



Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxishilfe DS-GVO VIII

Unternehmensrichtlinie zur Datenschutz-Organisation



INHALT

1. Grundsätze	4
2. Der betriebliche Datenschutzbeauftragte/Datenschutz- koordinatoren	5
3. Beschaffung/Hard- und Software	6
4. Verpflichtung/Schulung der Mitarbeiter	6
5. Transparenz der Datenverarbeitung	7
6. Erhebung/Verarbeitung von personenbezogenen Daten	7
7. Datenhaltung/Versand/Löschung	8
8. Externe Dienstleister/Auftragsverarbeitung/Wartung	9
9. Sicherheit der Verarbeitung	9
10. Rechenschafts- und Dokumentationspflicht	10

Unternehmensrichtlinie zur Datenschutz-Organisation

Die Umsetzung der DS-GVO und weiterer datenschutzrechtlicher Vorgaben macht es erforderlich, von Seiten der Geschäftsleitung klare Anweisungen zu erteilen. Wie ist mit personenbezogenen Daten zu verfahren, welches Selbstbild hat das Unternehmen bei der Datenverarbeitung und welche konkreten Ziele werden bei der Datenschutzorganisation verfolgt?

Das nachfolgende Muster stellt einen Vorschlag dar. Details können und sollen unternehmensspezifisch ergänzt werden. So verweist das Muster auf mehrere fiktive Anlagen, die ggf. konkret mit Inhalt gefüllt werden könnten:

- Anlage 1 - Checkliste zur Beachtung der Anforderungen an Privacy-by Design/ Privacy-by-Default
- Anlage 2 - Risikominimierung durch Datenschutz-Folgenabschätzung
- Anlage 3 - Verhaltensmaßnahmen bei einer Datenpanne
- Anlage 4 - Datenportabilität
- Anlage 5 - Umgang mit personenbezogene Daten/Erlaubnistatbestände der DS-GVO
- Anlage 6 - Kompatibilitätscheck bei Zweckänderung
- Arbeitsanweisungen zur Datensicherheit (siehe Punkt 9.3)

Muster-Richtlinie zur Datenschutzorganisation bei der XY-GmbH

1. Grundsätze

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei der XY-GmbH bestehenden Verantwortlichkeiten. Alle Mitarbeiter sind zur Einhaltung der Richtlinie verpflichtet.

Sie richtet sich an

>> die Personen oder Abteilungen, die über den Einsatz/die Bereitstellung eines Anwendungssystems entscheiden (hier kann entsprechend der Unternehmensorganisation der Name eingesetzt

werden: z.B. IT-Abteilung, Systemadministrator = nachstehend ist insoweit von IT-Abteilung die Rede);

>> die Personen oder Abteilungen, die über die Nutzung des Systems für ihre Aufgaben entscheiden (betroffen sind i.d.R. die Fachabteilungen; ggf. können diese benannt werden);

>> Benutzer, d.h. diejenigen, die das zur Verfügung gestellte System für die Erledigung ihrer betrieblichen Aufgaben nutzen (bei Speicherung personenbezogener Daten auf einem Arbeitsplatzrechner entscheidet der einzelne Benutzer ggf. auch über die im System erfolgende Verarbeitung und die dazu verwendeten Programme),

>> den betrieblichen Datenschutzbeauftragten (DSB), der ihre Umsetzung beratend und kontrollierend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Dabei gelten folgende Grundsätze:

>> Die DV-Hard- und Software sind für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.

>> Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.

>> Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.

>> Der Datenschutzbeauftragte berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSB auskunftspflichtig.

2. Der betriebliche Datenschutzbeauftragte/Datenschutzkoordinatoren

2.1 Die XY-GmbH hat nach Maßgabe des Artikels 37 DS-GVO einen betrieblichen Datenschutzbeauftragten (DSB) und einen Abwesenheitsvertreter bestellt. Die Kontaktdaten des Datenschutzbeauftragten sind zu finden unter: [...]

Der DSB nimmt die ihm kraft Gesetzes und aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation wahr.

2.2 Der Datenschutzbeauftragte unterrichtet und berät die Unternehmensleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.

Im Falle risikoreicher Datenverarbeitungen steht der DSB dem Verantwortlichen beratend bei der Abschätzung des Risikos zur Seite.

2.3 Der DSB berichtet unmittelbar der Unternehmensleitung.

2.4 Der DSB wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

2.5 Soweit es sich aufgrund organisatorischer Gegebenheiten (z.B. bei unselbstständigen externen Filialbetrieben) als notwendig erweist, ernennt die

Geschäftsleitung im Benehmen mit dem DSB für die jeweilige Organisationseinheit einen Datenschutzkoordinator.

Der Koordinator ist also insoweit ein dem DSB fachlich zugewiesener Mitarbeiter zur Einhaltung der für das Unternehmen geltenden Datenschutzvorschriften. Er informiert den DSB über vor Ort aufgetretene Datenschutzfragen. Er erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren und gibt die Meldung an den DSB weiter.

2.6 Das Unternehmen hat ein Verzeichnis über alle Verarbeitungsvorgänge zu führen. In jeder Fachabteilung wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DS-GVO zu dokumentieren. Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann der Datenschutzbeauftragte beratend hinzugezogen werden. Dem Datenschutzbeauftragten ist eine Kopie des Verfahrensverzeichnisses zu übergeben.

Auf Anfrage stellt das Unternehmen der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Unternehmensleitung ist hierfür der Datenschutzbeauftragte zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

2.7 Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSB wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

2.8 Der DSB berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Soweit der Bericht die Verarbeitung von Personaldaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Betriebsrat zugänglich gemacht.

3. Beschaffung/Hard- und Software

3.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden Person/Abteilung durch die zentrale DV-Beschaffung. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet. Die Verfahrensweisung **„Checkliste zur Beachtung der Anforderungen an Privacy-by Design/ Privacy-by-Default“ (Anlage 1)** ist maßgebend.¹

3.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzbeauftragte rechtzeitig vorab von der anfordernden Stelle zu informieren (siehe hierzu Näheres in Ziff. 5.2). Die Beschaffung erfolgt erst nach Stellungnahme des DSB. Der DSB berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die Durchführung einer Datenschutz-Folgenabschätzung richtet sich nach der Verfahrensweisung **„Risikominimierung durch Datenschutz-Folgenabschätzung“ (Anlage 2)**.²

3.3 Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z.B. private Notebooks) bedarf der Genehmigung durch die IT-Abteilung im Einzelfall.

3.4 Die IT-Abteilung führt ein Verzeichnis der eingesetzten Hardware und der verwendeten Anwendungsprogramme. Der DSB erhält eine Kopie (alternativ: Der DSB kann auf das Verzeichnis jederzeit zugreifen).

3.5 Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind die DV-Abteilung und der DSB unverzüglich zu informieren. Näheres regelt die Verfahrensweisung **„Verhaltensmaßnahmen bei einer Datenpanne“ (Anlage 3)**.³

4. Verpflichtung/Schulung der Mitarbeiter

4.1 Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

4.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushängung des von dem DSB erstellten Merkblatts durch die Personalabteilung (alternativ: insgesamt oder für bestimmte Bereiche durch den DSB).

¹ Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

² Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

³ Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

4.3 Mitarbeiter, die besonderen Geheimhaltungsverpflichtungen (z.B. Fernmeldegeheimnis nach § 88 TKG) unterliegen, werden von den Vorgesetzten ergänzend schriftlich verpflichtet. Die jeweilige Verpflichtungserklärung ist zu den Personalakten zu nehmen.

4.4 Der DSB ist über die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmenden weiteren Schulungen und die Feststellung evtl. Kontrollbedarfs zu informieren.

4.5 Für in Abstimmung mit den jeweiligen Abteilungsleitungen angesetzte Schulungstermine sind die betroffenen Mitarbeiter freizustellen.

5. Transparenz der Datenverarbeitung

5.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Datenschutzbeauftragte ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO. Der für ein Verfahren Verantwortliche bzw. der zuständige Datenschutzkoordinator meldet dieses zeitnah gemäß den vom DSB definierten Vorgaben. Gleiches gilt für Veränderungen (Change Request).



Ein öffentliches „Jedermann-Verzeichnis“ existiert nach der DS-GVO nicht mehr. Ein Großteil der hierin enthaltenen Informationen werden den betroffenen Personen dennoch nach den Artt. 13, 14 und 15 zur Verfügung gestellt.

5.2 Unabhängig von dieser Meldung ist der DSB bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren (vgl. Ziff. 6.3). Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Internet-Homepage etc.) ist der Erhebungsbogen etc. dem DSB zur Abstimmung vorzulegen.

5.3 Soweit der DSB feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilt er dies umgehend mit. Das Verfahren darf erst nach Zustimmung des DSB durchgeführt werden. Im Zweifel entscheidet die Geschäftsleitung.

5.4 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den DSB (bei Unternehmen mit regelmäßigen Auskunftsbegehren kann auch eine Zuständigkeit der Fachabteilung zweckmäßig sein). Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt.

Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld einvernehmlich durch den DSB und die IT-Abteilung festzulegen. Hierzu ist die Verfahrensanweisung „**Datenportabilität**“ zu beachten (**Anlage 4**).⁴

⁴ Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

6. Erhebung/Verarbeitung von personenbezogenen Daten

6.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. Weitere Erlaubnistatbestände, die den Umgang mit personenbezogenen Daten im Unternehmen legitimieren können, werden in der Verfahrensweisung „**Umgang mit personenbezogene Daten/Erlaubnistatbestände der DS-GVO**“ anhand zahlreicher (auf das Unternehmen angepasster) Beispielsfälle dargestellt (**Anlage 5**).⁵

6.2 Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (**bspw. Profiling**).

6.3 Vor Einführung neuer Arten von Erhebungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen.

Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren. Einen Kriterienkatalog dazu enthält die Verfahrensweisung „**Kompatibilitätscheck bei Zweckänderung**“ (**Anlage 6**).⁶ Dieser ist zu beachten.

Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

6.4 Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist der DSB zu kontaktieren.

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch die IT-Abteilung und der Registrierung durch die den Träger einsetzende Abteilung/Benutzer. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

⁵ Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

⁶ Die Anlage ist fiktiv, sie kann ggf. unternehmensspezifisch mit Inhalt gefüllt werden.

7.2 Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

7.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

7.4 Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

8. Externe Dienstleister/Auftragsverarbeitung/Wartung

8.1 Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist der DSB vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

8.2 Entsprechendes gilt, falls die XY-GmbH entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

9. Sicherheit der Verarbeitung

9.1 Für jedes Verfahren ist eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

9.2 Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität der Daten sowie der Belastbarkeit der Daten verarbeitenden Systeme ist ein allgemeines Sicherheitskonzept zu erstellen. Das Konzept orientiert sich an der zuvor erstellten Schutzbedarfsfeststellung und der Risikoanalyse. Dieses Konzept ist maßgeblich für alle weiteren Verfahren.

9.3 Neben dieser Richtlinie bestehen ergänzende Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen. Hierzu gehören u.a.

>> Arbeitsanweisung zum datenschutzgerechten Versand von Datenträgern und zur Verschlüsselung von Daten

>> Arbeitsanweisung zum Passwortverfahren



Eine Aufstellung technisch-organisatorischer Maßnahmen nach Art. 32 DS-GVO findet sich in der GDD-Praxishilfe DS-GVO IV, S. 21 f.

- >> Arbeitsanweisung zur Erteilung von Auskünften im Personalbereich
- >> Arbeitsanweisung zur PC- und Laptop-Nutzung
- >> Arbeitsanweisung Telearbeit/Home-Office

Ferner ist die Verarbeitung von Personaldaten in einer Anzahl von Betriebsvereinbarungen näher festgelegt. Hierzu gehören u. a. die Vereinbarung

- >> über die Nutzung von Telekommunikation (Telefon, E-Mail, Internet) in der *XY-GmbH*
- >> die Vergabe von Telearbeit/Homeoffice

10. Rechenschafts- und Dokumentationspflicht



Zur Rechenschafts- und Dokumentationspflicht siehe GDD-Praxishilfe IX - Accountability.

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein („Accountability“). Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.



Gesellschaft für Datenschutz
und Datensicherheit e.V.

Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Herausgeber:

Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)

Heinrich-Böll-Ring 10

53119 Bonn

Tel.: +49 2 28 96 96 75-00

Fax: +49 2 28 96 96 75-25

www.gdd.de

info@gdd.de

Stand:

Version 1.2 (Oktober 2017)