STIFTUNG DATENSCHUTZ

Themenblock 6

Alles im Blick – Absicherung durch Dokumentation

Referentin

Kirstin Vedder

Stiftung Datenschutz

Ziele des Vortrages

STIFTUNG DATENSCHUTZ

- ✓ Dokumentationspflicht und Rechenschaftspflicht! Unterschiede kennenlernen.
- ✓ Vorschläge zur praktischen Umsetzung von Dokumentationspflichten und Rechenschaftspflichten.
- ✓ Übersicht über mögliche Rechenschaftsmechanismen.
- ✓ Neue Ansätze bei der eigenen Herangehensweise zum Datenschutz.
- ✓ Bußgelder im Datenschutz durch Nachweise möglichst vermeiden/reduzieren.

Zur Orientierung

STIFTUNG DATENSCHUTZ

Was sagt das Gesetz? - Was ist die Vorgabe?

DSGVO

Was bedeutet das? - Übersetzung in die Praxis

Wie kann es umgesetzt werden? - Lösungsvorschläge und Tipps

Grundsätze der Verarbeitung

Grundsätze für die Verarbeitung personenbezogener Daten	Art.5 Absatz 1 DSGVO
Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	Art.5 Absatz 1 lit a)
Zweckbindung	Art.5 Absatz 1 lit b)
Datenminimierung	Art.5 Absatz 1 lit c)
Richtigkeit	Art.5 Absatz 1 lit d)
Speicherbegrenzung	Art.5 Absatz 1 lit e)
Integrität und Vertraulichkeit	Art.5 Absatz 1 lit f)

„Absicherung“ durch Dokumentation

STIFTUNG DATENSCHUTZ

Rechenschaftspflicht

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können.

Art.5 Absatz 2 DSGVO

Die Organisation muss die Einhaltung der Grundsätze aus der DSGVO gewährleisten und dies auch nachweisen können.
Ein Nachweis ist also ein Beweis!
Die Rechenschaftspflicht unterscheidet sich von konkret genannten Dokumentationspflichten.

Umfang und die Art und Weise der Nachweise, welche erbracht werden müssen, ist nicht vorgegeben. Es gibt jedoch genügend „Rechenschaftsmechanismen“, die, wenn sie richtig umgesetzt werden, den erforderlichen Beweis dafür liefern können, dass ein wirksamer Datenschutz bei Ihnen lebt und atmet.

Was eher nicht dazu gehört: Lippenbekenntnisse, veraltete und sehr verallgemeinerte Datenschutzhinweise oder alte, kopierte und nicht angepasste Mustervorlagen (zB. VVT).

Nachweispflicht gem. DSGVO

STIFTUNG DATENSCHUTZ

Verantwortung des Verantwortlichen

Der Verantwortliche setzt … geeignete technische und organisatorische Maßnahmen um, um sicherzustellen **und den Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt. [2]Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.

Art.24 Absatz 1 DSGVO

Grobe FAUSTREGEL für Maßnahmen: Je höher das Risiko – desto besser/umfangreicher/effizienter/strenger **die Maßnahmen zur Minderung** eines Risikos.
Stichworte für Fortgeschrittene: Risikoanalyse, Schwellwertanalyse, Datenschutzfolgenabschätzung (DSFA)

Bei der **Bestimmung von Maßnahmen** dürfen Sie alles in einen Topf werfen:
Um welche Verarbeitung geht es und wie umfangreich ist diese, wie sind die näheren Umstände der Verarbeitung, welche Daten werden wie lange verarbeitet, wie oft kann ein Schaden eintreten, wie hoch wäre ein Schaden, wie sind Ihre Ressourcen und Aufgaben…

Jede Maßnahmen, welche Sie bestimmen/planen, wird umgesetzt, geprüft und aktuell gehalten. -> Das Dokumentieren dieser Überlegungen und Ergebnisse ist ein Nachweis!

…einen Nachweis erbringen…

STIFTUNG DATENSCHUTZ

Pflicht zum Nachweis

Art.5 Abs. 2 + Art.24 Abs 1 DSGVO

„Sie brauchen keinen Ferrari, wenn Sie zum Bäcker fahren wollen.“

Die DSGVO gibt Ihnen die Möglichkeit sowohl die Maßnahmen als auch den Nachweis in einem angemessenen Umfang zu leisten.

Beispiele:

Sensibilisierung -> Schulungskonzept -> Schulung durchführen -> Schulungsinhalte und Teilnehmerlisten aufbewahren!

Schutz der Daten -> Schlüsselvergabe schriftlich regulieren -> Schlüsselvergaben schriftlich protokollieren -> Schlüsselvergaben prüfen (zählen) und ggf. Gegensteuern -> Prüfbericht mit Ergebnis dokumentieren und aufbewahren!

Datenschutz ernst nehmen - Besprechungen/Meetings zum Datenschutz -> Protokolle mit Maßnahmen erstellen -> Umsetzung der Maßnahmen prüfen -> Dokumentationen aufbewahren!

Dokumentationspflicht gem. DSGVO

STIFTUNG DATENSCHUTZ

Verzeichnis der Verarbeitungstätigkeiten (VVT)

Jeder Verantwortliche …führt ein Verzeichnis aller Verarbeitungstätigkeiten, … Dieses Verzeichnis enthält sämtliche folgenden Angaben: (konkretisierte Aufzählung).
Das … genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

Art.30 Absatz 1 und 3 DSGVO

Das Führen eines VVT ist eine **konkrete** Pflicht aus der DSGVO und das Fehlen ist bußgeldbehaftet.
Auf Anfrage der Aufsichtsbehörde ist ein VVT vorzulegen.
Ein einfaches Verzeichnis zu führen, ist also besser alles gar keins zu haben.

Fangen Sie ganz einfach an (z.B. mit einer Word oder Excel) und erweitern Sie Ihr VVT Schritt für Schritt.

VVT Anleitung und Muster der Stiftung Datenschutz:
https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/erfassung-von-verarbeitungstaetigkeiten-in-einem-verarbeitungsverzeichnis-270

Auch ein Blick auf die Seiten der Aufsichtsbehörden kann sich hier lohnen!

Rechenschaftspflicht über VVT abdecken?

STIFTUNG DATENSCHUTZ

Konkrete Pflicht zur Dokumentation

Art.30 Abs 3 DSGVO
Das Verzeichnis ist schriftlich zu führen.

Angaben im VVT:

Wer ist Verantwortlicher?
Wer ist Datenschutzbeauftragter?
Was sind die Zwecke der Verarbeitung?
Welche Daten werden verarbeitet?
Wer bekommt die Daten noch?
Gehen die Daten auch ins „Ausland“ (nicht EU/EWR)?
Wann werden die Daten gelöscht?
Welche Maßnahmen haben Sie zum Schutz der Datenverarbeitung ergriffen?

VVT bei Auftragsverarbeitung:

Für welche/n Verantwortliche/n führen Sie Tätigkeiten im Auftrag durch?
Welche Tätigkeiten führen Sie als Auftragsverarbeiter für andere aus?
Gehen die Daten auch ins „Ausland“ (nicht EU/EWR)?
Welche Maßnahmen haben Sie zum Schutz der Datenverarbeitung ergriffen?

Können die Fragen im VVT vollständig und richtig beantwortet werden, decken Sie bereits **einen Teil** der Rechenschaftspflichten gut ab.

Pflicht, Kür oder Clever?

STIFTUNG DATENSCHUTZ

Dokumentieren aller Verarbeitungen im „VVT“ und - wenn möglich – unter Angabe der „TOMs“

+

TOMs erstellen und konkrete Beweismöglichkeiten zu den getroffenen „TOMs“ mit-bestimmen.

Pflicht DSGVO

Clever

=

Dokumentierte Rechenschaft über die Gewährleistung der Grundsätze einer Datenverarbeitung und über die Sicherheit einer Verarbeitung.

Auch Datenschutzvorfälle sind nach Art. 33 Abs 5 DSGVO zu dokumentieren

Wen interessiert es?

Datenschutz-Aufsichtsbehörden können Dokumentationen und Nachweise von Ihnen anfordern.
Das tun sie idR unter bestimmten Umständen, wie z.B.:

- Sie haben einen Datenschutzvorfall und die Aufsichtsbehörde prüft den Vorgang und die Umstände.
- Eine betroffene Person hat sich bei der Aufsichtsbehörde beschwert und diese prüft den Vorgang und die Umstände.
- Die Aufsichtsbehörden führen eigene Prüfungen durch.

Auditoren (Prüfer) fragen gerne nach Beweisen und lassen sich nicht mit Lippenbekenntnissen abspeisen.

Ein Auftraggeber fordert den Nachweis zur Einhaltung, weil er Kontrollpflichten bei seinen Auftragnehmern durchführen muss.

Sollte es dann doch einmal so weit kommen, können die Nachweise wertvolle Entlastungen in Gerichtsverfahren sein.

Grundsatz 1 nachweisen

STIFTUNG DATENSCHUTZ

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden.

Art.5
Absatz 1 lit. a)
DSGVO

Die Verarbeitung muss nachvollziehbar sein. Dabei soll sich die betroffene Person darauf verlassen dürfen und erst einmal davon ausgehen können, dass seine Daten rechtmäßig verarbeitet werden. Die betroffene Person soll sich aber auch Gewissheit verschaffen und nachfragen können.

Pflicht zu Dokumentation:

- Dokumentieren Sie die Rechtsgrundlage der Verarbeitung im **VVT.** (Pflichtangabe)
- Geben Sie die Rechtsgrundlage in den **Datenschutzhinweisen** an. (Pflichtangabe)
- Erstellen Sie Datenschutzhinweise und stellen Sie diese leicht zugänglich zur Verfügung.

Weitere geeignete Nachweise:

- Führen Sie Schulungen durch und verwahren Sie die Anwesenheitsprotokolle und Schulungsinhalte.
- Erstellen Sie gut verständliche Datenschutz-Richtlinien und kommunizieren Sie diese leicht zugänglich an die Beschäftigten.
- Verpflichten Sie Beschäftigte auf die Vertraulichkeit und lassen Sie diese gegenzeichnen.
- Halten Sie Datenschutzhinweise einfach und stets aktuell.

Grundsatz 2 nachweisen

STIFTUNG DATENSCHUTZ

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; …

Art.5
Absatz 1 lit. b)
DSGVO

Keine Datenverarbeitung ohne festgelegten Zweck. Die Zwecke sollten dabei möglichst eindeutig beschrieben werden können und müssen legitim sein.

Pflicht zu Dokumentation:

- Dokumentieren Sie den Zweck der Verarbeitung im **VVT.** (Pflichtangabe)
- Geben Sie den Zweck in den **Datenschutzhinweisen** an. (Pflichtangabe)

Weitere geeignete Nachweise:

- Weisen Sie relevante Personen an, dass die Daten NICHT für andere Zwecke als die Vorgesehenen zu verwenden sind (Ein grundsätzliche schriftliche „Verpflichtung zur Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten“ für alle Mitglieder, Ehrenamtliche, Aushilfen).
- Bei Projekten: Besondere Datenschutzrelevanz in Projekten schulen und nachhalten. Insb. wenn viele neue Personen involviert sind.

Grundsatz 3 nachweisen

STIFTUNG DATENSCHUTZ

Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Art.5
Absatz 1 lit. c)
DSGVO

Datenminimierung bedeutet nicht, dass alles zu löschen ist. Viele Daten sollen für viele Mitarbeiter verfügbar sein. Achten Sie darauf, dass die Datenverarbeitung auf ein **notwendiges Maß** beschränkt ist. Nutzen Sie nur die Daten, welche wirklich erforderlich und gleichzeitig angemessen sind, um den Zweck zu erfüllen. Schauen Sie auch auf die Zugriffsberechtigungen.

Pflicht zu Dokumentation:

- Dokumentieren Sie die Datenkategorien und die Datenarten im **VVT.** (Pflichtangabe)
- Dokumentieren Sie die getroffenen Zugriffsrechte im **VVT** bei den „TOMs“.

Weitere geeignete Nachweise:

- Dokumentierte Überlegungen dazu, welche Daten für eine bestimmte Verarbeitung erforderlich sind (Beispiel: Mitgliedsantrag).
- Berechtigungen für Datenzugriffe, Aktenzugriffe festlegen, überprüfen und Prüfungen dokumentieren.

Grundsatz 4 nachweisen

STIFTUNG DATENSCHUTZ

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; …

Art.5
Absatz 1 lit. d)
DSGVO

Falsche Daten können zu falschen oder ungewollten Ergebnissen führen. Die Daten sollten daher stets sachlich richtig und aktuell sein. Sie sollten also in der Lage sein, unrichtige Daten zu korrigieren aber auch löschen zu können. Das können zum Beispiel nicht alle alten Softwareanbieter leisten.

Pflicht zu Dokumentation:

- Keine direkte Dokumentationspflicht aus der DSGVO.

Weitere geeignete Nachweise:

- Dokumentierte Überlegungen dazu, ob und wie Daten innerhalb einer bestimmte Verarbeitung korrigiert, ergänzt, gesperrt oder gelöscht werden können.
- Beim Einsatz neuer Software diese auf die Anforderungen hin prüfen und Überlegungen dokumentieren. Stichwort für Fortgeschrittenen: Privacy by design & default.

Grundsatz 5 nachweisen

STIFTUNG DATENSCHUTZ

Speicherbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die **die Identifizierung der betroffenen Personen** nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist…

Art.5
Absatz 1 lit. e)
DSGVO

Lösen Sie einen direkten grundsätzlich Personenbezug auf, wenn es möglich und sinnvoll ist (z.B. Nummer statt Name, Kürzel statt ausgeschrieben). Löschen Sie Daten grundsätzlich, wenn Sie diese wirklich nicht mehr benötigen.
Unterscheiden Sie zwischen „aktive“ Daten und „in-aktive“ Daten.

Pflicht zu Dokumentation:

- Dokumentieren Sie die Speicherdauer oder die Kriterien zur Speicherdauer der Verarbeitung im **VVT.** (Pflichtangabe)
- Geben Sie die Speicherdauer oder die Kriterien zur Speicherdauer in den **Datenschutzhinweisen** an. (Pflichtangabe)

Weitere geeignete Nachweise:

- Begrenzen Sie den Zugriff auf „in-aktive“ Daten.
- Erstellen Sie eine Löschvorgabe zur jeweiligen Verarbeitung und dokumentieren Sie diese.
- Prüfen Sie gelegentlich, ob die Löschungen stattfinden.
- Prüfen Sie, ob Daten pseudonymisiert verarbeitet werden können und setzen Sie dies ggf. um (z.B. Nummer statt Name).

Grundsatz 6 nachweisen

STIFTUNG DATENSCHUTZ

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete **technische und organisatorische Maßnahmen.**

Art.5
Absatz 1 lit. f)
DSGVO

Die Umsetzung dieses Grundsatzes schlägt sich deutlich in der „Sicherheit der Verarbeitung“ nieder. Als ein Herzstück der DSGVO hält es viele Möglichkeiten von Nachweisen vor. Es geht also um die sogenannten „TOMs“ (Technische und organisatorische Maßnahmen).

Pflicht zu Dokumentation:

- Dokumentieren Sie wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1. der Verarbeitung im **VVT.** (Pflichtangabe)
- Fangen Sie ganz einfach an (z.B. mit einer Word oder Excel) und verfeinern Sie Ihre „TOMs“ Schritt für Schritt.
- TOMs-Muster zur Anpassung der Stiftung Datenschutz findet Sie im Ehrenamt Ratgeber im VVT integriert:
- https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/erfassung-von-verarbeitungstaetigkeiten-in-einem-verarbeitungsverzeichnis-270

Vorlagenmuster VVT der Stiftung

STIFTUNG DATENSCHUTZ

A	B	C	D	E	F	G	
Verarbeitungstätigkeit	**Zwecke der Verarbeitung**	**Betroffene Personer**	**Personenbezogene Dat**	**Empfänger der Daten**	**Drittlandstransfer**	**Löschfrist(en)**	**Technische u**
Verarbeitungstätigkeit eintragen							
Verarbeitungstätigkeit eintragen							
Verarbeitungstätigkeit eintragen							
...							
Beispiele für mögliche Verarbeitungstätigkeiten:							
Mitgliederverwaltung	Verwaltung der Mitgliedschaft einschließlich der Durchführung des Mitgliedschaftsverhältnisses: Aufnahme neuer Mitglieder, die Abrechnung der Mitglieder, Informationen an Mitgliedern	Mitglieder	Name, Vorname, Geburtsdatum, Geschlecht, Adresse, Emailadresse, Telefonnummer, Datum des Vereinsbeitritts, Sportbereiche, Sportart, Tanzgruppe, Mannschaftszugehörigkeit	Keine	nicht zutreffend	2 Jahre nach Beendigung der Mitgliedschaft	*Verweis auf Tabellenl* *ggf. hier Besonderhe jeweiligen Verarbeitu*
Beitragsverwaltung	Finanzierung des Vereins	Mitglieder	Name, Vorname, Kontoinhaber, Bankverbindung	Steuerberater	nicht zutreffend	10 Jahre	*Verweis auf Tabellenl* *ggf. hier Besonderhe jeweiligen Verarbeitu*
Personalverwaltung einschließlich Lohnabrechnung über externen Dienstleister	Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses einschließlich Gehaltszahlung und Zahlungen von Steuern und Abgaben gemäß Sozialgesetze	Beschäftigte	Name, Vorname, Adresse, Familienstand, Religionszugehörigkeit, Kontoverbindung, Arbeitszeiten, Steuermerkmale	Dienstleister (extern); Vertrag zur Verarbeitung im Auftrag abgeschlossen	nicht zutreffend	10 Jahre	*Verweis auf Tabellenl* *ggf. hier Besonderhe jeweiligen Verarbeitu*

Beispieltabelle Maßnahmen

STIFTUNG DATENSCHUTZ

Grundsatz	Ziel-Konkretisierung	Welche konkreten Maßnahme?	Konkreter Nachweis
a	Organisatorische Maßnahme: Sensibilisieren der Organisation für den Datenschutz	Datenschutz-Richtlinie erstellen, Verantwortlichkeiten festlegen und kommunizieren	Schriftstück, Zugang und Erhalt sicherstellen (Intranet, Share, Dokument)
a	Organisatorische Maßnahme: Sensibilisieren der Mitarbeitenden für den Datenschutz	Mitglieder/Aktive/Ehrenamtliche mit Unterschrift verpflichten, sensibilisieren	Dokument „Verpflichtung auf die Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten“ unterschreiben lassen und aufbewahren
a	Organisatorische Maßnahme: Sensibilisieren der Mitarbeitenden für den Datenschutz	Mitglieder/Aktive/Ehrenamtliche informieren und schulen	Schulungsinhalte, Termine und Anwesenheitslisten aufbewahren
a-f	Verarbeitung dokumentieren und gesetzlicher Dokumentationspflicht aus Art.30 nachkommen	Erstellen eines vollständigen und aussagekräftigem Verzeichnis der Verarbeitungstätigkeiten (VVT) erstellen und Schritt für Schritt ausfüllen	**Aktualität, Richtigkeit und Vollständigkeit des VVT sicherstellen und prüfen.** Copy-Paste-Muster möglichst vermeiden, sondern anpassen.
e+f	Sicherheit der Verarbeitung durch konkretisierte technische Maßnahmen gewährleisten	Technische Maßnahmen festlegen und deren Umsetzung verfolgen. Erstellen von „allgemeingültigen TOMs“ und ggf. von spezifischen TOMs innerhalb einer bestimmten Verarbeitung.	Auflistung von TOMs, entsprechender Nachweis durch schriftliche Dokumentation oder technisch, automatisierte Protokollierung
a	Bereitstellen von Informationen (Transparenz durch Information). Nachkommen von gesetzlichen Informationspflichten	Konkrete Datenschutzhinweise erstellen	Aktuelle Datenschutzhinweise, welche auf die Verarbeitung passen. Copy-Paste-Muster möglichst vermeiden, sondern anpassen.
c-f	Das Risiko einer Verarbeitung einschätzen, um Maßnahmen zu bestimmen	Risikobewertung einer Verarbeitung vornehmen	Risikobewertung der Verarbeitung dokumentieren
e	Löschen von alten Datenträgern oder Datenbanken, Daten	Effektiven Lösch-, Vernichtungsprozess festlegen	Löschung, Vernichtung protokollieren und Protokolle aufbewahren
c+f	Datenminimierung durch Zugriffsrechte erreichen	Begrenzung des Zugriffs auf nur Daten für bestimmte Personen. Berechtigungskonzept vorhalten.	Berechtigungen auf Daten und Räume prüfen, ggf. Gegensteuern und Prüfungen dokumentieren
a	Betroffenenrechte Umsetzen	Verantwortlichkeit und Meldeprozess festlegen. Mitglieder/Aktive/Ehrenamtliche informieren (schulen)	Anliegen zu Betroffenenrechten jeder Art dokumentieren und geschützt verwahren
a+f	Umgang mit Datenschutzvorfällen	Verantwortlichkeit und Meldeprozess festlegen. Mitglieder/Aktive/Ehrenamtliche informieren (schulen)	Auch kleine Datenschutzvorfälle jeder Art dokumentieren, Maßnahmen ergreifen und geschützt verwahren

FAZIT

Der geforderten Rechenschaftspflicht kann durch „Nachweise als Beweise“ nachgekommen werden.

Welche konkreten Nachweise das sein sollen, wird nicht genannt.

Konkrete Nachweismöglichkeiten ergeben sich aus der Beantwortung der Fragen aus dem VVT.

Konkrete Nachweismöglichkeiten ergeben sich aus der aktiven Umsetzung von getroffenen technischen und organisatorischen Maßnahmen.

Fangen Sie bei den Verarbeitungen an, die ein hohes Risiko innehaben könnten.

Fangen Sie einfach und schlank an! Fragen und Lösungen werden sich ergeben.

Nutzen Sie unser Muster für die Dokumentation der Verarbeitung und der Maßnahmen.
https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/erfassung-von-verarbeitungstaetigkeiten-in-einem-verarbeitungsverzeichnis-270

STIFTUNG DATENSCHUTZ

Themenblock 6

Alles im Blick – Absicherung durch Dokumentation

Referentin

Kirstin Vedder

Stiftung Datenschutz