichtigen sind, die für die Entscheidung maßgeblich sind, ob überhaupt ein Bußgeld verhängt wird und wenn ja in welchem Umfang.

Somit kann man also festhalten: Wer im Bereich Datenschutz keine Vorkehrungen trifft, wird auch im schlimmsten Fall um ein empfindliches Bußgeld nicht herumkommen. Wer sich stattdessen proaktiv Gedanken macht, notwendige Maßnahmen rechtzeitig umsetzt und diese auch lückenlos dokumentieren kann, arbeitet und schläft in jedem Fall deutlich ruhiger.

Auch für den in Art. 82 DSGVO geregelten Schadenersatz gilt das ganz explizit. Durch die in der Verordnung geregelte Beweislastumkehr muss der Verantwortliche (also dein Unternehmen) Nachweise aufbringen, damit er „von der Haftung befreit“ wird, indem er „nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“. Das wird nur mit einer entsprechenden Dokumentation gelingen.

Außenwelt

Die einfachste Möglichkeit, sich datenschutzrechtlichen Ärger einzufangen, ist sicherlich die Darstellung in der Außenwelt, die als Anlass für Abmahnungen, Schadensersatzforderungen oder Bußgelder genommen werden kann, ohne dass diese Personen Kenntnisse der internen Abläufe und Prozesse haben. Hier einige Beispiele:

Risikofaktoren die von außen drohen

- Keine oder mangelhafte Informationspflichten in Form einer Datenschutzerklärung auf der Website
- Keine oder mangelhafte Einwilligungen für Newsletter oder Werbung im Onlineshop
- Keine oder mangelhafte Prozesse zur Einhaltung der Rechte von betroffenen Personen (zum Beispiel auf Auskunft, Löschung, Widerruf einer Einwilligung)
- Keine oder mangelhafte Umsetzung der Sicherheit auf Websites (zum Beispiel keine https-Verschlüsselung bei der Datenübertragung)
- Einsatz von IT-Systemen aus Drittstaaten ohne entsprechende Information für die Nutzer (zum Beispiel Versand von Newslettern durch US-Dienstleister)
- Hacken einer Webanwendung mit personenbezogenen Daten (zum Beispiel Online-Shop)

Daher solltest du in einem ersten Schritt zunächst diese Risiken minimieren. Hierzu sind unsere Dokumente bereits für dich vorbereitet.

Beschwerden und Prüfung durch Behörden

In allen Fällen, in denen sich betroffene Personen aus Sicht des Datenschutzes beschweren, Verstöße an Aufsichtsbehörden melden oder dein Unternehmen aus sonstigem Anlass in das Visier von Aufsichtsbehörden, Rechtsanwälten oder Gerichten gerät, werden zunächst einmal Dokumente eingefordert.

Hier gilt zu berücksichtigen, dass die Entscheidung häufig auf Basis der „nachweisbaren“ Dokumentation erfolgt. Wo es schon keine Dokumentation gibt, müssen Prüfungen vor Ort befürchtet werden, die im Regelfall weniger positiv ausfallen werden. Hier einige Beispiele:

Risikofaktoren die zu Beschwerden und Prüfung durch Behörden führen

- Keine oder mangelhafte Vertragsbasis mit Dienstleistern zur Auftragsverarbeitung
- Keine Erfüllung der allgemeinen Dokumentationspflichten (zum Beispiel Verzeichnis der Verarbeitungstätigkeiten)
- Keine oder mangelhafte Umsetzung der Informationspflicht an Betroffene (zum Beispiel Bewerber, Kunden, Patienten)
- Keine dokumentierten Verfahren zur regelmäßigen Überprüfung und Aktualisierung von Maßnahmen (Managementsystem)
- Keine oder mangelhafte Prozesse zur Meldung von Datenschutzverstößen
- Keine Nachweise der Wirksamkeit von Maßnahmen

Sofern die Risiken der Außenwelt abgesichert sind, sollten in einem zweiten Schritt diese Risiken minimiert werden. Auch hierzu liefern wir bereits für dich vorbereitete Dokumente.

Innensicht

Zuletzt solltest du dich noch mit den innerbetrieblichen Risikofaktoren beschäftigen. In vielen Fällen haben wir in der Praxis erlebt, dass Mitarbeiter mangels konkreter Regelungen und teilweise sogar vorsätzlich, Datenschutzverstöße begangen haben. Gerade bei den vorsätzlichen Verstößen kann man den Schaden nur zu begrenzen versuchen. Ein Organisationsverschulden durch mangelnde Regelungen (der Mitarbeiter weiß nicht, wie er sich richtig verhalten soll) ist dagegen einfach zu bewältigen. Die Lösung lautet: die notwendige Dokumentation für die notwendigen Mitarbeiter in der richtigen Form.

Einige Beispiele hierzu sind:

Risikofaktoren, die im Unternehmen drohen

- Keine oder mangelhafte Regelungen für Mitarbeiter
- Keine oder unzureichende Schulung der Mitarbeiter
- Keine oder mangelhafte Begrenzung von Berechtigungen in IT-Systemen
- Keine oder mangelhafte Dokumentation über IT-Systeme, Benutzer und Berechtigungen

Du solltest also nach der Erstellung der notwendigen Regelungen diese im dritten Schritt auch auf deine Mitarbeiter anwenden und an diese weitergeben.

Was sagen die Aufsichtsbehörden zur DSGVO?

Momentan verhalten sich die Aufsichtsbehörden beim Thema DSGVO zumindest in Deutschland sehr vorsichtig. Keine Behörde möchte beziehungsweise kann sich derzeit mit konkreten Anforderungen oder Vorgaben „zu weit aus dem Fenster lehnen“, da die DSGVO als europäische Verordnung einer in der ganzen EU harmonisierten und abgestimmten Sichtweise bedarf. Genau diese fehlt aber in der Praxis in vielen Bereichen, da es unterschiedliche Ansichten der einzelnen Aufsichtsbehörden gibt (alleine bei den 18 Behörden für Datenschutzaufsicht in Deutschland). Weiterhin fehlen verbindliche Ergänzungen zur DSGVO und als wichtigstes Element fehlt die komplette Rechtsprechung auf höchstrichterlicher Instanz (EuGH).

Diesem Umstand geschuldet sind viele Aufsichtsbehörden derzeit nicht besonders schnell, wenn es um Antworten auf die drängendsten Fragen der DSGVO geht (beispielsweise „Welche Verarbeitungstätigkeiten stehen zukünftig auf einer Black- oder eventuellen Whitelist für oder gegen die Durchführung einer Datenschutz-Folgenabschätzung?“, „Wohin melde ich die Kontaktdaten meines Datenschutzbeauftragten?“ oder „Welche Zertifikate zum Datenschutz werden für die DSGVO nutzbar sein?“).

Daher empfehlen wir dir, derzeit lieber auf Nummer sicher zu gehen und auch ohne konkrete Handlungsanweisungen der Aufsichtsbehörden deinen Verpflichtungen möglichst umfassend nachzukommen. In den nächsten Monaten und Jahren werden sicherlich an der ein oder anderen Stelle Lockerungen und Verschärfungen bei der Auslegung der DSGVO zu erwarten sein, bis dahin solltest du das Risiko möglichst geringhalten.

Datenschutzpaket als Managementsystem

Unser Ansatz kurz erläutert

Wir haben versucht unser Datenschutzpaket als Vorlage eines Managementsystems so aufzubauen, dass deine Mitarbeiter nur genau die Informationen bekommen (müssen), die sie zur korrekten Umsetzung des Datenschutzes benötigen. Daher gibt es viele kleine Dokumente, die nicht immer von allen Mitarbeitern verpflichtend zu lesen sind.

Weiterhin wollten wir mit den Dokumenten einen möglichst großen Bereich der DSGVO abdecken und dir dabei den größtmöglichen Nutzen zukommen lassen. Wir haben uns daher entschieden, unser Managementsystem auf der Basis von internationalen und deutschen Standards aufzubauen und dieses gleich als **Kombination aus Datenschutz und Informationssicherheit** zu gestalten. Das hat gute Gründe, denn ohne die Informationssicherheit (oder im engeren Sinne IT-Sicherheit) kommt auch der heutige Datenschutz nicht aus, der zur Erreichung der Vertraulichkeit, Integrität und Verfügbarkeit eben genau diese Schutzmechanismen benötigt, die bereits in der Vergangenheit in Informationssicherheitsmanagementsystemen (ISMS) gefordert wurden.

Du hast also mit dem Einsatz unseres DSGVO-Rettungspakets gleich mehrere Punkte erfüllt, nämlich:

Das leistet das DSGVO-Rettungspaket:

- die nachweisliche Einhaltung des Datenschutzes auf Basis der DSGVO.
- eine insgesamt reduzierte Risikosituation in deinem Unternehmen und damit verbunden auch weniger Haftungsrisiken für die Verantwortlichen (zum Beispiel Geschäftsführung, Inhaber), da wesentliche Regelungen und Dokumentationen bereits vorliegen.
- die nachweisliche Einhaltung zentraler Anforderungen aktueller Standards zur Informationssicherheit (wie ISO 27001 oder VdS 3473).
- mehr Sicherheit für deine Mitarbeiter, da sie in allen wesentlichen Bereichen des Datenschutzes Regelungen und Vorgaben nachlesen können und sich nicht auf ihr Bauchgefühl verlassen müssen.

Empfohlener Workflow für die Nutzung des Rettungspakets

1. Schritt-für-Schritt-Anleitung ausdrucken
2. Das Kapital 1 (Einstieg) in Ruhe lesen
3. Im Kapitel 2 die Fragen 2.1 bis 2.3 beantworten um zu entscheiden, welche Dokumente du benötigst
4. Nach und nach die Erklärungen zu den einzelnen Dokumenten in Kapitel 2 durchgehen, das jeweilige Dokument dazu öffnen und es gemäß der Erklärung in Kapitel 2 anpassen. Checkboxen zum Abhaken der erfolgten Anpassungen nutzen.
5. Dokument gegebenenfalls ausdrucken und wenn nötig unterschreiben (lassen)
6. Dokument abheften und gegebenenfalls in den audatis Manager in die Dateiablage hochladen (mehr dazu in Kapitel 3)

Icon-Legende

Um dir einen schnellen Überblick zu geben, haben wir Icons an die Dokumente angefügt:

Diese Dokumente werden nach außen hin sichtbar (zum Beispiel auf der Website).

Diese Dokumente richten sich an alle Mitarbeiter und sollten mit der Personalabteilung abgestimmt werden.

Diese Dokumente erfordern die Unterschrift eines Geschäftsführers.

Nur mit DSB-Pflicht

Diese Dokumente müssen nur bearbeitet werden, wenn du einen Datenschutzbeauftragten benötigst.

Auf Anfrage

Diese Dokumente müssen nur auf Anfrage bearbeitet werden. Dennoch ist es ratsam, sich bereits vor einer Anfrage mit den grundlegenden Workflows und Vorbereitungen der Dokumente auseinanderzusetzen.

Datenschutz im Unternehmen leben

Die reine Nutzung und Anpassung unserer Dokumente reicht natürlich nicht aus, um DSGVO-konform mit personenbezogenen Daten umzugehen und die gesetzlichen Vorgaben einzuhalten. Vielmehr muss anschließend die Umsetzung der in den Dokumenten genannten Regelungen durchgeführt und im Unternehmen implementiert und gelebt werden.

AUFBAU DER DATENSCHUTZ-ORGANISATION

2. Aufbau der Datenschutzorganisation

Um dir den Aufbau deiner Datenschutzorganisation möglichst einfach zu machen, beantworte bitte folgende Fragen. Daraus ergibt sich, welche Dokumentvorlagen du wirklich benötigst und welche du weglassen kannst. Alle Dokumente werden dann in Kategorien gegliedert kurz vorgestellt und dir wird in einfachen To-do-Schritten erklärt, was du genau an der Dokumentvorlage anpassen musst.

Benötigst du einen Datenschutzbeauftragten?

Unter folgenden Voraussetzungen muss dein Unternehmen auf jeden Fall einen Datenschutzbeauftragten benennen:

- Die Kerntätigkeit deines Unternehmens (als Verantwortlicher oder als Auftragsverarbeiter) erfordert eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen.
- Die Kerntätigkeit deines Unternehmens besteht in der umfangreichen Verarbeitung von besonders sensiblen Daten (zum Beispiel Gesundheitsdaten) oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

Was ist unter Kerntätigkeit zu verstehen? Damit sind die Haupttätigkeiten des Unternehmens gemeint und nicht die bloße Verarbeitung personenbezogener Daten als Nebentätigkeit. Ein Onlineshop, der Kundendaten auswertet, um Kaufvorschläge zu generieren, würde nicht unter die Verpflichtung fallen, da die Haupttätigkeit der Verkauf von Waren ist.

Zusätzlich zu den oben genannten Kriterien muss in Deutschland weiterhin ein Datenschutzbeauftragter bestellt werden, wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind (zum Beispiel weil sie E-Mails lesen und schreiben).

Das DSGVO-Rettungspaket unterscheidet sich, je nachdem ob du einen Datenschutzbeauftragen (DSB) brauchst oder nicht:

Mit DSB-Pflicht: Unterordner „mit DSB“ verwenden

Ohne DSB-Pflicht: Unterordner „ohne DSB“ verwenden

DSB intern oder extern benennen?

Für die meisten Unternehmen wird ein externer DSB die bessere Lösung sein. Ein interner Mitarbeiter wird zum einen darauf angewiesen sein, über eine fundierte Ausbildung zu verfügen oder zumindest eine hohe Motivation zu haben, sich umfangreiches Wissen über diesen neuen Tätigkeitsbereich anzueignen. Zudem muss der Mitarbeiter durch regelmäßige kostenpflichtige Weiterbildungen sein Wissen auf dem neuesten Stand halten. Außerdem gilt es zu bedenken, dass der interne Mitarbeiter unter Umständen nicht so einfach gekündigt werden kann, solange er DSB ist.

Eine Übersicht zahlreicher externer Datenschutzbeauftragter findest du in deinem DSGVO-Rettungspaket (Übersicht_Externe-Datenschutzbeauftragte_BvD, Quelle: BvD).

Dürfen deine Mitarbeiter das Internet und die IT-Systeme deines Unternehmens privat nutzen?

Grundsätzlich besteht die Möglichkeit, den Mitarbeitern die private Nutzung des Internets und der internen IT-Systeme (zum Beispiel E-Mail, Internet-Zugang) zu untersagen. Will man Mitarbeitern dies aber ermöglichen beziehungsweise es nicht explizit verbieten, dann ist die Vorlage F2 zwingend erforderlich.

private Internet/IT-Nutzung erlaubt beziehungsweise nicht untersagt**: Vorlage F2** nutzen

Dürfen deine Mitarbeiter private Geräte zur geschäftlichen Kommunikation nutzen (BYOD)?

Falls deine Mitarbeiter ihre privaten Geräte (Smartphone, Tablet et cetera) für die E-Mail-Kommunikation nutzen oder damit Zugriff auf interne Firmensysteme wie CRM, Kundensupport-Tool oder ähnliches haben, muss auch hier ein klarer Rahmen im Sinne des Datenschutzes definiert werden. In der Praxis ergibt es oft Sinn, die geschäftliche Nutzung von Privatgeräten zu verbieten. Denn der Verwaltungsaufwand, der mit der BYOD-Regelung einhergeht ist nicht unerheblich. Möglicherweise ist es effizienter, den Mitarbeitern Firmengeräte zu stellen. Falls nicht, sind Vorlagen K1 und K2 zwingend erforderlich.

BYOD erlaubt: **Vorlagen K1 und K2** nutzen

AUDATIS MANAGER

3. audatis Manager

Der audatis Manager (https://manager.audatis.de) ist eine webbasierte Datenschutzmanagement-Software, mit der du alle Aktivitäten und Anforderungen der DSGVO abdecken und gleichzeitig wichtige Aufgaben delegieren und automatisch dokumentieren kannst. Der größte Vorteil? Die Zeitersparnis! Der audatis Manager ermöglicht dir zum Beispiel die Verwaltung des Verzeichnisses der Verarbeitungstätigkeiten, von Auskunft-Anfragen sowie eine zentrale Datenschutz-Dokumentation. Ganz ohne teure Berater oder zeitfressende Datenschutz-Seminare.

Einrichtung des audatis Manager

Die Einrichtung des audatis Manager geht wie folgt:

1. Registriere dich für deine 12-monatige Lizenz des audatis Manager unter https://dsgvo2.ds-manager.net/mandant_create_new.html und wähle dabei in dem Feld „Gewünschte Version“ die Option „audatis Manager Standard (1 Mandant)" aus.
2. Du erhältst anschließend eine E-Mail, in der alle nötigen Schritte zur weiteren Einrichtung des Systems beschrieben sind. Zudem erhältst du eine E-Mail mit deinen Zugangsdaten als Administrator der Datenschutzmanagement-Software.
3. Lege mit den Zugangsdaten einen Benutzerzugang an, der die vollen Administratorrechte besitzt
4. Mach dich nach dem ersten Login mit den Mandanteneinstellungen vertraut und lade ein Firmenlogo im PNG-Dateiformat (mindestens 10x50 Pixel und maximal 250x300 Pixel) hoch.
5. Wähle anschließend mindestens eine Organisationseinheit auf Ebene 1 aus, zum Beispiel die Geschäftsführung deines Unternehmens.
6. Um dich mit dem audatis Manager vertraut zu machen, ist es sinnvoll, wenn du dich zunächst mit der Auftragsverarbeitung, den technischen und organisatorischen Maßnahmen sowie dem Verzeichnis der Verarbeitungstätigkeiten beschäftigst. Bevor du das Tool produktiv einsetzt, solltest du die Vorlagentextbausteine an deine Bedürfnisse anpassen.
7. Um das im DSGVO-Rettungspaket enthaltene Vorlagenpaket für ein Verzeichnis der Verarbeitungstätigkeiten zu aktivieren, gehe in die „Einstellungen“ der Software, klicke auf „Rechnungs- und Lizenzdaten“ und wähle dort unter „Vorlagenpaket Verarbeitungstätigkeiten bestellen“ das für dich passende Vorlagenpaket aus und bestätige die Bestellung mit dem folgenden Button.

Verzeichnis der Verarbeitungstätigkeiten

Die DSGVO verpflichtet Unternehmen zum Führen eines „Verzeichnisses von Verarbeitungstätigkeiten“. Es dient der Transparenz über die Verarbeitung personenbezogener Daten und der rechtlichen Absicherung. Der Datenschutzbeauftragte legt das „Verarbeitungsverzeichnis“ eine entsprechende Anfrage vorausgesetzt der Aufsichtsbehörde als Nachweis vor, dass die Vorschriften der DSGVO vom Unternehmen eingehalten wurden.

Die Führung des Verfahrensverzeichnisses ist für den Datenschutzbeauftragten oft eine undankbare und langwierige Aufgabe. Mit dem audatis Manager lassen sich interne und behördliche Verzeichnisse auf Knopfdruck erstellen und die Ansprechpartner in den Fachabteilungen in die Bearbeitung mit einbinden. Auf diese Weise hast du schnell eine Übersicht aller Verfahren mit Bezug zu personenbezogenen Daten und bist jederzeit auskunftsfähig gegenüber Betroffenen und Behörden.

Anlegen von Verarbeitungstätigkeiten

1. Wenn du auf der Startseite des audatis Manager das Modul „Verzeichnis der Verarbeitungstätigkeiten“ anklickst, gelangst du zu deinem persönlichen Verzeichnis der Verarbeitungstätigkeiten
2. In der anschließend angezeigten Maske lassen alle bisher angelegten Verarbeitungstätigkeiten einsehen und bearbeiten
3. Über den Button „Neue Verarbeitungstätigkeit anlegen“ gelangst du auf die Seite zum Anlegen einer neuen Verarbeitungstätigkeit (zum Beispiel Reisekostenabrechnung).
4. Für jede Verarbeitungstätigkeit werden die Bezeichnung, die Organisationseinheit, der Fachverantwortliche sowie der Status (offen, zur Prüfung, in Prüfung, geprüft [Mängel], geprüft [ok], freigegeben, nicht freigegeben) angezeigt
5. In der Spalte „Verz.“ wird angezeigt, ob die Verarbeitungstätigkeit im zu exportierenden Verzeichnis aufgelistet wird oder nicht. Durch einen Klick auf die Überschriften können die Verfahren sortiert werden.
6. Über die Filterfunktion hast du die Möglichkeit, Einträge aus dem Verzeichnis der Verarbeitungstätigkeiten nach individuellen Kriterien herauszufiltern
7. Über die Buttons in der Spalte „Arbeitsschritt“ kannst du die Verarbeitungstätigkeit ansehen, bearbeiten oder eine Aufgabe an den Fachverantwortlichen stellen.

Importieren von Vorlagen der Verarbeitungstätigkeiten

1. Im Modul „Verzeichnis der Verarbeitungstätigkeiten“ kannst du nach der Aktivierung deines Vorlagenpakets über den Button „Vorlage importieren“ die von dir bei der Aktivierung ausgewählten komplett dokumentierten Verarbeitungstätigkeiten auswählen und in dein eigenes Verzeichnis importieren.
2. Dort müssen dann zumindest die Organisationseinheit und ein Fachverantwortlicher hinterlegt werden. Alle anderen Angaben sollten einmal geprüft und gegebenenfalls an dein Unternehmen angepasst werden. Fertig.

Weitere Informationen und Ressourcen

Eine Anleitung zur Registrierung eines neuen Benutzers im audatis Manager findet sich hier: https://support.ds-manager.com/kb/faq.php?id=9

Das vollständige Benutzerhandbuch des audatis Manager findest du unter https://dsgvo2.ds-manager.net/asset/help/ audatis-MANAGER_Benutzerhandbuch.pdf

Außerdem gibt es noch mehrere Video-Tutorials zu weiteren Funktionen des audatis Manager. Unter anderem für den Schnelleinstieg sowie das Support- und User-Meeting: https://vimeo.com/audatis

Ablage und Management der Datenschutzorganisation

Alle für dein Unternehmen notwendigen Dokumentvorlagen (siehe Schritt-für-Schritt-Anleitung Kapitel 2) müssen auf dein Unternehmen angepasst und anschließend in den audatis Manager hochgeladen werden. Die Software dient dir als Archiv für kommende Auskunftsanfragen von Betroffenen und Behörden.

Auskunft und Dokumentationsnachweis

Für den Fall, dass eine Behörde oder andere Personen Auskunft von deinem Unternehmen zum Thema Datenschutz verlangen, hier ein paar praktische Tipps und Hinweise, wie du den audatis Manager nutzt, um darauf zu reagieren.

Beschwerde bei einer Behörde

Es kann vorkommen, dass sich ein Betroffener bei einer Aufsichtsbehörde für Datenschutz über dein Unternehmen beschwert. Dann wird im Regelfall ein schriftliches Verfahren in Gang gesetzt, bei dem die Behörde zunächst Unterlagen anfordert. Diese sollten bei der Antwort an die Behörde auch gleich mitgeliefert werden. Am häufigsten wird das ein Verzeichnis der Verarbeitungstätigkeiten sein, das direkt im Modul als „behördliches Verzeichnis“ heruntergeladen werden kann. Außerdem werden oftmals die Verträge zur Auftragsverarbeitung beziehungsweise deren Prüfung angefordert (diese sollten im Modul „Auftragsverarbeitung (AV)“ gepflegt werden). Außerdem sind die technischen und organisatorischen Maßnahmen (TOM) häufig Bestandteil der Anfragen.

Auskunft einer betroffenen Person

Erhältst du eine Datenschutz-Anfrage von externen Personen, zum Beispiel zur Auskunft über die Daten eines Betroffenen, so sollte diese Anfrage erst einmal dokumentiert werden. Alleine schon um die Frist von einem Monat zur Beantwortung im Blick behalten zu können, keine Elemente der Auskunft zu vergessen und die notwendigen Datenquellen zu identifizieren. Dazu gibt es ab Ende April 2018 im audatis Manager das Modul „Anfragen betroffener Personen“. Dort kannst du, geführt durch einen digitalen Assistenten, die wichtigsten Schritte dokumentieren, um Auskünfte, Berichtigungen, Löschaufträge, Widersprüche et cetera korrekt und nachweisbar umzusetzen.

Erfüllung der Informationspflichten

Die DSGVO schreibt zahlreiche Informationspflichten vor. Da dies eine recht komplexe Beschreibung von Informationen erfordert, gibt es im Modul „Verzeichnis der Verarbeitungstätigkeiten“ in jeder Verarbeitung einen Reiter „Informationspflicht“. Dort kann jeweils für eine Gruppe von Betroffenen ein Word-Dokument heruntergeladen werden, das entweder für direkt beim Betroffenen erhobene Daten (zum Beispiel eine Bewerbung) oder für durch Dritte erhobene Daten (zum Beispiel eine Bonitätsprüfung) alle notwendigen Informationen bereitstellt. Voraussetzung ist natürlich, dass die notwendigen Felder in der Verarbeitungstätigkeit ausgefüllt sind. Diese Dokumente können dann optisch angepasst und beispielsweise in gedruckter Form oder als PDF auf der Website genutzt werden.

Meldung von Datenschutzverletzungen

Zukünftig müssen Datenschutz- und Sicherheitsvorfälle binnen 72 Stunden an die Aufsichtsbehörde gemeldet werden, sofern ein entsprechendes Risiko für die Betroffenen besteht. Im Modul „Assistent bei Datenschutz- und Sicherheitvorfällen“ können diese einfach erfasst und durch einen Fragenkatalog abgearbeitet werden. Zunächst werden Datenpannen intern an alle hinterlegten Benutzer gemeldet (optional auch als SMS) und deren Abarbeitung dokumentiert. Am Ende kann ein Dokument zur Vorlage beziehungsweise Meldung bei der Aufsichtsbehörde heruntergeladen und genutzt werden.

Titelbild: Shutterstock / Aleksandrs Bondars