Richtlinie Datenschutz

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

Fassung gemäß Vorstandsbeschluss vom 05.08.2021

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Richtlinie Datenschutz
Version	21.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft
Erstmalige Freigabe	11.04.2019
Verabschiedet durch (Datum)	Vorstand (05.08.2021)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	Juli 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	11.04.2019	Ersterstellung	Daniel Fürdauer
20.0	29.07.2020	Jährliches Review, Redaktionelle Änderungen	Daniel Fürdauer
21.0	29.07.2021	Jährliches Review, Entfall der Anpassung bei 2.1.10	Daniel Fürdauer

Art der Freigabe – VHV Konzern

Version	Datum	Wesentliche Änderungen	Bestätigt von
19.0	11.04.2019	Nein	Sina Rintelmann (i.V. Carsten Kluge)
20.0	05.08.2020	Nein	Roman Lemke
21.0	30.07.2021	Nein	Roman Lemke
Wesentliche Änderungen	→Nein: Bestätigung durch Konzerndatenschutzbeauftragter →Ja: Bestätigung durch Vorstand VHV Holding		

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

1. ANPASSUNGEN AN DIE „KONZERNRICHTLINIE DATENSCHUTZ VERSION 21.1“ DER VHV GRUPPE

In den folgenden Punkten ist die „Richtlinie DATENSCHUTZ“ der VAV Versicherungs-Aktiengesellschaft (im Folgenden kurz VAV genannt) an die Konzernrichtlinie DATENSCHUTZ der VHV Gruppe anzupassen:

Allgemeine Anpassungen:

Das deutsche Bundesdatenschutzgesetz (BDSG) ist durch das österreichische Datenschutzgesetz (DSG) zu ersetzen.

Die Abteilung Konzerndatenschutz und Informationssicherheit (KDI) der VHV entspricht der Stabstelle Datenschutz und Informationssicherheit in der VAV. Die E-Mailadresse datenschutz_sicherheit@vhv.de entspricht datenschutz@vav.at bei der VAV.

Der Code of Conduct der deutschen Versicherungswirtschaft gilt nicht in Österreich. Es wird derzeit an einem österreichischen Code of Conduct gearbeitet.

Das WorkNet entspricht dem Intranet und dem Fileserver bei der VAV.

§203 StGB entfällt und entspricht der jeweils passenden Verschwiegenheitspflicht.

Gesetzesstellen des deutschen Rechts, die nicht explizit angepasst wurden, sind mit der entsprechenden Gesetzesstelle des österreichischen Rechts zu ersetzen.

Bei etwaigen Unklarheiten in Bezug auf die Richtlinie ist der Datenschutzbeauftragte zu kontaktieren.

2.1.1 Einwilligung

Die firmeninterne Nutzung von Fotos und Videos von Mitarbeitern beruht auf dem berechtigten Interesse des Verantwortlichen oder der konkludenten Einwilligung.

2.1.1.1 Einwilligung in Telefon- und E-Mail-Werbung

Direktwerbung per E-Mail stellt keine Ausnahme dar. Es ist zwingend eine Einwilligung erforderlich. Etwaige Ausnahmen sind nur nach Rücksprache und Freigabe mit bzw. durch den Datenschutzbeauftragten möglich.
Die angegebenen §§ sind nicht zu beachten und bei Unklarheiten ist der Datenschutzbeauftragte zu kontaktieren.

2.1.1.2 Einwilligung bei Gesundheitsdaten

Gesundheitsdaten dürfen nur auf gesetzlicher Grundlage (§11a VersVG ff) oder auf Grundlage einer mit der Datenschutzbehörde abgestimmten Einwilligungs- und Schweigepflichtentbindungserklärung verarbeitet werden. Die Einwilligungs- und Schweigepflichtentbindungserklärung berücksichtigt alle vorgenannten Voraussetzungen an eine wirksame Einwilligung. Sie kann grundsätzlich mit Wirkung für die Zukunft widerrufen

werden. Ist die Einwilligung allerdings für die Durchführung des Vertrages erforderlich, ist ein Widerruf nach den Grundsätzen von Treu und Glauben ausgeschlossen bzw. führt dazu, dass die Leistung in der Regel nicht erbracht werden kann, was dem Betroffenen sodann mitzuteilen ist.
Die Verarbeitung von Gesundheitsdaten ist im Detail mit dem Datenschutzbeauftragten festzulegen und hat in den Arbeitsanweisungen geregelt zu sein.
Die restlichen Absätze entfallen.

2.1.9 Verarbeitung von Mitarbeiterdaten

§26 BDSG gilt nicht.

2.1.11.1 Auftragsverarbeitung

Bei Auftragsverarbeitungen ist zwingend der Datenschutzbeauftragte einzubeziehen. Er stellt in weiterer Folge die Vertragsmuster zur Verfügung, die bei Bedarf anzupassen sind.

2.1.11.2 Datenverarbeitung durch Dienstleister ohne Auftragsverarbeitung

In Österreich gibt es keine vergleichbare Regelung. Unabhängig davon handelt es sich bei den angeführten Dienstleistern um eigene Verantwortliche und es sind die jeweiligen gesetzlichen Regelungen zu beachten.

2.1.12 Sonderfälle nach dem Code of Conduct

Der österreichische Branchenstandard (ÖBS) ist derzeit noch in Erstellung. Die beschriebenen Fälle wurden unabhängig davon geregelt und werden eventuell ebenfalls in den ÖBS aufgenommen.

2.1.12.1 Datenaustausch mit anderen Versicherern:

Das Kapitel ist wie folgt zu ersetzen:
Es gibt einen Datenaustausch mit anderen Versicherungen. Es gibt hierbei insbesondere das Bonus-Malus-System.
Der genaue Datenaustausch ist in den jeweiligen Arbeitsanweisungen geregelt und wird mit dem Datenschutzbeauftragten abgestimmt.

2.1.12.2 Datenübermittlung an Rückversicherer

Die Rückversicherer führen u.a. auch bei fakultativen Rückversicherungen im Einzelfall die Risikoprüfung und die Leistungsprüfung durch

2.1.12.4 Verarbeitung von Stammdaten in der Unternehmensgruppe

Die Stammdaten von Betroffenen werden ausschließlich in der VAV verarbeitet und es erfolgt keine zentralisierte Bearbeitung. Ausnahmen und insbesondere Auftragsverarbeitungen werden vertraglich geregelt.

3 Betroffenenrechte

Anfragen zu 3.1 Auskunftsrecht, 3.3 Recht auf Löschung, 3.4 Recht auf Einschränkung der Verarbeitung, 3.5 Recht auf Datenübertragbarkeit und 3.6.1 Widerspruch bei einwilligungsloser Verarbeitung zur Wahrung berechtigter Interessen sind nicht von den

jeweiligen Fachbereichen zu beantworten, sondern an die Stabstelle Datenschutz und Informationssicherheit weiterzuleiten. Die Stabstelle Datenschutz und Informationssicherheit legt die weitere Vorgehensweise fest.
Anfragen zu 3.6.2 Widerspruch bei Direktwerbung können entsprechend der jeweiligen Arbeitsanweisung direkt durchgeführt werden, oder an die Stabstelle Datenschutz und Informationssicherheit weitergeleitet werden.

4 Datenschutz-Folgenabschätzung

Die Rolle des Risikoverantwortliche übernimmt der dezentrale Risiko-Verantwortliche, der dezentrale Datenschutz-Verantwortliche oder eine sonstige fachlich qualifizierte Person.
Das Konzept zur DSFA der VHV Gruppe ist zu beachten und etwaige Abweichungen sind mit dem Datenschutzbeauftragten abzustimmen, die gesetzlichen Vorgaben müssen allerdings eingehalten werden.

5 Meldungen bei Verletzung des Schutzes personenbezogener Daten (Datenpanne):

Das Kapitel ist wie folgt zu ersetzen:
Bei Datenschutzvorfällen sind die Anweisungen im Intranet zu beachten und es ist nach der Richtlinie Data Breach Prozess, in der jeweils aktuellen Fassung, vorzugehen.

KONZERNRICHTLINIE

DATENSCHUTZ

KONZERNDATENSCHUTZ UND INFORMATIONSSICHERHEIT
KLASSIFIKATION: INTERN
VERSION 21.1

VHV GRUPPE

Dokumenteneigenschaften

Typ	Konzernrichtlinie
Geltungsbereich	Siehe Kapitel „Geltungsbereich“
Erstmalige Freigabe	03.12.2014
Verabschiedet durch (Datum)	VHV Vereinigte Hannoversche Versicherung a.G. (11.02.2021) VHV Holding AG (11.02.2021) VHV Allgemeine Versicherung AG (11.02.2020) Hannoversche Lebensversicherung AG (11.02.2020) WAVE Management AG (11.02.2020) Pensionskasse der VHV Versicherungen (11.02.2020)
Klassifikation	Intern
Dokumentenverantwortlicher Verantwortliche Abteilung	Ulrich Lintker (Abteilungsleiter KDI) Konzerndatenschutz und Informationssicherheit (KDI)
Fachlicher Ansprechpartner	Carsten Kluge
Letztes Review	Juli 2021

Historie

Version	Freigabedatum	Beschreibung der Änderung
15.0	01.01.2015	Initiale Erstellung
16.0	08.12.2016	Anpassung auf Code of Conduct (CoC)
17.0	18.12.2017	Änderung der Abteilungsbezeichnung wegen Neugründung Abteilung KDI, Anpassung des Geltungsbereiches, Streichung der Datenschutzgrundsätze aufgrund der neuen Konzernrichtlinie zum Datenschutzmanagementsystem, Anpassung des Postfaches für Sicherheitsvorfälle.
18.0	30.05.2018	Finale Anpassung des Dokuments auf die Vorgaben der DSGVO. Umstrukturierungen der Richtlinie und Aufnahme des Konzepts zur DSFA in der Anlage.
19.0	29.01.2019	Jährliches Review: Neue Versionierung, redaktionelle Änderungen und Anpassungen in den Kapiteln 2.1.10, 2.3.1, 0, 3.5 und 5.
20.0	28.01.2020	Redaktionelle Änderungen und Ergänzungen in Kapitel 3.3.

Version	Freigabedatum	Beschreibung der Änderung
21.0	15.02.2021	Jährliches Review: Neue Versionierung, redaktionelle Änderungen und Anpassungen in den Kapiteln 2.1.9, 2.1.10
21.1	05.07.2021	Redaktionelle Änderung und Anpassung in Kapitel 2.1.10

Änderungen zur Vorgängerversion sind grün hervorgehoben.

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhaltsverzeichnis

Abkürzungsverzeichnis

AO ..... Abgabenordnung
AV ..... Auftragsverarbeitung
BetrVG ..... Betriebsverfassungsgesetz
DSGVO ..... Datenschutz-Grundverordnung
GPS ..... Global Positioning System
SDM ..... Standard-Datenschutzmodell
SPoC ..... Single Point of Contact
TOM ..... Technische und organisatorischen Maßnahmen
TVG ..... Tarifvertragsgesetz
UWG ..... Gesetz gegen den unlauteren Wettbewerb
VVG ..... Versicherungsvertragsgesetz

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Zielsetzung der Konzernrichtlinie

Die Konzernrichtlinie Datenschutz ist Teil des Datenschutzmanagementsystems (DSMS) der VHV Gruppe. Ziel der Richtlinie ist, basierend auf den geltenden Datenschutzbestimmungen einen einheitlichen Datenschutzstandard innerhalb der Konzerngesellschaften der VHV Gruppe zu schaffen. Zu diesem Zweck gibt die Richtlinie Vorgaben und Hilfestellungen zur Umsetzung der in der Konzernrichtlinie Datenschutzmanagementsystem aufgestellten Datenschutzgrundsätze. Die Anforderungen der Konzernrichtlinie Datenschutz werden durch die Einzelgesellschaften in Arbeitsanweisungen weiter konkretisiert. Die Konzernrichtlinie Datenschutz steht neben der Konzernrichtlinie Informationssicherheit, deren Zielsetzung der generelle Schutz von Informationswerten ist.

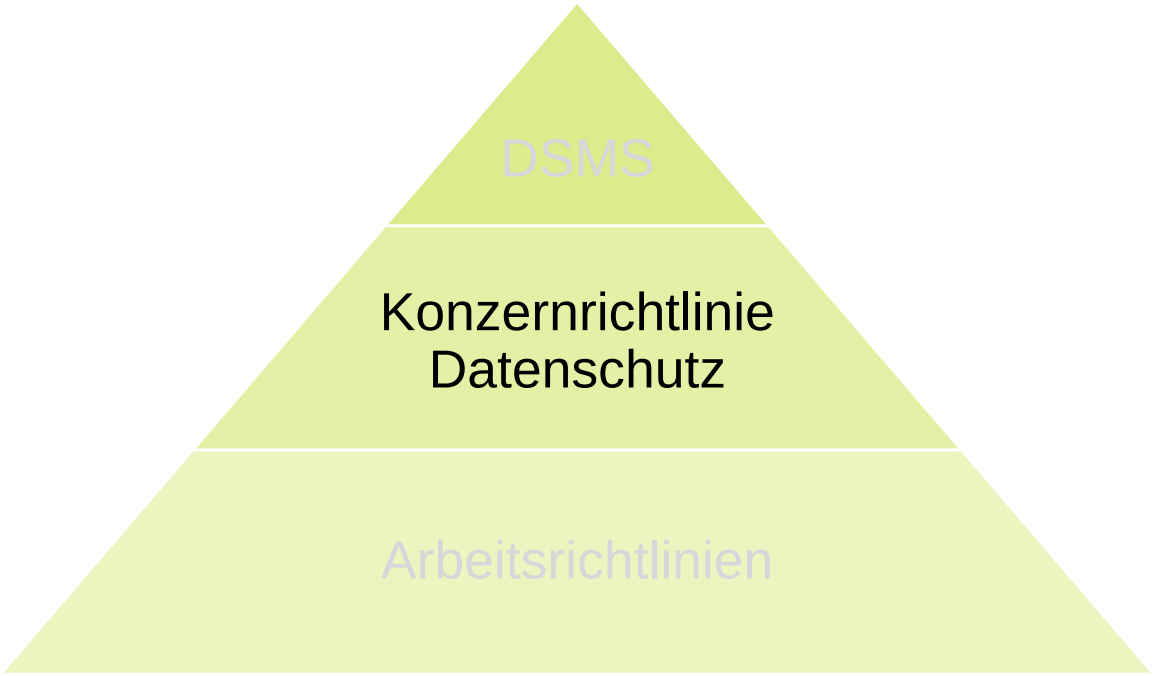

Abbildung 1: Einordnung der Konzernrichtlinie in die Dokumentenpyramide

1.2 Regulatorische und gesetzliche Vorgaben

Die Regelungen der Richtlinien leiten sich, nicht abschließend aufgezählt, aus folgenden relevanten Regelungen und Gesetzen mit datenschutzrechtlichem Bezug ab:

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung; folgend: DSGVO),
- Bundesdatenschutzgesetz (BDSG), in der jeweils gültigen Fassung,
- Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft (Code of Conduct, kurz: CoC), in der jeweils gültigen Fassung,
- Das Gesetz gegen den unlauteren Wettbewerb (UWG), in der jeweils gültigen Fassung.

1.3 Geltungsbereich

Die Konzernrichtlinie Datenschutz erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten von betroffenen Personen. Dies umfasst natürliche Personen, d. h. insbesondere die personenbezogenen Daten von Versicherungsnehmern, Geschädigten und Vermittlern sowie von Mitarbeitern der VHV Gruppe.

Die Konzernrichtlinie findet Anwendung auf die nachfolgenden Unternehmen der VHV Gruppe:

- VHV Vereinigte Hannoversche Versicherung a.G.
- VHV Holding AG
- VHV Allgemeine Versicherung AG
- Hannoversche Lebensversicherung AG
- (VAV Versicherungs-Aktiengesellschaft)
- WAVE Management AG

Für die VAV Versicherungs-Aktiengesellschaft findet diese Konzernrichtlinie nur nach Maßgabe eines ergänzenden Teils Anwendung, der die spezifisch für die VAV Versicherungs-Aktiengesellschaft geltenden Regelungen konkretisiert und vom Vorstand der VAV Versicherungs-Aktiengesellschaft in Kraft gesetzt wird.

Die nachfolgenden Gesellschaften werden von dieser Konzernrichtlinie insofern erfasst als sie Funktionen und Dienstleistungen für die vorstehenden Unternehmen wahrnehmen:

- VHV solutions GmbH
- VVH Versicherungsvermittlung Hannover GmbH
- Hannoversche – Consult GmbH
- Hannoversche Direktvertriebs GmbH
- VHV Vermögensanlage AG
- VHV Dienstleistungen GmbH
- digital broking GmbH
- Pensionskasse der VHV Versicherungen

1.4 Anwendbarkeit auf datenschutzrelevante Tätigkeiten

Die nachstehenden Regelungen sind anwendbar für jedes Verfahren, bei dem personenbezogene Daten verarbeitet werden. Personenbezogene Daten werden definiert als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung oder zu einem oder mehreren Merkmalen identifiziert werden kann.

> Von Kennungen sind umfasst: Name, Kennnummer (z. B. VN-Nummer, Schadennummer), Standortdaten, Online-Kennung etc.
>
> Merkmal bedeutet: Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person.

Eine Verarbeitung der genannten Daten liegt vor, wenn diese mit oder ohne Hilfe automatisierter Verfahren erhoben, erfasst, organisiert, geordnet, gespeichert, angepasst, verändert, ausgelesen, abgefragt, verwendet werden oder durch Übermittlung, Verbreitung offengelegt werden oder durch eine andere Form bereitgestellt werden, abgeglichen, verknüpft, eingeschränkt, gelöscht oder vernichtet werden.

Die Beurteilung, ob ein Prozess, der den oben genannten Voraussetzungen entspricht datenschutzrelevant ist, obliegt der fachlich verantwortlichen Person. Die Verantwortlichkeit ergibt sich aus Kapitel 4 der Konzernrichtlinie Datenschutzmanagement. In Zweifelsfällen wird der Datenschutzbeauftragte hinzugezogen.

2 Vorgaben zur Umsetzung der Datenschutzgrundsätze

Die in der Konzernrichtlinie DSMS aufgestellten Grundsätze zum Datenschutz ergeben sich aus dem Zusammenwirken einzelner zu erfüllenden gesetzlicher Vorschriften. Im Folgenden werden die zu den Datenschutzgrundsätzen typischen Anwendungsfälle geregelt:

2.1 Rechtmäßigkeit

Vor Beginn einer neuen Verarbeitungstätigkeit ist zu prüfen, ob die Verarbeitung der personenbezogenen Daten rechtmäßig ist. Grundsätzlich ist jede Verarbeitung von personenbezogenen Daten verboten, es sei denn sie ist erlaubt (sog. „Verbot mit Erlaubnisvorbehalt“). Eine Erlaubnis ist nur gegeben, wenn eine Rechtsgrundlage besteht, also wenn beispielsweise eine Einwilligung eingeholt worden ist. Gesetzliche Erlaubnistatbestände ergeben sich entweder aus der DSGVO oder anderen, spezialgesetzlichen Normen. Die Verarbeitung von personenbezogenen Daten ist somit grundsätzlich unter den nachfolgenden Bedingungen gestattet.

2.1.1 Einwilligung

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn die betroffene Person, zum Beispiel ein Versicherungsnehmer, seine Einwilligung in die Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere Zwecke gegeben hat. Die Einwilligung muss nachweisbar vorliegen, damit die Verarbeitung der personenbezogenen Daten im Kontext der Einwilligung erfolgen darf. Die Einwilligung ist mithin eine mögliche Grundlage für eine rechtmäßige Verarbeitung von personenbezogenen Daten.

<u>Voraussetzungen für eine wirksame Einwilligung:</u>

- Die Einwilligung muss auf der freien Entscheidung der betroffenen Person beruhen. Die betroffene Person muss in der Lage sein, ihre Einwilligung zu verweigern. Es gilt, jegliche Druck- oder Zwangssituation zu vermeiden. Bedeutung erlangt dies, wenn bspw. zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht. Eine Freiwilligkeit ist auch dann nicht gegeben, wenn die Durchführung eines Vertrages davon abhängig gemacht wird, obwohl die Datenverarbeitung für diese Durchführung nicht erforderlich ist (sog. „Kopplungsverbot“). Damit sind vornehmlich Daten gemeint, die gerade nicht zur Vertragsdurchführung benötigt werden. Beispielsweise darf der Vertragsschluss nicht an eine Einwilligung zu einem Newsletter-Versand gekoppelt werden.
- Die betroffene Person muss in verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache über die Zwecke und die Reichweite der Verarbeitung und auch über etwaige Datenempfänger informiert werden.
- Die betroffene Person muss über die Möglichkeit des Widerrufs vor Abgabe der Einwilligung in Kenntnis gesetzt werden und es ist auf die Folgen der Verweigerung der Einwilligung hinzuweisen.
- Es ist zu gewährleisten, dass für die Erbringung der Dienstleistung nur in die Verarbeitung der benötigten Daten eingewilligt wird.
- Sollte die Einwilligung zusammen mit mehreren anderen Erklärungen eingeholt werden (bspw. bei einem Versicherungsantrag), muss diese so hervorgehoben werden, dass sie ins Auge fällt.

<u>Form der Einwilligung:</u>

Vorab ist klarzustellen, dass die Einwilligung nach der Datenschutz-Grundverordnung an keine Form gebunden ist. Daher kann die Einwilligung grundsätzlich auch mündlich, in Textform oder elektronisch (bspw. am Telefon, per „Häkchen setzen“ im Browser, per E-Mail etc.) erfolgen. Die Einwilligung muss jedoch dokumentierbar sein. Die VHV hat mithin sicherzustellen, dass uns erteilte Einwilligungen nachweisbar sind. Daher gelten folgende Ausführungen:

Schriftform:

- Die Einwilligung sollte vornehmlich schriftlich eingeholt werden. Schriftlich meint dabei, dass die Einwilligung von der betroffenen Person handschriftlich unterzeichnet sein muss.

Textform:

- Die Einwilligung kann auch, ebenfalls gut dokumentierbar, in Textform eingeholt werden. Dies meint vornehmlich die Einwilligung per E-Mail-Nachricht.

Elektronische Form:

- Der Text der Einwilligungserklärung sollte zur Dokumentation zeitnah in Text- oder Schriftform bestätigt werden, wenn die elektronische Einwilligung bspw. durch „Häkchen-Setzung“ im Browser erfolgte.
- Die Bestätigung kann z. B. per E-Mail oder aber im Rahmen der Übermittlung der Police erfolgen.
- Die Bestätigung kann entfallen,
    - wenn im elektronischen Antragsprozess sichergestellt ist, dass die Abgabe der Erklärung protokolliert wird
    - und der Inhalt der Erklärung unverändert reproduzierbar in den Herrschaftsbereich des Betroffenen gelangt ist, z. B. durch einen Download.
    - Ferner müssen die Betroffenen den Erhalt und die Lesbarkeit, etwa durch Anklicken eines Feldes, bestätigt haben.

Mündlich:

- Möglichst nur in Ausnahmefällen, z. B. bei einer telefonischen Kontaktaufnahme, kann die Einwilligung auch mündlich erteilt werden, sofern der Gesprächsinhalt dokumentiert und der Betroffene unverzüglich eine Bestätigung in Text- oder Schriftform über die erteilte Einwilligung erhält.

Bei Rückfragen zu Formulierungen von Einwilligungserklärungen, insbesondere im Rahmen der Planung von Werbemaßnahmen, sollte die Abteilung Konzerndatenschutz und Informationssicherheit (folgend: KDI) kontaktiert werden (E-Mail: datenschutz_sicherheit@vhv.de).

Hinweis: Im Rahmen des Code of Conduct hat man in Abstimmung mit den Datenschutzaufsichtsbehörden zulässige Datenverarbeitungen im Versicherungsgeschäft geregelt und deren Voraussetzungen festgelegt. Dies hat dazu geführt, dass Einwilligungen im vorgenannten Sinne nur noch in wenigen Fällen erforderlich sind. Ein typischer Fall, in dem eine Einwilligung des Betroffenen noch benötigt wird, ist bei der Verarbeitung von Gesundheitsdaten im Rahmen einer Schweigepflichtentbindungserklärung.

Weitere Anwendungsfälle für die Einwilligung sind bspw.: Das Erstellen und Nutzen von Fotos und Videos der Mitarbeiter, z. B. im WorkNet oder in Werbevideos.

2.1.1.1 Einwilligung in Telefon- und E-Mail-Werbung

Telefon- und E-Mail-Werbung erfordern grundsätzlich eine Einwilligung des Betroffenen. Hierbei ist darauf zu achten, dass die Einwilligung optisch gut sichtbar ist und sich von etwaigen anderen, gleichzeitig eingeholten Einwilligungserklärungen abhebt, z. B. durch einen entsprechenden Fettdruck oder ein gesondertes Opt-in. Sie darf auch nicht an die Abgabe einer anderen Erklärung gekoppelt werden (vgl. Kapitel 2.1.1).

Eine Ausnahme davon stellt Direktwerbung per E-Mail dar. Diese erfolgt in der Regel auf Grund eines berechtigten Interesses des Werbenden, also einer anderen Rechtsgrundlage. Voraussetzung für eine Verarbeitung der Daten ohne Einwilligung ist zudem, dass das werbende Unternehmen die E-Mail-Adresse eines Betroffenen im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung erhalten hat, es diese Adresse nur zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet, der Betroffene der Nutzung seiner E-Mail-Adresse nicht widersprochen hat und der Betroffene bereits bei Eingabe seiner E-Mail-Adresse (und in jedem darauffolgenden Newsletter) klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen anfallen.

Eine weitere Ausnahme stellt die Direktwerbung per Post dar. Diese ist in der Regel aufgrund berechtigter Interessen seitens des Werbenden zulässig. Auch fällt postalische Werbung grundsätzlich nicht unter die strengen Voraussetzungen des § 7 Abs. 2 Nr. 2-4 UWG.

Bei Vorhaben im Bereich der Telefonie- oder E-Mail-Werbung sind zudem die Vorgaben des UWG zu beachten (insbesondere § 7 UWG).

Beispiel einer Einwilligung: „Ich willige mit der Angabe meiner E-Mail-Adresse und Telefonnummer ein, künftig über [Beschreibung des Werbegegenstands] per E-Mail und per Telefon informiert zu werden. Ich kann meine Einwilligung per E-Mail an [E-Mail-Adresse] oder telefonisch unter [Telefon-nummer] jederzeit mit Wirkung für die Zukunft widerrufen."

Achtung: Der Widerruf darf an keine strengeren Voraussetzungen geknüpft werden als die Erteilung der Einwilligung selbst. Das heißt: Wird die Einwilligung elektronisch eingeholt, muss auch der Widerruf elektronisch möglich sein. Ein Verweis auf bloße Schriftform wäre daher nicht zulässig.

Beispiel einer schriftlichen Einwilligungsbestätigung nach telefonischer Einwilligung: „Sehr geehrter Herr Mustermann,

vielen Dank für das freundliche Telefonat und Ihr Einverständnis, dass wir Sie für <Zweckangabe> kontaktieren dürfen.

Die <VHV Gesellschaft> ist ein starker Partner, wenn es um Ihre Absicherung geht. <kurzer Text zur Beschreibung der Werbemaßnahme>

Sie können Ihre Einwilligung zu der Teilnahme jederzeit widerrufen. Bitte schreiben Sie dazu an folgende E-Mail-Adresse: <E-Mail-Adresse für Werbeverweigerer>. Unsere Datenschutzhinweise finden Sie unter folgendem Link: <Link zu den Datenschutzhinweisen>.

Sollten Sie noch Fragen zu Ihrer Versicherung oder Interesse an weiteren Produkten haben, zögern Sie nicht, uns anzusprechen. Unsere kompetenten Berater freuen sich auf Ihren Anruf und stehen Ihnen gern für alle Fragen unter <Service-Nummer> zur Verfügung.

Freundlich grüßt Sie,

<VHV-Gesellschaft>"

2.1.1.2 Einwilligung bei Gesundheitsdaten

Gesundheitsdaten dürfen nur auf gesetzlicher Grundlage oder auf Grundlage der mit den Datenschutzaufsichtsbehörden abgestimmten Einwilligungs- und Schweigepflichtentbindungserklärung nach dem CoC verarbeitet werden. Die Einwilligungs- und Schweigepflichtentbindungserklärung berücksichtigt alle vorgenannten Voraussetzungen an eine wirksame Einwilligung. Sie kann grundsätzlich mit Wirkung für die Zukunft widerrufen werden. Ist die Einwilligung allerdings für die Durchführung des Vertrages erforderlich, ist ein Widerruf nach den Grundsätzen von Treu und Glauben ausgeschlossen bzw. führt dazu, dass die Leistung in der Regel nicht erbracht werden kann, was dem Betroffenen sodann mitzuteilen ist.

Die Verarbeitung von Gesundheitsdaten auf gesetzlicher Grundlage (vornehmlich gemäß Art. 6 in Verbindung mit Art. 9 DSGVO) ist zulässig, insbesondere wenn es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist. Das gilt beispielsweise für die Prüfung und Abwicklung der Ansprüche von Versicherten sowie von Geschädigten in der Haftpflichtversicherung. In diesen Fällen ist eine vorige Einwilligung nicht notwendigerweise einzuholen.

Ebenso kann die Verarbeitung von Gesundheitsdaten ohne Einwilligung zum Schutz lebenswichtiger Interessen der betroffenen oder anderer Personen erfolgen, wenn diese aus körperlichen oder rechtlichen Gründen außerstande sind, ihre Einwilligung zu geben. Insbesondere ist das der Fall, wenn für diese Personen Assistance-Leistungen (z. B. Notrufdienste, Krankentransport aus dem Ausland oder Koordination der medizinischen Behandlung) vereinbart und sie im Leistungsfall außer Stande sind, ihre Einwilligung abzugeben (z. B. weil nach einem Unfall ein Krankentransport für eine bewusstlose Person nötig ist).

Muster der aktuellen Einwilligungs- und Schweigepflichtentbindungserklärungen sind im WorkNet der VHV Gruppe zu finden und in den jeweiligen Antrags- bzw. Schadenprozessen hinterlegt. Sie unterscheiden sich je nach Sparte (Unfall, Leben, Kraftfahrt-Schaden). Aufgrund der Abstimmung mit den Datenschutz-Aufsichtsbehörden ist von individuellen Anpassungen abzusehen. Bei Fragen ist die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de) hinzuzuziehen.

2.1.2 Verarbeitung zur Erfüllung von Verträgen

Eine Verarbeitung von personenbezogenen Daten ist zulässig, wenn diese für die Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen oder dessen Partei die betroffene Person ist. Beispielsweise dürfen im Rahmen des Versicherungsgeschäfts Daten erhoben werden, die für die Erstellung eines Angebots, die Bearbeitung des Antrags, zur Beurteilung eines zu versichernden Risikos, zur Erfüllung der Beratungspflichten, zur Prüfung einer Leistungspflicht oder zur internen Prüfung des fristgerechten Forderungsausgleichs erforderlich sind.

Beispiel 1: Der Kunde übermittelt dem VU die für seine Kraftfahrtversicherung notwendigen personenbezogenen Daten. Das VU verarbeitet diese Daten zur Risikoprüfung und anschließenden Policierung sowie zur Vertragsabwicklung.

Beispiel 2: Der VN meldet zum Zwecke der Schadenanzeige personenbezogene Daten bei dem VU ein. Das VU verarbeitet diese Daten zum Zweck der Schadenregulierung.

Beispiel 3: Ein Interessent übermittelt dem VU personenbezogene Daten über eine Online-Maske, um sich ein Angebot erstellen zu lassen.

2.1.3 Verarbeitung aufgrund berechtigter Interessen

Eine Verarbeitung ist erlaubt, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Dabei dürfen nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Es erfolgt mithin eine Interessenabwägung im Einzelfall. Diese muss dokumentiert werden.

Sobald bspw. neue Werbeprodukte an Kunden oder Interessenten gerichtet werden sollen, in Form von Direktwerbung, ist mithin eine Interessenabwägung im Einzelfall vorzunehmen, wobei das Interesse des Unternehmens an der Werbung regelmäßig überwiegt, da dieses rechtlich anerkannt ist. Da dies jedoch nicht immer der Fall sein muss, sollte vor Durchführung solcher Maßnahmen, in der jeweiligen Planungsphase, die Abteilung KDI frühzeitig miteinbezogen werden (E-Mail: datenschutz_sicherheit@vhv.de). Auch die Ausgestaltung der Betroffenenrechte (vgl. Kapitel 3) ist bei Werbemaßnahmen regelmäßig von großer Wichtigkeit und mit der Abteilung Konzerndatenschutz abzustimmen.

Beispiele für Datenverarbeitung aufgrund von berechtigten Interessen: Der betroffene VN oder Interessent soll mit Werbung auf vergleichbare Produkte angesprochen werden; der Betrieb des HIS, der AVAD oder anderer Auskunfteien; Datenverarbeitungen im Inkassowesen; Datenverarbeitungen zur Verhinderung von Betrugsstraftaten, zentrale Nutzung von Stammdaten im Konzern etc.

2.1.4 Verarbeitung aufgrund rechtlicher Verpflichtungen

Die Verarbeitung von personenbezogenen Daten ist zudem gestattet, wenn die VHV Gruppe aufgrund einer gesetzlichen Regelung zur Datenverarbeitung verpflichtet ist.

Beispiele: Verarbeitung für steuerliche Zwecke (Aufbewahrungsfristen nach § 147 AO); Einhaltung der Vorschriften aus dem Geldwäschegesetz bei der Identifizierung von Kunden in der Lebensversicherung; Verarbeitungen basierend auf Tarif- und Betriebsvereinbarungen (§ 4 Abs. 1 TVG und § 77 Abs. 4 BetrVG); Meldepflichten gegenüber Behörden; etc.

Bei Unklarheiten, z. B. ob bei einem Vorgang eine rechtliche Pflicht zur Übermittlung besteht, z. B. gegenüber anfragenden Behörden, wenden Sie sich bitte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de).

2.1.5 Verarbeitung besonderer Kategorien von personenbezogenen Daten

Die Unternehmen der VHV Gruppe gewährleisten, dass besondere Kategorien von personenbezogenen Daten nur nach Maßgabe des Art. 9 Abs. 2 DSGVO verarbeitet werden.

Hiernach ist eine Verarbeitung u. a. zulässig, sofern diese:

- Auf einer ausdrücklichen für einen oder mehrere Zwecke gegebenen Einwilligung beruht (siehe auch 2.1.1.2 „Einwilligung bei Gesundheitsdaten“)
- Die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich ist (siehe auch 2.1.1.2 „Einwilligung bei Gesundheitsdaten“).

Besondere Kategorien personenbezogener Daten: Angaben zur rassischen und ethnischen Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten, Daten zum Sexualleben oder der sexuellen Orientierung.

2.1.6 Automatisierte Entscheidung im Einzelfall und Profiling

Die automatisierte Entscheidung im Einzelfall und das Profiling sind, sofern sie rechtliche Wirkung gegenüber der betroffenen Person entfalten oder die Person erheblich beeinträchtigen, nur zulässig, wenn:

- die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Unternehmen der VHV Gruppe erforderlich ist,
- oder die Entscheidung mit ausdrücklicher Einwilligung der betroffenen Person erfolgt,
- oder die Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag erfolgt und
    - dem Begehren stattgegeben wurde
    - oder die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht und der Verantwortliche für den Fall, dass dem Antrag nicht vollumfänglich stattgegeben wird, angemessene Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens im Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird.

Beim Einsatz von negativen automatisierten Entscheidungen im Einzelfall wird gegenüber den betroffenen Personen (Versicherungsnehmern und Anspruchstellern) gewährleistet, dass

- sie das Eingreifen einer Person des Unternehmens der VHV Gruppe erwirken können,
- sie ihren Standpunkt darlegen und die Entscheidung anfechten können,
- ihnen mitgeteilt wird, dass eine automatisierte Entscheidung getroffen wurde. Dabei werden ihnen, sofern sie nicht bereits informiert wurden, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der automatisierten Entscheidungsfindung mitgeteilt.

Automatisierte Entscheidungen im Einzelfall bei denen besondere Kategorien personenbezogener Daten (z. B. Gesundheitsdaten) verarbeitet werden, sind nur zulässig, wenn angemessene und spezifische Maßnahmen zum Schutz der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Personen getroffen wurden. Auch sind automatisierte Entscheidungen im Einzelfall bei Verarbeitung von Gesundheitsdaten nur nach ausdrücklicher Einwilligung zulässig oder, ohne Einwilligung, bei Entscheidungen im Rahmen der Leistungserbringung.

Die Verarbeitungsverfahren, in denen automatisierte Entscheidungen im Einzelfall getroffen werden, sind entsprechend zu dokumentieren und mit den hierfür vorgesehen Maßnahmen zu versehen.

Beispiele: Automatisierte Annahmentscheidungen bei Antragstellung; automatisierte Regulierungsentscheidungen; automatisierte Risikoprüfungen (insbesondere im Bereich Lebensversicherung); automatisierte Entscheidung bei der Auswahl von Bewerbern; automatisierte Entscheidungen über die Erfüllung von Merkmalen bei verhaltensbezogenen Tarifen, z. B. das Fahrverhalten honorierende Rabatte in der KFZ-Versicherung.

Hinweis: In den jeweiligen Datenschutzhinweisen werden die betroffenen Personen in angemessenem Umfang über ihre Rechte nach automatisierten Entscheidungen im Einzelfall, die Rechtsgrundlage und die Verarbeitungszwecke informiert. Bei Rückfragen oder bei der Einführung neuer Verfahren zur automatisierten Entscheidung im Einzelfall und Profiling, wenden Sie sich bitte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de).

2.1.7 Scoring

Die Verarbeitung personenbezogener Daten zum Zweck einer Scorebildung (das meint die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person) ist nur unter bestimmten Bedingungen zulässig.

Dies sind insbesondere, seitens der Auskunfteien, dass die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind, dass für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt wurden und dass im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren. Auch müssen die grundsätzlichen Vorgaben des Datenschutzrechts eingehalten werden.

Für die Unternehmen, die diese Wahrscheinlichkeitswerte weiterverarbeiten wollen, gibt das Gesetz weitere Zulässigkeitsmerkmale vor, die eine Nutzung dieser Daten rechtfertigt. Insbesondere ist nach der Gesetzeslage das Verarbeiten von „harten Negativmerkmalen“ (bspw. Informationen über das Vorliegen von rechtskräftigen oder für vorläufig vollstreckbar erklärten Urteilen bzgl. der jeweiligen Forderung, Informationen über festgestellte Forderungen im Insolvenzverfahren, Informationen über ausdrücklich anerkannte Forderungen) ein gesetzlich anerkanntes berechtigtes Interesse der Unternehmen (vgl. Kapitel 2.1.3 „Verarbeitung aufgrund berechtigter Interessen“). Sollen künftig neue Scoring-Verfahren eingeführt werden sollte zur vorigen Prüfung die Abteilung KDI konsultiert werden (E-Mail: datenschutz_sicherheit@vhv.de).

Beispiel: Vor Vertragsschluss werden bei Beantragung einer KFZ-Versicherung die sog. „harten Negativmerkmale“ des VN, auf Basis der Ergebnisse einer Auskunftei, abgefragt und geprüft.

2.1.8 Datenverarbeitung zu statistischen Zwecken

Sofern die Fachbereiche personenbezogene Daten für statistische Zwecke benötigen, ist das Formular zur Datenanforderung personenbezogener Daten zu befüllen.

Die Formulare finden Sie im WorkNet. Sie werden zudem in den relevanten Abteilungen (z. B. TSK oder in den Steuerungseinheiten der Gesellschaften) vorgehalten.

Die Versicherungswirtschaft errechnet auf der Basis von Statistiken und Erfahrungswerten mit Hilfe versicherungsmathematischer Methoden die Wahrscheinlichkeit des Eintritts von Versicherungsfällen sowie deren Schadenhöhe und entwickelt auf dieser Grundlage Tarife. Dazu werten Unternehmen neben Daten aus Versicherungsverhältnissen, Leistungs- und Schadenfällen auch andere Daten von Dritten (z. B. des Kraftfahrtbundesamtes) aus. Zur Ermittlung der risikogerechten Prämie werden solche Tarife auf die individuelle Situation des Antragstellers angewandt. Darüber hinaus kann eine Bewertung des individuellen Risikos des Antragstellers durch spezialisierte Risikoprüfer, z. B. Ärzte, in die Prämienermittlung einfließen. Hierzu werden auch personenbezogene Daten einschließlich ggf. besondere Kategorien personenbezogener Daten, wie Gesundheitsdaten, verwendet, die nach den gesetzlichen Vorgaben verarbeitet worden sind.

Grundsätzlich gilt, dass im Rahmen einer Statistik verwendete personenbezogene Daten zu anonymisieren oder zumindest zu pseudonymisieren sind, sobald dies nach dem Statistikzweck möglich ist. Merkmale mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können, sind gesondert zu speichern. Daneben greifen die allgemeinen Grundsätze der Datensparsamkeit (Beschränkung auf das notwendige Minimum, Datenlöschung nach Erfüllung des Auswertungszwecks etc.).

Für Datenverarbeitungen zu statistischen Zwecken können auch besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, verarbeitet werden, wenn dies für den jeweiligen Statistikzweck erforderlich ist und die Interessen der VHV Gesellschaft an der Verarbeitung die Interessen der betroffenen Personen an einem Ausschluss von der Verarbeitung erheblich überwiegen. Das gilt in der Regel z. B. für Statistiken zur Entwicklung und Überprüfung von Tarifen oder zum gesetzlich vorgeschriebenen Risikomanagement. Bei diesen Vorgängen ist mithin auch keine vorige Einwilligung in die Verarbeitung nötig, sofern die gesetzlichen Vorgaben eingehalten werden.

2.1.9 Verarbeitung von Mitarbeiterdaten

Die Verarbeitung von personenbezogenen Daten von Mitarbeitern erfolgt auf Basis von Art. 88 DSGVO und § 26 BDSG. Sofern es sich um Personalangelegenheiten handelt, werden die Daten nur in der Personalabteilung verarbeitet und aufbewahrt. Eine doppelte Aufbewahrung der Personalakte im Fachbereich ist unzulässig.

Beispiele: Verarbeitung der Daten zur Begründung, Durchführung oder Abwicklung des Beschäftigungsverhältnisses, angemessene Fragen zu gesundheitlichen Beeinträchtigungen, die die Erfüllung des Arbeitsverhältnisses über das normale Maß hinaus beeinträchtigen im Rahmen des Einstellungsgesprächs; Nutzung der Mitarbeiterdaten für Regelbeurteilungen, Ablage des Arbeitsvertrages des Mitarbeiters außerhalb der Personalakte; Gesprächsaufzeichnungen zur Qualitätskontrolle nach Einwilligung oder Interessenabwägung im Einzelfall; Stichprobenkontrolle des dienstlichen E-Mail-Verkehrs; präventive Videoüberwachung an bestimmten, besonders sicherheitsrelevanten Orten auf dem Unternehmensgelände; konzerninterner Personaldatenfluss zwischen den Einzelgesellschaften etc.

Bei der Verarbeitung von Mitarbeiterdaten sind auch stets die geltenden Betriebsvereinbarungen zu beachten.

2.1.10 Datenübermittlung in Drittländer

Eine Datenübermittlung in Drittländer ist zulässig, wenn im Drittland als Zielland ein angemessenes Datenschutzniveau herrscht. Die Unternehmen der VHV Gruppe übermitteln personenbezogene Daten nur in Drittländer sofern, das angemessene Datenschutzniveau:

- festgestellt ist durch einen Angemessenheitsbeschluss der Europäischen Kommission,
- hergestellt wird durch verbindliche interne Datenschutzvorschriften,
- hergestellt wird durch Standarddatenschutzklauseln,
- hergestellt wird durch genehmigte Verhaltensregeln,
- hergestellt wird durch einen genehmigten Zertifizierungsmechanismus,
- hergestellt wird durch sonstige Maßnahmen.

Drittländer sind solche Staaten außerhalb der EU/des EWR.

Ein angemessenes Schutzniveau besteht momentan in folgenden Drittstaaten: Andorra, Argentinien, Kanada (nur kommerzielle Organisationen), Färöer, Guernsey, Israel, Isle of Man, Jersey, Neuseeland, Schweiz, Uruguay und Japan). Ferner gilt das Vereinigte Königreich Großbritannien (UK) aufgrund des am 28.06.2021 verabschiedeten Angemessenheitsbeschluss bis zum 27.07.2025 als Drittland mit einem angemessenen datenschutzrechtlichen Niveau. Aufgrund der Bestrebungen die UK-Datenschutzgesetze zukünftig stärker von der DSGVO abweichen zu lassen beabsichtigt die EU-Kommission dieses eng zu verfolgen.

In diese ist die Datenübermittlung daher ausdrücklich gestattet.

Durch die Entscheidung „Schrems II“ (C-311/18) des europäischen Gerichtshofes kann der Datentransfer in die USA nicht mehr auf das Privacy Shield gestützt werden.

Übermittlungen personenbezogener Daten in Drittländer sind nur dann zulässig, wenn diese ein Datenschutzniveau aufweisen, das den europäischen Grundrechten der Sache nach gleichwertig ist. Da dies nach den Feststellungen des höchsten europäischen Gerichts in den USA weitgehend nicht der Fall ist, erklärt der EuGH in seiner Entscheidung das „EU-US Privacy Shield“ für ungültig, auf dessen Grundlage eine Übermittlung personenbezogener Daten in die USA bisher in vielen Fällen erfolgte.

Die sogenannten Standardvertragsklauseln, die europäische Unternehmen mit Anbietern in Drittländern abschließen können, um das europäische Datenschutzniveau auch in den Drittländern zu wahren, erklärt der EuGH dagegen unter bestimmten Bedingungen für grundsätzlich zulässig.

In die Beurteilung sind die Umstände der Übertragung und ggf. weitere mögliche Schutzmaßnahmen mit einzubeziehen. Die zusätzlichen Schutzmaßnahmen müssen ein den Umständen angemessenes Schutzniveau garantieren und dürfen durch das US-Recht nicht unterminiert werden.

Vor der Frage nach der Zulässigkeit der Übermittlung in den jeweiligen Drittstaat (und mithin des angemessenen Schutzniveaus) muss auf erster Stufe sichergestellt werden, dass die Übermittlung an sich zulässig ist. Dies meint die Prüfung, ob die zu übermittelnden bspw. Adress- und Identifizierungsdaten überhaupt durch eine Rechtsgrundlage (vgl. Kapitel 2.1.1 bis 2.1.9, sowie 0) auf zulässige Weise übermittelt werden können. Wenn dies bejaht wird, folgt die Prüfung und die Frage, ob der Drittstaat ein angemessenes Schutzniveau hat.

Wenn Sie im Rahmen eines Projekts, eines Auftrags oder eines anderen Vorgangs die Datenübermittlung in ein Drittland anstreben, wenden Sie sich bitte frühzeitig an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de).

Beispiel: Die VHV mietet zur Datenspeicherung einen Cloud-Storage bei einem amerikanischen Unternehmen an. Die Server werden in den USA betrieben. Um die Datenübermittlung im Ausland zu legalisieren, schließt die VHV mit dem amerikanischen Unternehmen EU-Standardvertragsklauseln ab, in denen die Modalitäten der Datenverarbeitung geregelt werden.

2.1.11 Datenübermittlung an Dienstleister und Verarbeitung durch Dienstleister

Für einige Geschäftsprozesse ist es notwendig, Dienstleister einzusetzen und diesen für die Erledigung des Auftrags personenbezogene Daten zu übermitteln bzw. Zugriff auf bei uns liegende Daten zu ermöglichen. Ein Dienstleister kann im Rahmen einer sog. „Auftragsverarbeitung“ oder im Rahmen einer „Funktionsübertragung“ für uns tätig werden.

2.1.11.1 Auftragsverarbeitung

Bei einer Verarbeitung im Auftrag wird ein Dienstleister mit der Durchführung der Datenverarbeitung beauftragt, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird (sog. „Auftragsverarbeiter“). Er unterliegt vielmehr den Weisungen (welche zu dokumentieren sind) des Auftraggebers. Ein Auftragsverarbeiter ist mithin eine natürliche oder juristische Person, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des verantwortlichen Unternehmens verarbeitet. Im Falle einer Weitergabe personenbezogener Daten im Rahmen einer Verarbeitung im Auftrag bleibt der Auftraggeber die für die Verarbeitung verantwortliche Stelle (sog. „Verantwortlicher“).

Beispiele: Telefondienstleistungen (Call Center Tätigkeit); Druckdienstleistungen; automatisierte Rechnungsprüfung mit festem, von uns vorgegebenem Regelwerk; IT-Dienstleistungen wie Hosting- und Fernwartungstätigkeiten; Scannen und Zuordnung von Eingangspost; Entsorgung von Dokumenten; externe Sicherstellung der korrekten Verbuchung von Zahlungseingängen; externe Antrags- und Vertragsbearbeitung und externe Schaden- und Leistungsbearbeitung

Vor der Auftragserteilung sind folgende Maßgaben zu befolgen:

- Bei der Auswahl des Auftragnehmers ist sicherzustellen, dass dieser die für die Verarbeitung notwendigen technischen und organisatorischen Anforderungen und Sicherheitsmaßnahmen gewährleisten kann. Hierzu muss der Dienstleister vor der Beauftragung überprüft werden und hinreichende Garantien bieten.
- Die Durchführung der Auftragsdatenverarbeitung sollte grundsätzlich in einem schriftlichen Vertrag geregelt werden, in dem die Anforderungen zum Datenschutz und zur Informationssicherheit vereinbart sind. Insbesondere muss festgelegt werden, dass der Auftragnehmer die Daten ausschließlich nach den Weisungen des Auftraggebers verarbeiten darf.

Notwendige und per Gesetz vorgeschriebene Inhalte gemäß Art. 28 DSGVO sind bspw.: Festlegung von Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen.

Diese notwendigen Vertragsinhalte sind in unseren Vertragsmustern, welche im WorkNet abrufbar sind, bereits eingearbeitet. Unsere Vertragsmuster sind mit unserer zuständigen Datenschutzaufsichtsbehörde abgestimmt.

Vorsorglich sollten sich die zuständigen Mitarbeiter folgende Fragen stellen:

- Liegen mit allen Auftragsverarbeitern schriftliche Verträge entsprechend dem Muster von KDI vor?
- Sind die Vereinbarungen unterschrieben und auf die nutzende/verantwortliche Gesellschaft geschlossen?
- Ist sichergestellt, dass den Auftragsverarbeitern schriftliche Weisungen zum Umgang mit den Daten erteilt werden?
- Werden die AV-Verträge regelmäßig überwacht?
- Wird der AV-Dienstleister nach Beendigung des Auftrags/spätestens nach Vertragsbeendigung schriftlich um Löschung der Daten ersucht bzw. werden die vereinbarten Löschfristen überwacht und der Dienstleister um Bestätigung ersucht?
- Wurden die Sicherheitskonzepte des Dienstleisters bei der Beauftragung überprüft?

- Finden Vor-Ort-Kontrollen statt?
- Werden vereinbarte Auflagen nachgehalten?
- Werden sicherheitsrelevante Vorfälle, die der Dienstleister meldet, unverzüglich an KDI bzw. das Postfach sicherheitsvorfall@vhv.de weitergeleitet?

Wichtig für die Praxis: Bei der Beauftragung von Dienstleistern sind grundsätzlich die jeweils für die Beschaffung der Dienstleistung relevanten Prozesse zu berücksichtigen (z. B. Einkaufsprozess, Softwarebeschaffungsprozess). Im Rahmen dieser Prozesse wird KDI regelmäßig eingebunden.

Grundsätzlich ist bei der Verwendung der Musterverträge folgendes zu beachten: Es ist seitens des jeweiligen Fachbereichs notwendig zu überprüfen, welches Muster auf die vorliegende Konstellation anwendbar ist.

Bitte prüfen Sie dazu, ob der Vertrag, auf den sich die Datenverarbeitung bezieht, vom Risikoverantwortlichen oder von der VHV Holding AG geschlossen worden ist. Sollte der Haupt-/Rahmenvertrag von der VHV Holding AG geschlossen worden sein, so verwenden Sie bitte das Muster „VHV Vertrag Auftragsverarbeitung DSGVO Holding“. Andernfalls nutzen Sie bitte das Muster „VHV Vertrag Auftragsverarbeitung DSGVO“.

Ungeachtet dessen, welches Muster für die ADV verwendet werden muss, muss der Auftragnehmer die ebenfalls im WorkNet erhältliche Datenschutz-Selbstauskunft („VHV TOM Selbstauskunft“) hinsichtlich der technisch-organisatorischen Maßnahmen ausfüllen. Bitte leiten Sie die ausgefüllte Selbstauskunft an das Postfach datenschutz_sicherheit@vhv.de weiter.

Der Vertrag zur Auftragsverarbeitung ist vom Fachbereich schon möglichst ausführlich vorzubefüllen, sodass eine Einigung mit den Dienstleistern zeitnah und reibungslos verlaufen kann. Gerne berät Sie die Abteilung KDI auch bei der Erstellung des Entwurfs.

Nach Prüfung des Dokuments seitens KDI wird der Entwurf vom Fachbereich an den Auftragsverarbeiter (Dienstleister) verschickt.

Bei jedweden vertraglichen Verhandlungen und Änderungen ist KDI miteinzubeziehen.

Der Besteller trägt dafür Sorge, dass die Vereinbarung und die Selbstauskunft von beiden Seiten unterschrieben und sodann ordnungsgemäß (im Einkauf) archiviert werden. Eine Kopie/ein Scan der Vertragsdokumente ist der Abteilung KDI zur Verfügung zu stellen.

2.1.11.2 Datenverarbeitung durch Dienstleister ohne Auftragsverarbeitung

Bei der Datenverarbeitung durch Dienstleister ohne Auftragsverarbeitung (ehemals „Funktionsübertragung“) erhalten Dienstleister des Verantwortlichen personenbezogene Daten zur eigenverantwortlichen Aufgabenerfüllung. In der Eigenverantwortlichkeit liegt der wesentliche Unterschied zur weisungsgebundenen Auftragsverarbeitung. Die Funktionsübertragung ist nach dem Code of Conduct insbesondere im folgenden Fall möglich:

Ein Dienstleister kann personenbezogene Daten zur eigenverantwortlichen Aufgabenerfüllung erhalten, soweit dies für die Zweckbestimmung des Versicherungsverhältnisses mit dem Betroffenen erforderlich ist.

Beispiele: Sachverständiger wird mit der Begutachtung eines Versicherungsfalles beauftragt; Abschleppunternehmen erbringt vertraglich vereinbarte Versicherungsleistungen (Schutzbrief); Krankentransportdienstleister, Haushaltshilfen, Schlüsseldienste etc., die vertraglich vereinbarte Versicherungsleistungen (in Form von Sachleistungen) erbringen.

Gemeint sind also Fälle, in denen die Datenübermittlung zwingend erforderlich ist, um die vertraglich vereinbarten Leistungen gegenüber dem Versicherungsnehmer erbringen zu können.

Davon unberührt bleiben Übermittlungen von personenbezogenen Daten an Rechtsanwälte, Steuerberater und Wirtschaftsprüfer im Rahmen von deren Aufgabenerfüllungen.

Besondere Kategorien personenbezogener Daten, insbesondere Gesundheitsdaten, dürfen in diesem Rahmen nur verarbeitet werden, wenn die betroffenen Personen eingewilligt haben oder eine gesetzliche Grundlage vorliegt (vgl. Kapitel 0 und 2.1.5). Soweit die jeweilige VHV Gesellschaft einer Verschwiegenheitspflicht gemäß § 203 StGB unterliegt, muss sie die eingesetzten Dienstleister hinsichtlich der Daten, die sie nach den Grundsätzen der Funktionsübertragung erhalten, Verschwiegenheit zu wahren und weitere Dienstleister sowie Stellen, die für sie tätig sind, zur Verschwiegenheit zu verpflichten.

Wichtig für die Praxis: Bei der Beauftragung von Dienstleistern sind grundsätzlich die jeweils für die Beschaffung der Dienstleistung relevanten Prozesse zu berücksichtigen (Einkaufsprozess). Bei Rückfragen ist die Abteilung KDI via datenschutz_sicherheit@vhv.de einzubeziehen.

2.1.12 Sonderfälle nach dem Code of Conduct

Im Rahmen des Code of Conduct wurden weitere zulässige Fälle von Datenverarbeitungen sowie deren Voraussetzungen beschrieben. Es handelt sich um typische Geschäftsvorfälle im Versicherungsgeschäft:

2.1.12.1 Datenaustausch mit anderen Versicherern

In manchen Fällen müssen Daten mit anderen Versicherern ausgetauscht werden. So kann es sein, dass ein Kunde die Versicherung wechselt und der nachfolgende Versicherer Angaben von uns in unserer Rolle als Vorversicherer benötigt.

Eine Datenübermittlung ist in diesem Fall zulässig, wenn

1. bei der Risikoeinschätzung zur Überprüfung von Schadenfreiheitsrabatten, insbesondere der Schadensfreiheitsklassen in der KFZ-Haftpflichtversicherung und Vollkaskoversicherung,
2. zur Übertragung von Ansprüchen auf Altersvorsorge bei Anbieter- oder Arbeitgeberwechsel,
3. zur Übertragung von Altersrückstellungen in der Krankenversicherung auf den neuen Versicherer,
4. zur Ergänzung oder Verifizierung der Angaben der Antragsteller oder Versicherten.

In den Fällen der Nummern 1 und 4 ist der Datenaustausch zum Zweck der Risikoprüfung nur zulässig, wenn die betroffenen Personen bei Datenerhebung im Antrag über den möglichen Datenaustausch und dessen Zweck und Gegenstand informiert werden. Nach einem Datenaustausch zum Zweck der Leistungsprüfung werden die betroffenen Personen vom Daten erhebenden Unternehmen über einen erfolgten Datenaustausch im gleichen Umfang informiert (vgl. Kapitel 2.3).

Außerhalb des Verhältnisses Vor-/Nachversicherer ist ein Datenaustausch mit anderen Versicherern zulässig, soweit dies

1. zur Bearbeitung gemeinsamer, mehrfacher oder kombinierter Risiken erforderlich ist,
2. ein gesetzlicher Forderungsübergang stattgefunden hat,
3. ein Teilungs- oder Regressverzichtsabkommen zwischen den Unternehmen besteht
4. und für diese Fälle kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse der betroffenen Person dem entgegensteht.

Des Weiteren ist ein Datenaustausch im Rahmen des HIS zulässig unter Beachtung des Leitfadens des GDV und der Vorgaben in der Arbeitsrichtlinie „HIS“. Diese ist im WorkNet abrufbar.

Wichtig für die Praxis: Der Datenaustausch zwischen den VU ist stets zu dokumentieren. Bei Fragen hinsichtlich der Zulässigkeit der Übermittlung ist die Abteilung KDI hinzuzuziehen (E-Mail: datenschutz_sicherheit@vhv.de).

2.1.12.2 Datenübermittlung an Rückversicherer

Nach dem Code of Conduct sind Datenübermittlungen an Rückversicherer zulässig. Allerdings ist hierbei zu beachten, dass ein Rückversicherer grundsätzlich nur anonymisierte oder pseudonymisierte Daten erhalten darf, die keinen Rückschluss auf eine bestimmte Person zulassen. Denn in der Regel benötigt der Rückversicherer für seine Tätigkeit auch keine Daten mit Personenbezug.

Eine Übermittlung von personenbezogenen Daten an Rückversicherer ist ausnahmsweise dann zulässig, wenn dies

- für den Abschluss oder die Erfüllung des Versicherungsvertrages erforderlich ist oder
- zur Sicherstellung der Erfüllbarkeit der Verpflichtungen des Unternehmens aus den Versicherungsverhältnissen erfolgt und kein Grund zu der Annahme besteht, dass ein überwiegendes schutzwürdiges Interesse der betroffenen Person dem Unternehmensinteresse entgegensteht.

Dies kann der Fall sein, wenn im Rahmen des konkreten Rückversicherungsverhältnisses die Übermittlung personenbezogener Daten an Rückversicherer aus folgenden Gründen erfolgt:

- Die Rückversicherer führen z. B. bei hohen Vertragssummen oder bei einem schwer einzustufenden Risiko im Einzelfall die Risikoprüfung und die Leistungsprüfung durch,
- die Rückversicherer unterstützen die Unternehmen bei der Risiko- und Schadenbeurteilung sowie bei der Bewertung von Verfahrensabläufen,
- die Rückversicherer erhalten zur Bestimmung des Umfangs der Rückversicherungsverträge einschließlich der Prüfung, ob und in welcher Höhe sie an ein und demselben Risiko beteiligt sind (Kumulkontrolle) sowie zu Abrechnungszwecken Listen über den Bestand der unter die Rückversicherung fallenden Verträge,
- die Risiko- und Leistungsprüfung durch den Erstversicherer wird von den Rückversicherern stichprobenartig oder in Einzelfällen kontrolliert zur Prüfung ihrer Leistungspflicht gegenüber dem Erstversicherer.

Für Fragen zu der datenschutzrechtlichen Ausgestaltung der Verträge wenden Sie sich bitte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de).

2.1.12.3 Tarifkalkulationen

Tarifkalkulationen sind nur mit anonymisierten – oder zumindest pseudonymisierten – Daten erlaubt. Dies gilt auch dann, wenn Dienstleister oder Verbände mit der Erstellung unternehmensübergreifender Statistiken oder zur Tarifkalkulation eingesetzt werden (vgl. Kapitel 2.1.8).

2.1.12.4 Verarbeitung von Stammdaten in der Unternehmensgruppe

Zum Zwecke der zentralisierten Bearbeitung von bestimmten Verfahrensabschnitten und Geschäftsabläufen (z. B. Telefonate, Post, Inkasso) ist es zulässig, dass in der Unternehmensgruppe die Stammdaten von Antragstellern, Versicherten und weiteren Personen zentralisiert verarbeitet werden. Die Einsicht in weitergehende Vertragsinhalte ist allerdings den jeweiligen Konzerngesellschaften und den dort tätigen Personen vorbehalten, es sei denn, eine Konzerngesellschaft wird im Auftrag einer anderen Konzerngesellschaft tätig. So ist z. B. die VHV solutions GmbH im Auftrag der übrigen Konzerngesellschaften tätig, so dass die dort tätigen Mitarbeiter auch weitere, als die Stammdaten der Betroffenen einsehen und verarbeiten dürfen.

2.2 Zweckbindung und Nichtverkettbarkeit

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

Das bedeutet, dass bei der Verarbeitung der personenbezogenen Daten der Zweck dieser Verarbeitung im Vorfeld festgelegt werden muss. So muss bereits bei der Erhebung personenbezogener Daten die betroffene Person darüber informiert werden, wofür die Daten verwendet werden sollen. Grob beschreibende Formulierungen genügen insoweit nicht, sondern bedürfen der Konkretisierung. In den Datenschutzhinweisen (diese werden grundsätzlich bspw. bei Vertragsschluss dem Betroffenen mitgeteilt, vgl. Kapitel 2.3) der VHV Gruppe werden die relevanten Zwecke auf angemessene Weise konkretisiert dargestellt.

Beispiel 1: Die Daten werden zum Zweck der Beschäftigung von Mitarbeitern erhoben, sie dürfen nicht ohne gültige Rechtsgrundlage für Zwecke des Adresshandels an Dritte übermittelt werden.

Beispiel 2: Die Daten eines VN werden zum Zweck der KFZ-Tarifierung erhoben, sie dürfen nicht zum Zweck des Vertriebs einer Lebensversicherung verarbeitet werden.

Nichtverkettbarkeit meint die (technische) Sicherstellung der Zweckbindung und deren Nachweisbarkeit. Sie bezeichnet die technische Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden, für den sie erhoben wurden. Dies soll verhindern, dass die Daten für weitere Zwecke eingesetzt werden und mit anderen, unter Umständen öffentlich zugänglichen Daten kombiniert werden. Daraus folgt weiterhin, dass eine Verarbeitung nach Zwecken getrennt ermöglicht werden muss (sog. „Funktionstrennung“) bzw. dass die Daten je nach Verarbeitungszweck voneinander getrennt gespeichert werden (sog. „Datentrennung“). So muss bspw. der Datenbestand ggfs. durch Duplizierung und Reduzierung auf den für den neuen Zweck erforderlichen Umfang angepasst werden.

2.3 Transparenz und Informationspflichten

Die VHV Gruppe verarbeitet personenbezogene Daten nach dem Grundsatz der Transparenz. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung von personenbezogenen Daten leicht zugänglich, verständlich und in klarer einfacher Sprache verfasst sind. Der Betroffene soll dadurch die Möglichkeit haben den Verarbeitungszyklus nachvollziehen zu können.

Diese Informationen müssen bei allen relevanten Verfahren, in denen Daten erhoben werden, erteilt werden, z. B. im Antragsprozess, im Bewerberprozess, in den Vertriebsprozessen etc.

2.3.1 Informationspflicht: Datenerhebung beim Betroffenen

Werden Daten beim Betroffenen selbst erhoben, ist er zum Zeitpunkt der Datenerhebung über folgendes zu informieren:

- den Namen und die Kontaktdaten des Verantwortlichen (jeweiliges Unternehmen der VHV Gruppe) sowie gegebenenfalls seines Vertreters;
- die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- wenn die Verarbeitung aufgrund berechtigter Interessen erfolgt, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und

- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Art. 46, Art. 47 oder Art. 49 Abs. 1 Unterabschnitt 2 DSGVO einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung oder eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche möglichen Folgen die Nichtbereitstellung hätte und
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Ausnahme: Eine Information kann insbesondere unterbleiben, wenn der Betroffene bereits über die notwendigen Informationen verfügt. Dies meint insbesondere, dass der jeweilige Betroffene nur einmal informiert werden muss.

Ob im Einzelfall eine Ausnahme vorliegt ist nach Maßgabe des Art. 13 Abs. 4 DSGVO und des § 32 Abs. 1 BDSG zu entscheiden. Für die Unterstützung bei einer solchen Entscheidung wenden Sie sich bitte an die Abteilung KDI (datenschutz_sicherheit@vhv.de).

Die notwendigen Dokumente und Prozessschritte sind bereits in Absprache mit KDI implementiert worden. Nähere Informationen finden Sie in den jeweiligen WorkNet-Dokumenten der Gesellschaften/Sparten (bspw. „Datenschutz-Hinweise im Angebotsprozess“) bzw. in den Druckstücken. Zudem wird auf die Datenschutzschulung zur DSGVO, die Sie in Ihrem Portal finden, verwiesen.

Bei Rückfragen zu den Informations- und Hinweispflichten ist die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de) einzubinden.

Kontrollfragen für die Praxis:

- Ist sichergestellt, die Betroffenen (Interessenten, Versicherungsnehmer, Sachverständigen, Vermittler, Geschädigten etc.) im Rahmen der erstmaligen Datenerhebung über die vorgenannten Informationen informiert werden und ist dies entsprechend dokumentiert?
- Enthalten die Hinweise eine aktuelle Liste der eingesetzten Dienstleister?

2.3.2 Informationspflichten bei indirekter Datenerhebung

Die VHV Gruppe erhebt in bestimmten Fällen bei Dritten personenbezogene Daten von betroffenen Personen. Zur Einhaltung der Transparenzpflicht ist daher zu gewährleisten, dass die betroffenen Personen vom jeweils Verantwortlichen über die Verarbeitung der personenbezogenen Daten informiert werden. Dies beinhaltet:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- zusätzlich die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;
- die Kategorien personenbezogener Daten, die verarbeitet werden;
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten;
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln.

Folgende Informationen sind zusätzlich zur Verfügung zu stellen, wenn sie erforderlich sind, um eine faire und transparente Verarbeitung zu gewährleisten:

- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
- wenn die Verarbeitung auf berechtigten Interessen beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden;
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten sowie auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung und eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
- wenn die Verarbeitung auf Art. 6 Abs. 1 lit. a oder Art. 9 Abs. 2 lit. a DSGVO beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird;
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- aus welcher Quelle die personenbezogenen Daten stammen und gegebenenfalls ob sie aus öffentlich zugänglichen Quellen stammen;
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

Im Unterschied zu Artikel 13 muss also bei Artikel 14 DSGVO zusätzlich über die Datenquelle und die verarbeiteten Datenkategorien informiert werden. Die Datenquelle muss dabei so genau wie möglich, zumindest jedoch in Kategorien benannt werden.

Von der Informationspflicht sind Ausnahmen möglich:

- Eine Information kann unterbleiben, wenn der Betroffene bereits über die notwendigen Informationen verfügt. Dies meint insbesondere, dass der jeweilige Betroffene nur einmal informiert werden muss.
- Die Information einen unverhältnismäßigen Aufwand für die jeweilige Einzelgesellschaft bedeuten würde. Dies meint bspw. den Fall, dass zu einer Person nur Name und Vorname bekannt ist. Hier müsste nicht zur bloßen Erfüllung der Informationspflicht eine Einwohnermeldeamt-Anfrage, Adressrecherche, oder ähnliches angestrengt werden, um die Adresse der Person zu ermitteln. Dies wäre ein unverhältnismäßiger Aufwand.

Ob im Einzelfall eine Ausnahme vorliegt ist nach Maßgabe des Art. 14 Abs. 5 DSGVO und des § 33 Abs. 1 Nr. 2 BDSG zu entscheiden. Für die Unterstützung bei einer solchen Entscheidung wenden Sie sich bitte an die Abteilung KDI (datenschutz_sicherheit@vhv.de).

Beispiel: Erhebung von Daten aus öffentlichen Quellen oder Verzeichnissen, z. B. zum Zwecke der Werbung oder der Kontaktaufnahme; Datenerhebung von Zeugen, Bezugsberechtigten, Mitversicherten, abweichenden Kontoinhabern etc.

2.4 Treu und Glauben

Die VHV Gruppe verarbeitet personenbezogene Daten nach dem Grundsatz von Treu und Glauben. Der Grundsatz „Treu und Glauben“ soll gemeinsam mit dem Transparenzgrundsatz sicherstellen, dass der Betroffene eine Vorstellung davon bekommt, wer seine Daten verarbeitet, für welche Zwecke die Daten verarbeitet und durch wen diese verarbeitet werden. Dieses wird insbesondere durch die zu berücksichtigenden Informationspflichten erreicht, welche unter 2.3 „Transparenz und Informationspflichten“ erläutert werden.

2.5 Datenminimierung und Speicherbegrenzung

Die Unternehmen der VHV Gruppe verarbeiten personenbezogene Daten entsprechend des Prinzips der Datenminimierung. Die Verarbeitung und Erhebung von personenbezogenen Daten soll dabei auf den Umfang beschränkt sein, der zur Erfüllung des jeweiligen Zweckes erforderlich ist. Damit einher geht der Grundsatz der Speicherbegrenzung, wonach Daten nur solange gespeichert werden dürfen, wie dies zur Erfüllung des jeweiligen Speicherzwecks erforderlich ist.

Zur Erreichung dieser Grundsätze werden bei der Verarbeitung von personenbezogenen Daten folgende Maßnahmen ergriffen:

- Reduzierung von erfassten Attributen der betroffenen Personen,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten,
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten,
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen,
- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren,
- Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren.

Hinweis für die Praxis: Die jeweiligen Informationseigentümer innerhalb der VHV Gruppe haben dafür Sorge zu tragen, dass für die Systeme, für die sie zuständig sind, Fristen zur Löschung und Sperrung der dort verarbeiteten personenbezogenen Daten definiert und umgesetzt werden. Dabei sind grundsätzlich auch etwaige gesetzliche Aufbewahrungsfristen zu beachten.

2.6 Richtigkeit der Datenverarbeitung

Die personenbezogenen Daten der VHV Gruppe müssen sachlich richtig und auf dem neuesten Stand gehalten werden. Zu diesem Zwecke etabliert die VHV Gruppe Maßnahmen, die eine fehlerhafte Zuordnung von personenbezogenen Daten ausschließen.

Der Grundsatz der Richtigkeit der Datenverarbeitung wird durch den Anspruch auf Berichtigung und Vervollständigung von unrichtigen bzw. unvollständigen Daten gemäß Art. 16 DSGVO gestützt (siehe Kapitel 3.2 „Berichtigung“).

Beispiel: Korrektur von unzutreffenden Daten, z. B. im Falle eines Umzugs, einer Heirat etc.

2.7 Vertraulichkeit, Verfügbarkeit und Integrität

Die VHV Gruppe gewährleistet die Vertraulichkeit und Verfügbarkeit von personenbezogenen Daten sowie deren Integrität.

Personenbezogene Daten sind vertraulich zu behandeln. Eine unbefugte Erhebung, Verarbeitung oder Nutzung dieser Daten ist untersagt. Insbesondere ist es untersagt, personenbezogene Daten für eigene private oder wirtschaftliche Zwecke zu nutzen, an Unbefugte zu übermitteln oder diesen auf andere Weise zugänglich zu machen.

Beschäftigte der VHV Gruppe, die regelmäßig personenbezogene Daten verarbeiten, werden bei Aufnahme der Tätigkeit von der Personalabteilung auf die datenschutzrechtliche Vertraulichkeit verpflichtet. Die Verpflichtung gilt über das Ende der Tätigkeit bei der VHV Gruppe hinaus fort, ebenso bei Wechseln innerhalb des Unternehmens.

Die VHV Gruppe gewährleistet durch technische und organisatorische Maßnahmen die Vertraulichkeit, Verfügbarkeit und Integrität der personenbezogenen Daten. Beispiele hierfür sind:

- Vertraulichkeit: Berechtigungskonzepte, Verschwiegenheitsvereinbarungen
- Verfügbarkeit: Einrichtung von Backupsystemen und Vertretungsregelungen
- Integrität: Festlegung von Zuständigkeiten, Datenpflegeprozesse (Richtigkeit der Verarbeitung)

Weitere Regelungen zur Vertraulichkeit, Verfügbarkeit und Integrität finden sich in der „Konzernrichtlinie Informationssicherheit“, die Sie im WorkNet abrufen können.

Beispiele von Sicherheitsmaßnahmen, die diese Grundsätze umsetzen: Einsatz von gängigen Authentifizierungsverfahren, Einsatz von aktuellen Verschlüsselungsmethoden, Vorliegen und Umsetzung von Berechtigungskonzepten entsprechend dem Need-to-Know-Grundsatz, Durchführung von Datensicherungen, Protokollierung von Änderungen an personenbezogenen Daten, Zugangskontrollen, Zutrittskontrollen, Pseudonymisierung von Daten etc.

2.8 Privacy by Default und Privacy by Design

Die Verfahren, Anwendungen und Prozesse der VHV Gruppe orientieren sich an den Grundsätzen Datenschutz durch Technikgestaltung (Privacy by Design) und Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default).

Hiermit ist gemeint, dass Datenschutz und Sicherheit bereits bei der Planung und Gestaltung von IT-Systemen, Softwareprodukten u. ä. Berücksichtigung finden muss. Hierzu wird insbesondere auf die Arbeitsrichtlinie „Sichere Softwareentwicklung“ im WorkNet verwiesen.

Beispielhafte Kontrollfragen für eine Umsetzung sind:

- Werden in der Softwareentwicklung Anonymisierungs- oder Pseudonymisierungsmöglichkeiten berücksichtigt?
- Sind Lösch- und Sperrmechanismen nebst entsprechender Regeln standardmäßig vorgesehen?
- Werden Verfahren der sicheren Authentisierung und Authentifizierung berücksichtigt?
- Werden die gängigen Standards der Softwareentwicklung (siehe Arbeitsrichtlinie sichere Softwareentwicklung) beachtet?
- Werden aktuelle Verschlüsselungstechnologien entsprechend den Arbeitsrichtlinien eingesetzt?
- Besteht für die Nutzer, z. B. bei Apps oder sonstigen Online-Diensten, die Möglichkeit, bestimmte Funktionen zu aktivieren bzw. zu deaktivieren?
- Kann der Kunde auf Websites selbst Einstellungen zur Privatsphäre vornehmen? Z. B. Cookies deaktivieren?
- Werden nur die Datenfelder, z. B. bei Anträgen oder Angeboten abgefragt, die zur Vertragsbearbeitung/Angebotsbearbeitung erforderlich sind? Sind freiwillige Angaben als solche gekennzeichnet?
- Besteht die Möglichkeit, Datenschutzrechte (Widerspruch etc.) ohne Hindernisse geltend zu machen?
- Werden Einwilligungen nur dann eingeholt, wenn diese wirklich erforderlich sind?
- Können Einwilligungen jederzeit, d. h. ohne Grund und ohne Hindernisse widerrufen werden?
- Sind Einwilligungen als solche gekennzeichnet und für den Betroffenen transparent?
- Sind die Datenschutzhinweise leicht zugänglich?

Der Datenschutz in der VHV Gruppe wird unter den Stichworten Privacy by Design und Privacy by Default, nach folgenden Prinzipien umgesetzt:

- Bereits bei der Planung von neuen Verarbeitungsverfahren muss proaktiv die Einhaltung der zuvor genannten Datenschutzgrundsätze berücksichtigt werden.
- Die für den Datenschutz notwendigen Maßnahmen sind Bestandteil der Architektur von Geschäftsprozessen und IT-Systemen.

3 Betroffenenrechte

Die VHV Gruppe muss sicherstellen, dass Betroffene, z. B. Versicherte, Antragsteller oder weitere Personen, deren personenbezogene Daten verarbeitet werden, ihre Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten ausüben können. Insoweit sieht die DSGVO eine Reihe von Betroffenenrechten vor.

3.1 Auskunftsrecht

Betroffene Personen haben das Recht zu erfahren, ob sie betreffende personenbezogene Daten verarbeitet werden und sie können Auskunft, über die beim Unternehmen über sie gespeicherten Daten verlangen.

In der VHV Gruppe wurden Prozesse etabliert und Dokumente erstellt, die dieser Voraussetzung gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Betroffenenrechte“ der Sparten bzw. Gesellschaften.

Grundsätzlich gilt: Für die Beantwortung von Auskunftsersuchen sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. Zur Unterstützung kann der Datenschutzexperte hinzugezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de) wenden.

3.2 Berichtigung

Die VHV Gruppe gewährleistet für die Betroffenen die Möglichkeit, sie betreffende unrichtige personenbezogene Daten zu berichtigen oder zu vervollständigen, sofern die Zwecke der Verarbeitung dies zulassen.

In der VHV Gruppe wurden Prozesse etabliert und Dokumente erstellt, die dieser Voraussetzung gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Betroffenenrechte“ der Sparten bzw. Gesellschaften.

Grundsätzlich gilt: Für die Berichtigung von Auskunftsersuchen sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. Zur Unterstützung kann der Datenschutzexperte hinzugezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de) wenden.

3.3 Recht auf Löschung / Recht auf Vergessenwerden

Das Recht auf Vergessenwerden soll sicherstellen, dass personenbezogene Daten nicht dauerhaft zur Verfügung stehen. Es begründet mithin eine Verpflichtung zur Datenlöschung für die verantwortliche Stelle. Damit korrespondierend steht dem Einzelnen gemäß Art. 17 Abs. 2 DSGVO ein Recht auf Löschung gegenüber der verantwortlichen Stelle zu, sofern:

- die personenbezogenen Daten für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind,
- die betroffene Person eine zuvor erteilte Einwilligung widerruft,
- die betroffene Person Widerspruch gegen die Verarbeitung einlegt (siehe unten),
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden oder die Verarbeitung von Anfang an unzulässig war,
- die Löschung aus einer anderen rechtlichen Verpflichtung nach Unionsrecht oder nationalem Recht erforderlich ist,
- personenbezogene Daten auf Basis des Art. 8 DSGVO erhoben wurden.

Eine Löschpflicht besteht nicht, soweit die Daten erforderlich sind:

- zur Erfüllung einer rechtlichen Verpflichtung der Einzelgesellschaft, insbesondere zur Erfüllung gesetzlicher Aufbewahrungspflichten,
- für die Verarbeitungen für statistische Zwecke,
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke (z. B. zur Aufarbeitung des Holocaust) oder
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

In der VHV Gruppe wurden Prozesse etabliert und Dokumente erstellt, die diesen Voraussetzungen gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Betroffenenrechte“ der Sparten bzw. Gesellschaften.

Grundsätzlich gilt: Für die Bearbeitung von Löschbegehren sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. In Zweifelsfällen kann der Datenschutzexperte zur Unterstützung herangezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (E-Mail: datenschutz_sicherheit@vhv.de) wenden.

3.4 Recht auf Einschränkung der Verarbeitung

Eine Einschränkung der Verarbeitung (Sperrung) kann ausnahmsweise vom Betroffenen verlangt werden, wenn

- die Richtigkeit der personenbezogenen Daten bestritten wird, für die Dauer der Überprüfung der Richtigkeit,
- die Verarbeitung unrechtmäßig ist und die betroffene Person statt Löschung die Einschränkung der Verarbeitung verlangt,
- die VHV Gruppe die Daten nicht mehr benötigt, die betroffene Person diese jedoch zur Geltendmachung, Ausübung und Verteidigung von Rechtsansprüchen benötigt,
- die betroffene Person Widerspruch gegen die Verarbeitung eingelegt hat und die berechtigten Gründe der VHV Gruppe überwiegen.

In der VHV Gruppe wurden Prozesse etabliert, die dieser Voraussetzung gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Betroffenenrechte“ der Sparten bzw. Gesellschaften.

Grundsätzlich gilt: Für die Bearbeitung von Anfragen zur Einschränkung der Verarbeitung sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. In Zweifelsfällen kann der Datenschutzexperte zur Unterstützung herangezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (E-Mail: daten-schutz_sicherheit@vhv.de) wenden.

3.5 Recht auf Datenübertragbarkeit

Die VHV Gruppe stellt betroffenen Personen auf Verlangen die sie betreffenden und durch sie bereit gestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung. Es wird zudem ermöglicht, die personenbezogen Daten direkt an andere Verantwortliche zu übertragen, sofern dies erwünscht ist.

In der VHV Gruppe wurden Prozesse etabliert und Dokumente erstellt, die dieser Voraussetzung gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Datenkopie und Datenportabilität“ der Sparten bzw. Gesellschaften. Bitte achten Sie darauf, dass der Betroffene im Fall der Datenkopie darauf hinzuweisen ist, dass er die Auskunft auch in einem anderen Format erhalten kann.

Grundsätzlich gilt: Für die Bearbeitung von Anfragen zur Einschränkung der Verarbeitung sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. In Zweifelsfällen kann der Datenschutzexperte zur Unterstützung herangezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (E-Mail: daten-schutz_sicherheit@vhv.de) wenden.

3.6 Widerspruchsrecht

Die betroffenen Personen können in bestimmten Konstellationen der Verarbeitung ihrer Daten widersprechen.

3.6.1 Widerspruch bei einwilligungsloser Verarbeitung zur Wahrung berechtigter Interessen

Erfolgt eine Datenverarbeitung durch den Verantwortlichen ohne Einwilligung, also insbesondere aufgrund der gesetzesmäßigen Wahrnehmung berechtigter Interessen, so steht dem Betroffenen fortan das Recht zu, dieser Verarbeitung zu widersprechen:

- Grundsätzlich ist einem Widerspruch nur stattzugeben, wenn dieser unter Darlegung persönlicher Versagungsgründe erfolgt, welche die berechtigten Interessen des Verantwortlichen überwiegen. Es erfolgt eine Interessenabwägung im Einzelfall.
- Wenn der Widerspruch rechtmäßig eingelegt wurde, dürfen die personenbezogenen Daten fortan nicht mehr verarbeitet werden.

3.6.2 Widerspruch bei Direktwerbung

Im Falle der Direktwerbung ist einem Widerspruch in die werbetechnische Datenverarbeitung auch ohne Angabe von Gründen und ohne Interessenabwägung stets unverzüglich Folge zu leisten, Art. 21 Abs. 2 und 3 DSGVO. Der Widerspruch erstreckt sich in diesem Falle auch auf sämtliche Maßnahmen zur Erstellung von Nutzerprofilen, die mit der Werbung in Zusammenhang stehen:

- die betroffene Person das Recht, jederzeit Widerspruch gegen die Verarbeitung sie betreffender personenbezogener Daten zum Zwecke derartiger Werbung einzulegen
- Widerspricht die betroffene Person der Verarbeitung für Zwecke der Direktwerbung, so werden die personenbezogenen Daten nicht mehr für diese Zwecke verarbeitet.

In der VHV Gruppe wurden Prozesse etabliert und Dokumente erstellt, die dieser Voraussetzung gerecht werden.

Hinweis für die Praxis: Die notwendigen Arbeits- und Prozessschritte finden Sie im WorkNet in den jeweiligen Arbeitsrichtlinien „Betroffenenrechte“ der Sparten. Dabei ist insbesondere zu beachten, dass Betroffene, die der Datenverarbeitung zu Werbezwecken widersprochen haben (sog. „Werbeverweigerer“) in die jeweiligen Negativ-Listen eingetragen werden.

Grundsätzlich gilt: Für die Bearbeitung von Widersprüchen sind in der Regel die für den Betroffenen zuständigen Fachbereiche verantwortlich. In Zweifelsfällen kann der Datenschutzexperte zur Unterstützung herangezogen werden. Sollten sich Sachverhalte als juristisch kompliziert darstellen, wird sich der Datenschutzexperte an die Abteilung KDI (datenschutz_sicherheit@vhv.de) wenden.

4 Datenschutz-Folgenabschätzung

Die Datenschutz-Folgenabschätzung (folgend: DSFA) ist durchzuführen, wenn die Form der Verarbeitung personenbezogener Daten aufgrund ihrer Art (z. B. Einführung einer neuen Technologie), ihres Umfangs, der Umstände oder Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat. Sie dient der systematischen Risikobetrachtung bei der Verarbeitung von personenbezogenen Daten und der Bestimmung geeigneter Abhilfemaßnahmen, insbesondere technische und organisatorische Vorkehrungen, um diese Risiken einzudämmen.

Eine DSFA ist stets vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge vom Risikoverantwortlichen durchzuführen. Prüffragen, die zur Ermittlung der Relevanz einer DSFA beitragen sollen, sind an relevanten Stellen im Unternehmen, z. B. im Projektantragsprozess, verankert. Auch Änderungen an bestehenden Verfahren können unter die Pflicht zur DSFA fallen.

Da eine DSFA meist nicht ad-hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig vom Risikoverantwortlichen, unterstützt durch den Informationssicherheits- und den Datenschutzbeauftragten, auf den Weg gebracht werden.

Eine DSFA ist kein einmaliger Vorgang. Sollten sich neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA noch nicht berücksichtigt werden, so ist die DSFA zu überprüfen und anzupassen.

In der VHV Gruppe wurde daher ein Konzept zur DSFA erstellt. Dieses finden Sie in Anlage A zu dieser Richtlinie. Darin enthalten sind detaillierte Vorgaben und Arbeitsschritte, um den gesetzlichen Vorgaben gerecht zu werden.

Hinweis für die Praxis: Die Relevanzprüfung in Bezug zur DSFA ist im Projektantragsprozess und im Softwareentwicklungsprozess verankert. Wenn die Relevanzprüfung positiv verlaufen sollte, ist wie in dem „Konzept Datenschutz-Folgenabschätzung“ beschrieben weiter zu verfahren.

Beispiele für die Notwendigkeit einer DSFA sind in **Anlage A.5** des Konzepts enthalten.

5 Meldungen bei Verletzung des Schutzes personenbezogener Daten (Datenpanne)

Die VHV Gruppe hat ein Verfahren zur Meldung von Verletzungen des Schutzes personenbezogener Daten etabliert. Der Fachbereich, in dem die Verletzung oder der Verdacht einer Verletzung bekannt geworden ist, hat sich unter Angabe der zur Verletzung führenden Fakten unverzüglich an das Postfach: sicherheitsvorfall@vhv.de zu wenden. Dafür ist das im WorkNet hinterlegte Dokument „Meldeformular Datenschutz und Informationssicherheit“ zu verwenden. Unter einer Verletzung des Schutzes personenbezogener Daten fallen die Vernichtung, der Verlust oder die unbeabsichtigte oder unrechtmäßige Veränderung oder die unbefugte Offenlegung bzw. der unbefugte Zugang zu personenbezogenen Daten.

Der Datenschutzbeauftragte stößt nach Prüfung des Sachverhalts, der durch das Formular mitgeteilt wurde, die notwendigen Maßnahmen zur Abwendung und Eindämmung der potenziellen Schäden an.

Hat die Bewertung zum Ergebnis, dass die Verletzung zu einem Risiko für Rechte und Freiheiten von natürlichen Personen führt, ist die Verletzung binnen 72 Stunden der zuständigen Aufsichtsbehörde mit den gesetzlich geforderten Angaben zu melden. Diese Frist beginnt mit der Kenntnisnahme des Vorfalls im Konzern und nicht erst mit Versendung des Meldebogens an KDI zu laufen.

Der Datenschutzbeauftragte übernimmt die Meldung gegenüber der Aufsichtsbehörde in Abstimmung mit der betroffenen Geschäftsleitung.

Die Meldung beinhaltet:

- Eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Ursache, der Datenkategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von der VHV Gruppe ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Im Falle eines hohen Risikos für die Rechte und Freiheiten der Betroffenen werden diese durch die betroffene Gesellschaft informiert. Der Datenschutzbeauftragte übernimmt auch diesbezüglich die Koordinations- und Abstimmfunktion im Konzern und gegenüber der betroffenen Geschäftsleitung.

Beispiele einer Datenpanne: Der Versand von Standmitteilungen oder sonstigen Informationen zu Versicherungsverträgen an einen unberechtigten Dritten; die Löschung durch eine nicht autorisierte Person; die Unmöglichkeit der Wiederherstellung eines Backups; das Abhandenkommen eines Schlüssels zu den Geschäftsräumen; ein Datendiebstahl (durch Hacking oder physisches Eindringen in eine geschützte Umgebung); ein Befall durch Ransomware oder der Verlust eines mobilen, unverschlüsselten Datenträgers; das irrtümliche Verschicken einer E-Mail in den CC- statt den BCC-Verteiler etc.

Hinweis für die Praxis in Fällen von Datenpannen: In dem Meldeformular sollte unter „Art des Vorfalls“ der Punkt „Datenpannenvorfall“ angekreuzt und daraufhin Kapitel 3 des Dokuments ausgefüllt werden. Die Angaben sollten so genau und detailreich wie möglich sein.

Die mögliche Kommunikation mit dem unberechtigten Empfänger der Daten übernimmt der zuständige Fachbereich unter Rücksprache mit der Abteilung KDI (**datenschutz_sicherheit@vhv.de**). Bezüglich der Zeichnung dieser Dokumente ist sich an den Arbeitsrichtlinien Beschwerdemanagement der Fachbereiche zu orientieren.

6 Änderungen

Redaktionelle Änderungen sowie Änderungen an dieser Konzernrichtlinie, die aufgrund veränderter rechtlicher Regelungen und Rahmenbedingungen notwendig geworden sind, dürfen durch den Leiter KDI ohne vorherige Zustimmung der Geschäftsleitung der Gesellschaften der VHV Gruppe vorgenommen werden. Weiterhin können Änderungen im Glossar o. ä. oder in den Anlagen durch die Mitarbeiter in der Abteilung KDI in Abstimmung mit dem zuständigen Abteilungsleiter vorgenommen werden. Die Geschäftsleitung der Gesellschaften der VHV Gruppe ist über erfolgte Änderungen zu informieren.

Diese Konzernrichtlinie wird grundsätzlich einmal jährlich in schriftlich dokumentierter Form überprüft. Dabei wird insbesondere überprüft, ob die Konzernrichtlinie mit der Geschäftsstrategie abgestimmt ist. Anlassbezogen wird diese Konzernrichtlinie auch ad-hoc überprüft. Ein entsprechender Anlass besteht insbesondere, wenn es zu einer Änderung des regulatorischen Umfeldes oder der Geschäftsstrategie kommt.

A Datenschutz-Folgenabschätzung

A.1 Einleitung

Auch bei einer rechtmäßigen Verarbeitung personenbezogener Daten können Risiken für die betroffenen Personen entstehen. Deswegen sieht die Datenschutzgrundverordnung (DSGVO) vor, dass durch geeignete Abhilfemaßnahmen, insbesondere technische und organisatorische Vorkehrungen, diese Risiken eingedämmt werden. Um eine systematische Risikobetrachtung zu ermöglichen, hat der Gesetzgeber ein spezielles Instrument, nämlich die sog. Datenschutz-Folgenabschätzung eingeführt (Art. 35 Abs. 1, 7 DSGVO).

Die DSGVO dient zur Beschreibung, Bewertung und Eindämmung von Risiken, die durch Datenverarbeitungen für die Rechte und Freiheiten von natürlichen Personen entstehen können. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung personenbezogener Daten aufgrund ihrer Art (z. B. Einführung einer neuen Technologie), ihres Umfangs, der Umstände oder Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die betroffenen Personen zur Folge hat.

Die DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen. Sofern mehrere ähnliche Verarbeitungsvorgänge ähnliche Risiken aufweisen, können diese zusammengefasst werden.

Eine DSFA ist stets vor der Aufnahme der zu betrachtenden Verarbeitungsvorgänge vom Risikoverantwortlichen durchzuführen. Prüffragen, die zur Ermittlung der Relevanz einer DSFA beitragen sollen, sind an relevanten Stellen im Unternehmen, z. B. im Projektantragsprozess, verankert. Auch Änderungen an bestehenden Verfahren können unter die Pflicht zur DSFA fallen.

Da eine DSFA meist nicht ad-hoc in wenigen Tagen erstellt werden kann, muss sie rechtzeitig vom Risikoverantwortlichen, unterstützt durch den Informationssicherheits- und den Datenschutzbeauftragten, auf den Weg gebracht werden.

Eine DSFA ist kein einmaliger Vorgang. Sollten sich neue Risiken ergeben, die Bewertung bereits erkannter Risiken ändern oder wesentliche Änderungen im Verfahren ergeben, die in der DSFA noch nicht berücksichtigt werden, so ist die DSFA zu überprüfen und anzupassen.

A.2 Rollen

Eine DSFA kann im Allgemeinen nur von einem interdisziplinären Team erstellt werden, das Kompetenzen im Bereich Datenschutz, Informationssicherheit, Risikoermittlung und in den Fachprozessen mitbringt. Da es letztendlich um Risikoentscheidungen geht, ist der Risikoverantwortliche unabdingbar und trägt die Verantwortung für die Durchführung des DSFA-Verfahrens.

A.2.1 Datenschutzbeauftragter

- Auf Anfrage: Beratung bei der Datenschutz-Folgenabschätzung und Überwachung der Durchführung durch die hierfür Verantwortlichen.
- Konsultation der zuständigen Aufsichtsbehörde gemäß Art. 36 Abs. 1 DSGVO, Erwägungsgrund 84.
- Anlaufstelle für die zuständigen Aufsichtsbehörden für Fragen im Zusammenhang mit der Verarbeitung oder der Konsultation der Aufsichtsbehörde gemäß Art. 36 DSGVO.
- Meldung von Verfahren, die im Rahmen der DSFA ein besonderes Risiko aufweisen.

A.2.2 Risikoverantwortlicher

- Ermittlung der mit der Verarbeitung von personenbezogenen Daten zusammenhängenden Risiken auch aus Betroffenensicht und ggf. die Durchführung und Dokumentation einer Datenschutz-Folgenabschätzung, sofern diese erforderlich ist.
- Unterstützung des Informationssicherheitsbeauftragten bei dem Durchlaufen der Relevanzprüfung.

A.2.3 Informationssicherheitsbeauftragter

Unterstützung des Risikoverantwortlichen bei der Durchführung der Datenschutz-Folgenabschätzung, insbesondere bei der Risikobeurteilung und Maßnahmendefinition.

A.2.4 Auftragsverarbeiter / Hersteller / Sonstige Dienstleister

Unterstützung des Risikoverantwortlichen, z. B. hinsichtlich der beim Dienstleister vorhandenen technischen und organisatorischen Maßnahmen.

A.3 Gewährleistungsziele und Schutzziele

Es hat sich im Bereich der IT-Sicherheit bzw. Informationssicherheit bewährt, Anforderungen als Schutzziele zu formulieren. Die Anforderungen des Datenschutzes sind gesetzlich normiert. Diese Anforderungen lassen sich ebenfalls mit Hilfe von Schutz-, bzw. Gewährleistungszielen umsetzen, die in kompakter und methodisch zugänglicher Form die operativen Risiken explizit machen, vor denen es durch eine angemessene Verfahrensgestaltung und Maßnahmen zu schützen gilt. Folgende Schutzziele angelehnt an das Standard-Datenschutzmodell gelten derzeit im Bereich des Datenschutzes als etabliert:

- die Zweckbindung einer Datenverarbeitung mit Personenbezug,
- die Begrenzung der Datenverarbeitung auf das erforderliche und datensparsame Maß,
- die Berücksichtigung der Betroffenenrechte, wonach in einem Verfahren Prozesse insbesondere für die Beauskunftung, die Korrektur, das Sperren und das Löschen von Betroffenendaten vorzusehen sind,
- die Transparenz von Verfahren als Voraussetzung dafür, dass die rechtlich festgelegten Anforderungen an ein Verfahren sowohl für die Organisation selber, als auch zumindest in einer allgemeinverständlichen Form für den Betroffenen sowie für die Aufsichtsbehörden überprüfbar sind,
- die Informationssicherheit der eingesetzten Komponenten zur Datenverarbeitung.

Die bisherigen datenschutzrechtlichen Grundsätze und Gewährleistungsziele werden in der DSGVO fortgeschrieben und weiterentwickelt. Den Risiken der Informationssicherheit wird klassisch mit der Sicherung der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit begegnet. Aufbauend hierauf werden zusätzlich als spezifische Datenschutzschutzziele formuliert: Nichtverkettbarkeit, Datenminimierung, Transparenz und Intervenierbarkeit.

A.4 Ablauf der Datenschutz-Folgenabschätzung

Der Gesamtprozess der DSFA gliedert sich in vier Phasen. Eine Vorbereitungsphase, die zur Organisation der DSFA dient, die Bewertungsphase, die Maßnahmenphase und die Berichtsphase. Im Anschluss an die vierte Phase soll eine Überwachung und Fortschreibung der DSFA erfolgen.

A.4.1 Vorbereitungsphase (Relevanzprüfung)

Zunächst muss sich der Risikoverantwortliche mit der Frage auseinandersetzen, ob im konkreten Fall die Durchführung einer DSFA überhaupt erforderlich ist. Die DSGVO definiert die gesetzliche „Relevanzschwelle“ in Art. 35 Abs. 1 und nennt in Art. 35 Abs. 3 sodann einen nicht abschließenden Katalog mit Anwendungsfällen. Art. 35 Abs. 1 DSGVO bestimmt, dass wenn „aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ der Betroffenen besteht, eine DSFA durchzuführen ist. Dies impliziert, dass die bloße Datenverarbeitung als solche keine Notwendigkeit für die Durchführung einer DSFA auslöst. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang zu dokumentieren und dem Datenschutzbeauftragten (datenschutz_sicherheit@vhv.de) zur Kenntnis zu bringen.

Art. 35 Abs. 3 DSGVO benennt einige Faktoren, die wahrscheinlich zu einem hohen Risiko führen:

- Bei systematischen und umfassenden Bewertungen persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitungen einschließlich Profiling gründen und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlicher Weise erheblich beeinträchtigen.
- Bei umfangreicher Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Abs. 1 oder von Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 9a;
- Bei systematischer weiträumiger Überwachung öffentlich zugänglicher Bereiche.

Die Aufsichtsbehörden sind verpflichtet, Fälle von Datenverarbeitungen zu definieren und zu veröffentlichen, in denen vorab eine DSFA vorzunehmen ist (vgl. Art. 35 Abs. 4 DSGVO). Die aktuelle Liste von Verarbeitungsvorgängen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist, finden Sie in diesem Dokument unter A.5 „Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO für den öffentlichen und nichtöffentlichen Bereich (Liste der Nds. Aufsichtsbehörde)“.

Ebenso werden die Aufsichtsbehörden ermächtigt, Fälle zu definieren und zu veröffentlichen, in denen eine DSFA explizit nicht vorzunehmen ist (Art. 35 Abs. 5 DSGVO).

Mit Hilfe des Templates zur „Datenschutz-Folgenabschätzung“ kann eine Relevanzprüfung vorgenommen werden und damit die Notwendigkeit zur Durchführung einer DSFA ermittelt werden.

Sofern die Relevanzprüfung die Notwendigkeit einer DSFA ergibt, ist weiter – entsprechend dieses Konzepts – zu verfahren. Sofern die Prüfung negativ ausfällt, ist das Ergebnis zu dokumentieren und dem Datenschutzbeauftragten zuzuleiten.

A.4.2 Bewertungsphase

Nachdem die Vorbereitungsphase und die entsprechende Relevanzprüfung mit dem Ergebnis, dass eine DSFA durchzuführen ist, abgeschlossen wurde, schließt sich eine detaillierte Risikoanalyse an. Hier werden die Kriterien für die Bewertung der Risiken ausgewiesen und sodann beurteilt. Dieses erfolgt durch den Risikoverantwortlichen unter Einbindung des Informationssicherheitsbeauftragten und des Datenschutzbeauftragten.

A.4.2.1 Beschreibung des Vorhabens

Es ist zu definieren, was im Rahmen der DSFA geprüft wird, also der konkrete Prüfgegenstand. Die betrachteten Verarbeitungsvorgänge sind von anderen (Geschäfts-) Prozessen abzugrenzen und ausführlich und abschließend mit allen Datenflüssen und den insoweit genutzten IT-Systemen zu beschreiben. Wesentlich ist es, die Zwecke der Verarbeitungsvorgänge festzulegen.

Beispiel zur Verdeutlichung:

PERSONENBEZOGENE DATEN	ZWECK
GPS-Zeit	Errechnung des Punktewertes infolge der Fahrweise eines Kunden zur Berechnung des persönlichen Nachlasses
GPS-Position	Anzeige der Fahrdaten eines Kunden in seinem Portal und in seiner App
Aktuelle Geschwindigkeit auf Basis der GPS-Positionen	Diebstahlschutz für das Fahrzeug eines Kunden
GPS-Signalqualität	Navigation zu günstigen Tankstellen
Akku-Status	Navigation zu Fuß zum Fahrzeug
Input-Status	Anzeige und Export aller gefahrenen Routen in einem frei definierten Zeitfenster
Status externe Stromversorgung	Zur Verfügung stellen der eigenen Fahrdaten (Standort und kumulierter Punktwert) an Freunde, die ebenfalls einen Telematik-Vertrag abgeschlossen haben (dieses ist durch den Kunden frei bestimmbar und jederzeit abwählbar)
Beschleunigung in X-, Y- und Z-Richtung	Sicherstellung, dass dem Kunden nach einem Unfall nichts passiert oder ein Rettungsdienst beauftragt wird

Tabelle 1: Beispiel des Zwecks von Verarbeitungsvorgängen

PHASE DES GESCHÄFTS-PROZESSES	DETAILLIERTE BESCHREBUNG DER PHASE	TECHNISCHE SYSTEME BZW. VERFAHREN, DIE FÜR DIE PROZESS-PHASE RELEVANT IST	WEITERE UNTERSTÜTZENDE WERTE, DIE FÜR DIE PROZESS-PHASE RELEVANT SIND
Erhebung personenbezogener Daten	Nach Abschluss des entsprechenden Versicherungsvertrages wird dem Versicherungsnehmer die Telematikbox unseres Dienstleisters kostenlos zur Verfügung gestellt. Die Erhebung der personenbezogenen Daten erfolgt im Anschluss durch die Telematikbox des Dienstleisters. Dazu ist die Telemaikbox in den Zigarettenanzünder einzustecken und die Zündung des Fahrzeuges zu bestätigen.	Telematikbox Server Verschlüsselungserfahren	Interne Mitarbeiter Mitarbeiter des Dienstleisters Wartungspersonal
Verarbeiten personenbezogener Daten	Beim Dienstleister werden die erfassten und über das Netz der Telekom übermittelten Daten ausgewertet und in einen Scorewert umgerechnet	Arbeitsplatz-PCs, Applikationsserver Fileserver Berechnungssoftware	Mitarbeiter des Dienstleisters Wartungspersonal
Übermittlung personenbezogener Daten	Es findet lediglich die Übermittlung des Scorewertes an die VHV statt. Das Portal und die App kommunizieren regelmäßig zur Anzeige der Scorewerte und der gefahrenen Strecke mit dem Backend des Dienstleisters. Für den Transport wird der HTTPS-Standard zum Schutz gegen Zugriffe von außen verwendet.	HTTPS	Mitarbeiter Mitarbeiter des Dienstleisters Wartungspersonal
Aufbewahrung personenbezogener Daten	Der Scorewert wird im Rechenzentrum der VHV gespeichert, ebenso wie die pseudonymisierten Daten der Telematik-Kunden. Darüber hinaus speichert der Dienstleister alle Fahrdaten in seinem Rechenzentrum.	Server	Mitarbeiter Mitarbeiter des Dienstleisters Wartungspersonal

PHASE DES GESCHÄFTS-PROZESSES	DETAILLIERTE BESCHREBUNG DER PHASE	TECHNISCHE SYSTEME BZW. VERFAH-REN, DIE FÜR DIE PROZESS-PHASE RELE-VANT IST	WEITERE UN-TERSTÜT-ZENDE WERTE, DIE FÜR DIE PROZESS-PHASE RELE-VANT SIND
Vernichtung personenbe-zogener Da-ten	Die unterschiedlichen Daten werden nach Beendigung des Vertrages und Abschluss aller Forderungen aus dem Vertrag nach Ablauf der entsprechenden Aufbewah-rungsfristen gelöscht. Grunddaten (Angaben zum Kunden) wie Name, Anschrift, Beruf, Bankverbindung, Kommunikationsdaten sind buchungsrele-vant und unterliegend damit der 10-jährigen Aufbewahrungsfrist. Fahrdaten werden vertragsgemäß noch 14 Tage nach Kündigung im Portal zur Ver-fügung gestellt. Im Anschluss werden die Daten gelöscht. Es sei denn, dass der Tele-matik-Vertrag ununterbrochen drei Jahre bestanden hat. Dann kann der Kunde seine Daten auch drei Jahre rückwirkend einse-hen. Nach Abschluss von drei Jahren wird das älteste Jahr gelöscht. Nachlassdaten sind buchungsrelevant und werden dementsprechend 10 Jahre nach Beendigung des Vertrages gelöscht.	Hardware	Mitarbeiter Mitarbeiter des Dienstleisters Datenträgerver-nichter

Tabelle 2: Phase in Geschäftsprozessen

A.4.2.2 Identifikation der Akteure und betroffenen Personen

Neben der Beschreibung des Prüfgegenstandes ist die Identifikation der handelnden und betroffenen Akteure vorzunehmen. Dies umfasst insbesondere die Personen, die unmittelbar Einfluss auf das Verfahren nehmen können sowie solche Personen, die mittelbar oder unmittelbar durch den Einsatz betroffen sind oder in einer entsprechenden datenschutzrechtlichen Beziehung zu einander stehen.

Für jede dieser Akteursgruppen ist zu beschreiben, welche Rolle sie bei der Datenverarbeitung spielen, welche Rechtsbeziehungen zwischen ihnen bestehen und welche Interessen bei ihnen vorliegen. Die Besonderheit einer DSFA besteht darin, dass neben dem Risiko missbräuchlicher Datennutzung durch unbefugte Dritte vor allem das Risiko betrachtet wird, dass durch die missbräuchliche, den eigentlichen Zweck überdehnende oder überschreitende – sowie sogar bestimmungsgemäße – Nutzung von Daten durch die Organisation selbst entsteht. Insofern ist bei der Identifikation der Betroffenen stets zu eruieren, welche Motive zur Nutzung von Daten bestehen können.

Unter diesem Punkt ist auch zu prüfen, ob Gremien, z. B. der Betriebsrat, aufgrund von Mitbestimmungsvorschriften einzubeziehen ist.

A.4.2.3 Identifikation der maßgeblichen Rechtsgrundlagen

Aus Art. 5 Abs. 2 DSGVO folgt, dass der Verantwortliche die Einhaltung seiner Rechenschaftspflicht nachweisen können muss. Zur Rechtmäßigkeit der Verarbeitung gemäß Art. 5 Abs. 1 lit. a DSGVO gehört die Identifikation der einschlägigen Rechtsgrundlagen im Sinne von Art. 6 DSGVO. Als Eingriff in das Grundrecht auf Schutz personenbezogener Daten der Betroffenen gemäß Art. 8 Grundrechtecharta bedarf jede Datenverarbeitung einer Rechtfertigung.

Die betreffenden Rechtsgrundlagen werden im Folgenden aufgeführt:

- Verarbeitung zur Vertragserfüllung oder Vertragsanbahnung – Art. 6 Abs. 1 lit. b DSGVO
- Einwilligung des Betroffenen (ohne Gesundheitsdaten) – Art. 6 Abs. 1 lit. a DSGVO
- Erfüllung einer rechtlichen Verpflichtung – Art. 6 Abs. 1 lit. c DSGVO
- Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten – Art. 6 Abs. 1 lit. f DSGVO
- Einwilligung in die Verarbeitung besonderer Kategorien (insbesondere Gesundheitsdaten) – Art. 9 Abs. 2 lit. a DSGVO
- Verarbeitung zu statistischen oder zu Forschungszwecken – Art. 9 Abs. 2 lit. j in Verbindung mit Art. 89 Abs. 1 DSGVO
- Verarbeitung besonderer Kategorien personenbezogener Daten zur Verteidigung von Rechtsansprüchen – Art. 9 Abs. 2 lit. f. DSGVO
- Rechtmäßige automatisierte Entscheidungen im Einzelfall einschließlich Profiling – Art. 22 Abs. 2 lit. a DSGVO
- Rechtmäßige automatisierte Entscheidungen im Einzelfall – Art. 22 Abs. 2 lit. a DSGVO
- Rechtmäßige Verwendung eines Wahrscheinlichkeitswerts bei Scoring § 31 Abs. 1 BDSG
- Rechtmäßige Verwendung eines Wahrscheinlichkeitswerts von Auskunfteien bzgl. Bonität § 31 Abs. 2 BDSG
- Verarbeitung für Zwecke des Beschäftigungsverhältnisses § 26 Abs. 1 BDSG
- Verarbeitung besonderer Kategorien personenbezogener Daten zur Erfüllung von Rechten und Pflichten § 26 Abs. 2 BDSG
- Verarbeitung von Beschäftigtendaten mit Einwilligung § 26 Abs. 2 BDSG
- Verarbeitung von Beschäftigungsdaten auf Basis von Kollektivvereinbarungen § 26 Abs. 3 BDSG
- Erhebung personenbezogener Gesundheitsdaten bei Dritten § 213 VVG

Um die geeignete Rechtsgrundlage zu identifizieren, kann der Datenschutzbeauftragte beratend hinzugezogen werden.

A.4.2.4 Identifikation der Bewertungsmaßstäbe anhand der Schutzziele

Das Verfahren wird anhand der Schutzziele durchgeführt, welche die DSGVO vorsieht. Verlangt wird die Sicherung des Verfahrens in Bezug zur:

- Datenminimierung:
  Die Verarbeitung und Erhebung von personenbezogenen Daten soll dabei auf den Umfang beschränkt sein, der zur Erfüllung des jeweiligen Zweckes erforderlich ist.
- Verfügbarkeit:
  Die Anforderung den Verlust der Daten zu vermeiden, beinhaltet auch die Nutzbarkeit der Daten (und eine Auskunftsfähigkeit über sie) zu gewährleisten, da ein Verlust dieser Fähigkeit einem Verlust der Daten in der Auswirkung für den Verarbeitungszweck gleichkommt.
- Integrität:
  Aus den Anforderungen von Nr. 3 und Nr. 4 der Anlage zu § 9 BDSG, unbefugte Veränderungen und Entfernungen auszuschließen, ist das Gewährleistungsziel Integrität auf der Ebene der Daten abzuleiten
- Vertraulichkeit:
  Die Verpflichtung zur Wahrung der Vertraulichkeit ergibt sich insbesondere aus den Gewährleistungspflichten der Nr. 3 und Nr. 4 der Anlage zu § 9 BDSG, aus Art. 5 Abs. 1 lit. f DSGVO.

- Transparenz:
  Das Gewährleistungsziel Transparenz (Art. 5 Abs. 1 lit. a) bezeichnet die Anforderung, dass in einem unterschiedlichen Maße sowohl Betroffene, als auch die Betreiber von Systemen sowie zuständige Kontrollinstanzen erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen einer Datenverarbeitung besitzt.
- Nichtverkettbarkeit:
  Das Gewährleistungsziel Nichtverkettung wird aus dem Grundsatz der Zweckbindung Art. 1 Abs. 1 lit. b DSGVO abgleitet und bezeichnet die Anforderung, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden.
- Intervenierbarkeit:
  Das Gewährleistungsziel Intervenierbarkeit wird abgeleitet aus Art. 5 Abs. 1 lit. a, lit. d, lit. f. und bezeichnet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt und die verarbeitende Stelle verpflichtet ist, die entsprechenden Maßnahmen umzusetzen.

Bei der Betrachtung der Schutzziele ist zu berücksichtigen, dass die Betroffenenperspektive eingenommen wird. Eine DSFA hat nicht das Ziel, die Geschäftsprozesse unseres Hauses zu schützen, sondern die Rechte und Freiheiten natürlicher Personen, unserer Kunden, unserer Mitarbeiter zu schützen. Zur Bewertung wurde ein Template erstellt, dass Sie im WorkNet unter „Datenschutz-Folgenabschätzung“ finden. Dieses soll mögliche Angreifer, Angriffsmotive und Angriffsziele berücksichtigen.

A.4.2.5 Identifikation möglicher Missbrauchsszenarien / Risikoquellen

Zunächst müssen die Quellen des Risikos für die Rechte und Freiheiten der Betroffenen identifiziert werden. Insbesondere ist zu bestimmen, welche Personen motiviert sein könnten, die Verarbeitungsvorgänge und die hierin verarbeiteten Daten in unrechtmäßiger Weise zu nutzen und welches ihre Beweggründe und mögliche Ziele sein können.

Hierbei geht es nicht nur um vorsätzliche Angriffe von außen, z. B. von Hackern, mit dem Ziel der Schädigung des Unternehmens, z. B. durch Erpressung oder durch vorsätzliche Datenmanipulationen. Es geht auch um Risiken, die sich aus der Organisation heraus ergeben können, beispielsweise durch ein vorsätzliches oder fahrlässiges Verhalten von internen Mitarbeitern. So ist z. B. das Interesse, „Bewegungsprofile zu erstellen“ oder ein „Nutzerverhalten zu analysieren“, um gezielter Werbung vornehmen zu können oder die eigenen Produkte zu verbessern bzw. Risiken besser kalkulieren zu können, ein realistisches Missbrauchsszenario.

Ein weiteres realistisches Szenario wäre z. B., dass ein Mitarbeiter (Sachbearbeiter, Administrator etc.) ein Interesse daran haben könnte, jemanden Drittes zu begünstigen oder – im Gegenteil dazu – jemanden zu schaden, indem er z. B. Manipulationen an Daten vornimmt oder diese zweckwidrig nutzt, z. B. zur Weitergabe an einen Dritten.

Ein Cloudbetreiber ist z. B. in der Lage, auf Daten, die in seinem operativen Umfeld gespeichert sind, zuzugreifen. Hierdurch könnte er die Daten z. B. analysieren, übermitteln oder mit anderen Daten, von anderen Kunden, kombinieren.

Risiken können auch aus der Zugriffsmöglichkeit von Dritten, z. B. von Sicherheitsbehörden entstehen. Bei einem Zugriff durch Dritte stellt sich insbesondere die Frage nach der Sicherung der Berechtigung des Datenzugriffs aber auch nach der Sicherung der Transparenz und der Integrität.

LFD.	DATENSCHUTZ-GEFÄHRDUNG
1	Auftragsverarbeitung in Drittstaaten
2	Datenabfluss/unberechtigter Zugriff durch erstmaligen Einsatz innovativer Technik
3	Fehlerhaftes Ratingverfahren/Klassifizierung
4	Kontrollverlust des Betroffenen über seine personenbezogene Daten
5	Wesentliche prozessuale und/oder technischen Änderungen
6	Schwächen in Datenqualität
7	Reputationsschäden - z. B. unrechtmäßige Veröffentlichung personenbezogene Daten
8	Unbeabsichtigter/unrechtmäßige Veränderung von personenbezogenen Daten
9	Unbeabsichtigter/unrechtmäßige Vernichtung, Verlust von personenbezogenen Daten
10	Unberechtigter Zugriff auf besonders sensible Daten
11	Unberechtigter Zugriff durch Dritte (u. a. Behörden, Dienstleister)
12	Unrechtmäßige Übermittlung an einen Dritten
13	Unrechtmäßige Verarbeitung personenbezogener Daten durch Auftragsverarbeiter
14	Unzureichende Steuerung/Überwachung des Auftragsverarbeiters
15	Videoüberwachung öffentlich zugänglicher Bereiche
16	Hohe Anzahl an Zugriffsberechtigten
17	Unzureichende Information über Profiling an Betroffenen
18	Zu umfangreiche Datensammlung
19	Zweckänderung (Überdehnung) ohne Information an Betroffenen

Tabelle 3: Datenschutz-Gefährdungen

A.4.2.6 Schutzbedarf und Eingriffsintensität

An dieser Stelle ist der Schutzbedarf zu ermitteln. Der Schutzbedarf wird eingeteilt in die Stufen „normal“, „erhöht“ und „hoch“ und ist in der nachstehenden Tabelle skizziert:

SCHUTZBEDARF	BESCHREIBUNG
Normal	Da *jede* Verarbeitung personenbezogener Daten einen Eingriff in die Grundrechte der betroffenen Person darstellt, kann der Schutzbedarf gemäß SDM niemals niedriger als „normal“ sein. Deshalb ist grundsätzlich davon auszugehen, dass jedes personenbezogene Verfahren mindestens *normalen Schutzbedarf* aufweist. Weniger schutzbedürftig können folgerichtig nur Verarbeitungen mit nichtpersonenbezogenen Daten sein.

SCHUTZBEDARF	BESCHREIBUNG

Erhöht	• Verarbeitung nicht veränderbarer Personendaten, die ein Leben lang zuordenbar sind (z. B. biometrische Daten)
	• Verbreitung eindeutig identifizierender, hoch verknüpfbarer Daten (Krankenversichertennummer, Steuer-ID)
	• Gesetzlich begründete Intransparenz der Verfahrensweisen für Betroffene (z. B. Verfassungsschutz, Scoring)
	• Verarbeitung von Daten in Verfahren mit möglichen gravierenden, finanziellen Auswirkungen für Betroffene
	• Verarbeitung von Daten in Verfahren mit möglichen Auswirkungen auf die Reputation des Betroffenen
	• Verarbeitung von Daten mit möglichen Auswirkungen auf die körperliche Unversehrtheit des Betroffenen
	• Verarbeitung von Daten, die Auswirkungen auf die
	  • Grundrechtsausübung einer Vielzahl Betroffener haben;
	  • Gefahr von Diskriminierung, Stigmatisierung;
	  • Eingriffe in besonders geschützten inneren Lebensbereich eines Betroffenen.
	
	Wenn besondere Arten personenbezogener Daten gemäß Art. 35 Abs. 3 DSGVO verarbeitet werden, bedarf es grundsätzlich keiner weiteren Abstimmung oder Erwägungen, sondern es ist von einem „hohen Schutzbedarf“ auszugehen.

Hoch	Von einem hohen *Schutzbedarf* ist auszugehen, wenn ein Betroffener von den Entscheidungen bzw. Leistungen der Organisation unmittelbar existentiell abhängig ist und zusätzliche Risiken für den Betroffenen nicht bemerkbar sind.

Tabelle 4: Schutzbedarf

Ein normaler Schutzbedarf liegt vor, wenn personenbezogene Daten betroffen sind. Von einem hohen Schutzbedarf ist auszugehen, wenn besonders schutzwürdige Daten, insbesondere Gesundheitsdaten, Daten der Unfall- oder Lebensversicherung, genetische Daten etc. betroffen sind. Von einem sehr hohen Schutzbedarf ist bei einem direkten Einfluss auf Leib oder Leben auszugehen. Durch den „Kumulierungseffekt“ kann ein hoher Schutzbedarf auch bei Datenverarbeitungen entstehen, die für sich alleine betrachtet nur einen normalen Schutzbedarf aufweisen würden. Dies kann der Fall sein, wenn Daten von sehr vielen Personen erhoben werden („Kumulierung vieler Daten“) oder aber wenn Daten durch einzelne Personen (z. B. Administratoren) zu verschiedenen Zwecken erhoben werden, wobei sich die betroffenen Personen jeweils in verschiedenen Rollen befinden („Kumulierung vieler Berechtigungen“).Weist das Verfahren eine hohe Eingriffsintensität auf, bedarf es keiner weiteren Erwägungen, d. h. der hohen Eingriffsintensität steht ein hoher Schutzbedarf auf Seiten des Betroffenen gegenüber.

A.4.2.7 Eintrittswahrscheinlichkeit

Die Abstufungen der Eintrittswahrscheinlichkeiten werden aus dem Risikomanagement inkl. der Erweiterungen aus dem Informationssicherheitsrisikomanagements abgeleitet. Hierbei wird die Eintrittswahrscheinlichkeit anhand eines 100-Jahre-Ereignisses ermittelt.

Die Eintrittswahrscheinlichkeit wird in vier Stufen unterteilt:

- **Maximal = sehr hoch (4)** (größer 50% = Eintritt innerhalb von 2 Jahren)
- **Signifikat = hoch (3)** (zwischen 20% und 50% = Eintritt alle 2 bis 5 Jahre),
- **Eingeschränkt = mittel (2)** (zwischen 5% und 20% = Eintritt alle 5 bis 20 Jahre) und
- **Vernachlässigbar = niedrig (1)** (kleiner 5% = Eintritt alle 20 bis 100 Jahre)

A.4.2.8 Ergebnis der Risikobewertung

Im Ergebnis der Bewertungsphase ist für jede der Gefährdungen ein spezifischer Risikowert ermittelt worden, der die Priorisierung der Risikobehandlung aufzeigt.

Ein grüner Risikowert (1-3) wird grundsätzlich akzeptiert, da auch eine weitere kompensierende Maßnahme keine wesentliche Reduktion des Risikos erzeugen würde.

Ein gelber Risikowert (4-7) ist mit risikominimierenden Maßnahmen zu kompensieren. Hier ist explizit die Wirtschaftlichkeit in Hinblick auf die Schutzwirkwirkung zu überprüfen.

Ein roter Risikowert (8-12) ist umgehend durch eine reduzierende Maßnahme zu kompensieren.

EINTRITTSWAHRSCHEINLICHKEIT		**RISIKOWERT**		
sehr hoch	**< 2 Jahre**	4	8	12
hoch	**2 - 5 Jahre**	3	6	9
mittel	**> 5 - 20 Jahre**	2	4	6
gering	**> 20 Jahre**	1	2	3
SCHADENSZENARIEN		**SCHADENPOTENZIAL**		
Finanzieller Schaden		normal	erhöht	hoch
Reputativer Schaden				
Regulatorischer Schaden				

Tabelle 5: Risikobewertung

A.4.3 Maßnahmenphase

Die ermittelten Risiken müssen, abhängig von ihrem Risikowert (siehe Kapitel „Ergebnis der Risikobewertung“) durch geeignete Abhilfemaßnahmen (technische und organisatorische Vorkehrungen) eingedämmt werden. An dieser Stelle sind daher die erforderlichen Maßnahmen zu definieren, zu planen und in die Umsetzung zu bringen. Die Verantwortlichkeiten sind klar zu benennen. Verbleibende Restrisiken werden ermittelt und im Risikobehandlungsplan dokumentiert.

Sobald für den Betroffenen ein hohes Risiko und oder eine hohe Eintrittswahrscheinlichkeit bewertet wird, muss eine Abhilfemaßnahme geplant werden. In diesem Fall darf keines der Gewährleistungsziele, die vollständig in Art. 5 DSGVO verankert sind, unbeachtet bleiben. Abweichungen von den Standard-Maßnahmen, die das Standard Datenschutzmodell (SDM) vorsieht, sind zu begründen und die funktionale Äquivalenz von Ersatzmaßnahmen zu den empfohlenen Maßnahmen wäre nachzuweisen.

Beispiele für technische und organisatorische Maßnahmen für die jeweiligen Schutzziele sind:

Das Gewährleistungsziel **Datenminimierung** kann erreicht werden durch:

- Reduzierung von erfassten Attributen der betroffenen Personen,
- Reduzierung der Verarbeitungsoptionen in Verarbeitungsprozessschritten,
- Reduzierung von Möglichkeiten der Kenntnisnahme vorhandener Daten,
- Bevorzugung von automatisierten Verarbeitungsprozessen (nicht Entscheidungsprozessen), die eine Kenntnisnahme verarbeiteter Daten entbehrlich machen und die Einflussnahme begrenzen, gegenüber im Dialog gesteuerten Prozessen,

- Implementierung automatischer Sperr- und Löschroutinen, Pseudonymisierungs- und Anonymisierungsverfahren, Regelungen zur Kontrolle von Prozessen zur Änderung von Verfahren.

Typische Maßnahmen zur Gewährleistung der **Verfügbarkeit** sind:

- Anfertigung von Sicherheitskopien von Daten, Prozesszuständen, Konfigurationen, Datenstrukturen, Transaktionshistorien u. ä. gemäß einem getesteten Konzepts,
- Schutz vor äußeren Einflüssen (Schadsoftware, Sabotage, höhere Gewalt),
- Dokumentation der Syntax der Daten,
- Redundanz von Hard- und Software sowie Infrastruktur,
- Umsetzung von Reparaturstrategien und Ausweichprozessen,
- Vertretungsregelungen für abwesende Mitarbeiter

Typische Maßnahmen zur Gewährleistung der **Integrität** bzw. zur Feststellung von Integritätsverletzungen sind:

- Einschränkung von Schreib- und Änderungsrechten,
- Einsatz von Prüfsummen, elektronische Siegeln und Signaturen in Datenverarbeitungsprozessen gemäß eines Kryptografiekonzepts,
- dokumentierte Zuweisung von Berechtigungen und Rollen,
- Prozesse zur Aufrechterhaltung der Aktualität von Daten,
- Festlegung des Sollverhaltens von Prozessen und regelmäßiges Durchführen von Tests zur Feststellung und Dokumentation der Funktionalität, von Risiken sowie Sicherheitslücken und Nebenwirkungen von Prozessen,
- Festlegung des Sollverhaltens von Abläufen bzw. Prozessen und regelmäßiges Durchführen von Tests zur Feststellbarkeit bzw. Feststellung der Ist-Zustände von Prozessen

Typische Maßnahme n zur Gewährleistung der **Vertraulichkeit** sind:

- Festlegung eines Rechte- und Rollenkonzeptes nach dem Erforderlichkeitsprinzip auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle,
- Implementierung eines sicheren Authentisierungsverfahrens,
- Eingrenzung der zulässigen Personalkräfte auf solche, die nachprüfbar zuständig (örtlich, fachlich), fachlich befähigt, zuverlässig (ggf. sicherheitsüberprüft) und formal zugelassen sind sowie keine Interessenskonflikte bei der Ausübung aufweisen,
- Festlegung und Kontrolle der Nutzung zugelassener Ressourcen insbesondere Kommunikationskanäle,
- spezifizierte, für das Verfahren ausgestattete Umgebungen (Gebäude, Räume)
- Festlegung und Kontrolle organisatorischer Abläufe, interner Regelungen und vertraglicher Verpflichtungen (Verpflichtung auf Datengeheimnis, Verschwiegenheitsvereinbarungen etc.),
- Verschlüsselung von gespeicherten oder transferierten Daten sowie Prozesse zur Verwaltung und zum Schutz der kryptografischen Informationen (Kryptokonzept),
- Schutz vor äußeren Einflüssen (Spionage, Hacking).

Typische Maßnahmen zur Gewährleistung der **Nichtverkettung** sind:

- Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten,
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten,
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung,
- Trennung nach Organisations-/Abteilungsgrenzen,
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements durch die verantwortliche Stelle und eines sicheren Authentisierungsverfahrens,
- Zulassung von nutzerkontrolliertem Identitätsmanagement durch die verarbeitende Stelle,
- Einsatz von zweckspezifischen Pseudonymen, Anonymisierungsdiensten, anonymen Credentials, Verarbeitung pseudonymer bzw. anonymisierter Daten,
- geregelte Zweckänderungsverfahren.

Typische Maßnahmen zur Gewährleistung der **Transparenz** sind:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Geschäftsprozesse, Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen, Zusammenspiel mit anderen Verfahren,
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren,
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden, Geschäftsverteilungspläne, Zuständigkeitsregelungen,
- Dokumentation von Einwilligungen und Widersprüchen,
- Protokollierung von Zugriffen und Änderungen,
- Nachweis der Quellen von Daten (Authentizität),
- Versionierung,
- Dokumentation der Verarbeitungsprozesse mittels Protokollen auf der Basis eines Protokollierungs- und Auswertungskonzepts,
- Berücksichtigung der Auskunftsrechte von Betroffenen im Protokollierungs- und Auswertungskonzept.

Typische Maßnahmen zur Gewährleistung der **Intervenierbarkeit** sind:

- differenzierte Einwilligungs-, Rücknahme- sowie Widerspruchsmöglichkeiten,
- Schaffung notwendiger Datenfelder z. B. für Sperrkennzeichen, Benachrichtigungen, Einwilligungen, Widersprüche, Gegendarstellungen,
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes,
- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem,
- Implementierung standardisierter Abfrage- und Dialogschnittstellen für Betroffene zur Geltendmachung und/oder Durchsetzung von Ansprüchen,
- Nachverfolgbarkeit der Aktivitäten der verantwortlichen Stelle zur Gewährung der Betroffenenrechte,
- Einrichtung eines Single Point of Contact (SPoC) für Betroffene,
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten.

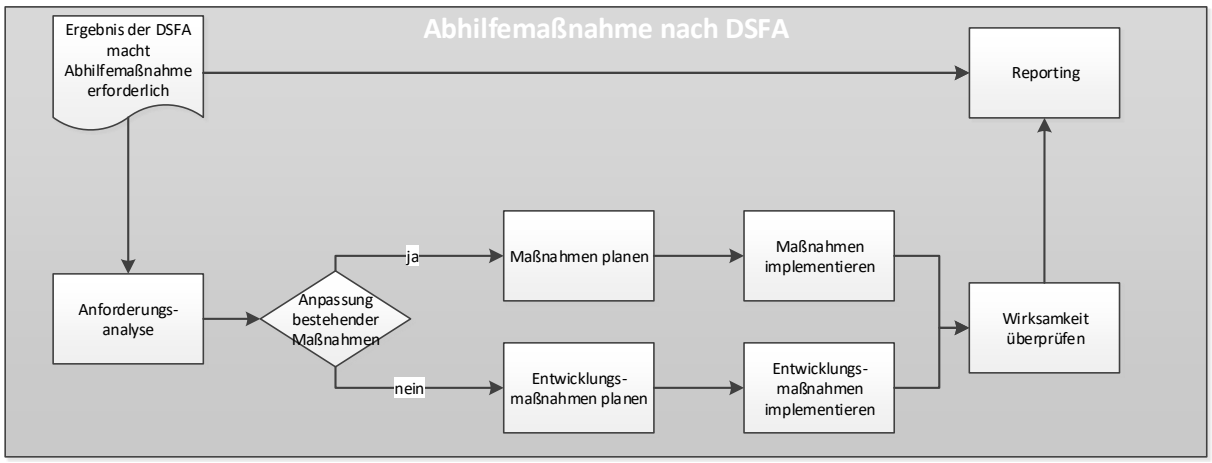

Abbildung 2: Planung und Wirksamkeitsprüfung von Abhilfemaßnahmen

Bevor die geplante Datenverarbeitung eingesetzt wird, müssen die für die Eindämmung des Restrisikos geeigneten Abhilfemaßnahmen (insbesondere TOMs) umgesetzt sein. Vorher darf die Verarbeitung personenbezogener Daten nicht stattfinden. Sofern sich bei der Umsetzung herausstellt, dass geplante

Maßnahmen nicht (wirksam) realisiert werden können, müssen andere geeignete Maßnahmen ausgewählt, die Restrisikobewertung angepasst oder die Verarbeitungsvorgänge insgesamt angepasst werden, so dass sie den Anforderungen der DSGVO genügen.

Nachdem Abhilfemaßnahmen umgesetzt wurden, müssen sie auf ihre Wirksamkeit getestet werden. Möglicherweise zeigt sich bei der Umsetzung der Maßnahmen, dass weitere Risiken bestehen, die ebenfalls zu behandeln sind.

A.4.3.1 Wirksamkeit der Maßnahmen

Die jeweiligen Maßnahmen sind vom Informationssicherheitsbeauftragten auf ihre Wirksamkeit hin zu überprüfen. Sollte sich die Wirksamkeit nicht ergeben oder die erwartete Schutzwirkung nicht entfalten sind weitere Maßnahmen zu ergreifen.

A.4.3.2 Dokumentation: Nachweis über die Einhaltung der DSGVO

Nach der Bewertungs- und Maßnahmenphase müssen die Bewertungsergebnisse und die Entscheidung für die getroffene Maßnahmenauswahl dokumentiert werden. Damit eine DSFA die eingangs erwähnten positiven Effekte erzielen kann, ist es notwendig, dass der Prozess umfänglich dokumentiert wird.

A.4.3.3 Freigabe der Verarbeitungsvorgänge

Im Anschluss und mit Vorliegen der vollständigen Dokumentation können die Verarbeitungsvorgänge formal durch den Risikoverantwortlichen freigegeben werden.

A.4.3.4 Überprüfung der DSFA

Um eine ordnungsgemäße Durchführung sicherzustellen, ist es sinnvoll, den DSFA-Bericht von einem unabhängigen Dritten überprüfen zu lassen. Insoweit bietet sich der Datenschutzbeauftragte an, der ohnehin im Rahmen des Verfahrens eingebunden ist. Zu diesem Zweck legt der Risikoverantwortliche dem Datenschutzbeauftragten den finalen DSFA-Bericht mit einer angemessenen Frist zur Prüfung vor. Der Datenschutzbeauftragte erstellt daraufhin eine abschließende Stellungnahme.

A.4.4 Berichtsphase

Damit eine DSFA die anfangs erwähnten Effekte erzielen kann, ist es notwendig, dass der Prozess umfänglich dokumentiert und in Form eines Berichts zugänglich gemacht wird. Ein solcher DSFA-Bericht sollte einer standardisierten Gliederung folgen, die es Aufsichtsbehörden, Unternehmen und der Öffentlichkeit erleichtert, die Ergebnisse zu bewerten und zu vergleichen.

A.4.4.1 DSFA-Bericht

Ein Bericht für eine Datenschutz-Folgenabschätzung muss gemäß Art. 35 Abs. 7 mindestens die folgenden Angaben enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Abs. 1 und

- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird,

wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Sofern eine Konsultation der Aufsichtsbehörde notwendig ist, muss ein DSFA-Bericht um die folgenden Angaben ergänzt werden (Art. 36 Abs. 3):

- gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
- die Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Datenschutz-Folgenabschätzung gemäß Art. 35 und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Die Erstellung des DSFA-Berichts obliegt dem Risikoverantwortlichen. Nach Fertigstellung des Berichts übermittelt der Risikoverantwortliche den Bericht an den Datenschutzbeauftragten, damit dieser den Bericht, gemeinsam mit seiner Stellungnahme der Geschäftsleitung zur Kenntnis bringen kann. Sofern kein hohes Restrisiko verbleibt, steht es dem Datenschutzbeauftragten frei, die Berichte gemeinsam mit dem jährlichen Tätigkeitsbericht zu verbinden.

A.4.4.2 Verbleiben eines Restrisikos

Ergibt die DSFA, dass trotz technischer und organisatorischer Maßnahmen zur Risikoeindämmung weiterhin ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht (Restrisiko) und soll das Verfahren oder die Technologie dennoch eingeführt werden, informiert der Datenschutzbeauftragte die Geschäftsleitung der betroffenen Gesellschaft, dass eine Konsultation der zuständigen Aufsichtsbehörde erfolgen muss. Die Kommunikation in Richtung der zuständigen Aufsichtsbehörde obliegt dem Datenschutzbeauftragten.

Die Geschäftsleitung der zuständigen Gesellschaft trifft unter Berücksichtigung der Empfehlungen der Aufsichtsbehörde und der Einbindung des Datenschutzbeauftragten eine Entscheidung, ob die Verarbeitungsvorgänge angesichts der verbleibenden Restrisiken durchgeführt werden können und ggf. welche zusätzlichen Abhilfemaßnahmen in diesem Fall zum Einsatz kommen sollen. Die Aufsichtsbehörde kann ihrerseits die in Art. 58 DSGVO genannten Befugnisse ausüben und z. B. eine Warnung, Anweisung oder Untersagung aussprechen.

A.4.5 Überwachung und Fortschreibung der DSFA

Die Abschätzung von Datenschutzfolgen ist kein einmaliger und linearer Prozess, sondern muss über die Lebensdauer eines Prüfgegenstands ggf. mehrfach wiederholt werden. Insofern ist durch den Risikoverantwortlichen kontinuierlich zu überwachen, ob sich die Rahmenbedingungen des Einsatzes in technischer, organisatorischer Weise ändern, die neue Datenschutzrisiken nach sich ziehen. Die Überwachung, ob sich die rechtlichen Parameter für die Durchführung der DSFA ändern, obliegt dem Datenschutzbeauftragten.

Auch ist durch den Informationssicherheitsbeauftragten zu überwachen, ob die gewählten Schutzmaßnahmen den erwarteten Nutzen haben oder ob andere Maßnahmen zu ergreifen sind. Die Dokumentation der DSFA ist mit solchen Informationen kontinuierlich fortzuschreiben.

A.5 Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO für den öffentlichen und nichtöffentlichen Bereich (Liste der Nds. Aufsichtsbehörde)

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
1	Umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder besonderen Amtsgeheimnis unterliegen, auch wenn es sich nicht um Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO handelt (Interne Anmerkung: Lebens- und Unfallversicherungsunternehmen unterliegen einem Berufsgeheimnis gemäß § 203 StGB)	Sozialleistungsträger Große Anwaltssozietäten	Eine große Rechtsanwaltskanzlei, die schwerpunktmäßig familienrechtliche Mandate betreut.
2	Umfangreiche Verarbeitung von personenbezogenen Daten über den Aufenthalt von natürlichen Personen	Fahrzeugdatenverarbeitung – Car Sharing/Mobilitätsdienste Fahrzeugdatenverarbeitung – Zentralisierte Verarbeitung der Messwerte oder Bilderzeugnisse von Umgebungssensoren Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen bietet einen Car-Sharing-Dienst oder andere Mobilitätsdienstleistungen an und verarbeitet hierfür insbesondere umfangreich Positions- und Abrechnungsdaten. Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren. Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
3	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personenerhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind • und der Erzeugung von Datengrundlagen dienen, die dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den betroffenen Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen können.	Fraud-Prevention-Systeme Scoring durch Auskunfteien, Banken oder Versicherungen	Zur Prävention von Betrugsfällen verarbeitet der Betreiber eines Online-Shops umfassende Datenmengen. Das Ergebnis der Prüfung ist ein Risikowert, der darüber entscheidet, ob einem Käufer der Rechnungskauf als Zahlungsart angeboten wird oder nicht. Eine Auskunftei führt ein Scoring im Hinblick auf die Vertrauenswürdigkeit von Personen durch. Eine Bank führt Scoring durch, um das Ausfallrisiko der Rückzahlungen von Personen zu bestimmen. Eine Versicherung führt ein Scoring durch, um das Risiko einer Person im Hinblick auf bestimmte Eigenschaften o-der Aktivitäten der Person zur Bestimmung der Höhe einer Versicherungspolice zu bestimmen.
4	Mobile optisch-elektronische Erfassung personenbezogener Daten in öffentlichen Bereichen, sofern die Daten aus verschiedenen Erfassungssystemen in großem Umfang zentral zusammengeführt werden.	Fahrzeugdatenverarbeitung – Umgebungssensoren	Ein Unternehmen erhebt personenbezogene Daten, die Fahrzeuge über ihre Umgebung generieren und ermittelt daraus beispielsweise freie Parkplätze oder verbessert Algorithmen zum automatisierten Fahren.

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
5	Umfangreiche Erhebung und Veröffentlichung oder Übermittlung von personenbezogenen Daten, die zur Bewertung des Verhaltens und anderer persönlicher Aspekte von Personen dienen und von Dritten dazu genutzt werden können, Entscheidungen zu treffen, die Rechtswirkung gegenüber den bewerteten Personen entfalten, oder diese in ähnlich erheblicher Weise beeinträchtigen	Betrieb von Bewertungsportalen Inkassodienstleistungen – Forderungsmanagement Inkassodienstleistungen – Factoring	Ein Online-Portal bietet Nutzern die Möglichkeit an, Leistungen von Selbstständigen öffentlich feingranular zu bewerten. Z. B. ein Online-Bewertungsportal für Ärzte, Selbstständige oder Lehrer. Ein Unternehmen verarbeitet für seine Kunden in großem Umfang personenbezogene Daten von Schuldnern, insbesondere Vertragsdaten, Rechnungsdaten und Daten über Vermögensverhältnisse von Schuldnern zur Geltendmachung von Forderungen. Ggf. werden Daten an Auskunfteien übermittelt. Ein Unternehmen lässt sich in großem Umfang Forderungen übertragen um diese auf eigenes Risiko geltend zu machen. Es verbarbeitet hierfür insbesondere Vertragsdaten, Rechnungsdaten, Scoringdaten und Informationen über Vermögensverhältnisse von Schuldnern. Ggf. werden Daten an Auskunfteien übermittelt.

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
6	Verarbeitung von umfangreichen personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die betroffenen Personen ergeben, oder diese in andere Weise erheblich beeinträchtigen	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen Geolokalisierung von Beschäftigten	Zentrale Aufzeichnung der Aktivitäten am Arbeitsplatz (z. B. Internetverkehr, Mailverkehr und die Nutzung von Wechselmedien) mit dem Ziel, von Seiten des Verantwortlichen unerwünschtes Verhalten (z. B. Versand interner Dokumente) zu erkennen. Ein Unternehmen erstellt Bewegungsprofile von Beschäftigen (z. B. per RFID, Handy-Ortung oder GPS) zur Sicherung des Personals (Wachpersonal, Feuerwehrleute), zum Schutz von wertvollem Eigentum des Arbeitgebers oder eines Dritten (LKW mit Ladung, Geldtransport) oder zur Koordination von Arbeitseinsätzen im Außendienst.
7	Erstellung umfassender Profile über die Interessen, das Netz persönlicher Beziehungen oder die Persönlichkeit der betroffenen Personen	Betrieb von Dating- und Kontaktportalen Betrieb von großen Sozialen Netzwerken	Ein Dating Portal erstellt Profile der Nutzer um möglichst passende Kontaktvorschläge zu generieren.

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
8	Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und der Weiterverarbeitung der so zusammengeführten Daten, sofern • die Zusammenführung oder Weiterverarbeitung in großem Umfang vorgenommen werden, • für Zwecke erfolgen, für welche nicht alle der zu verarbeitenden Daten direkt bei den betroffenen Personen erhoben wurden, • die Anwendung von Algorithmen einschließen, die für die betroffenen Personen nicht nachvollziehbar sind.	Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden. Tätigkeit von Auskunfteien	Eine Unternehmen mit umfangreichem Stamm an natürlichen Personen als Kunden, analysiert Daten über das Kaufverhalten der Kunden und die Nutzung der eigenen Webangebote einschließlich des eigenen Webshops, verknüpft mit Bonitätsdaten von dritter Seite und Daten aus der Werbeansprache über soziale Medien einschließlich der vom Betreiber des sozialen Medium bereitgestellten Daten über die angesprochenen Mitglieder, um Informationen zu gewinnen, die zur Steigerung des Umsatzes eingesetzt werden können.
9	Einsatz von künstlicher Intelligenz zur Verarbeitung personenbezogener Daten, zur Steuerung der Interaktion mit den betroffenen Personen oder zur Bewertung persönlicher Aspekte der betroffenen Personen	Kundensupport mittels künstlicher Intelligenz	Ein Unternehmen setzt ein System ein, welches mit Kunden durch Konversation interagiert und für deren Beratung personenbezogene Daten durch eine künstliche Intelligenz verarbeitet.
10	Nicht bestimmungsgemäße Nutzung von Sensoren eines Mobilfunkgeräts im Besitz der betroffenen Personen oder von Funksignalen, die von solchen Geräten versandt werden, zur Bestimmung des Aufenthaltsorts oder der Bewegung von Personen über einen substantiellen Zeitraum	Offline-Tracking von Kundenbewegungen in Warenhäusern, Einkaufszentren o. ä. Verkehrsstromanalyse auf der Grundlage von Standortdaten des öffentlichen Mobilfunknetzes	Ein Unternehmen verarbeitet die WLAN-, Bluetooth- oder Mobilfunksignale von Passanten und Kunden, um die Laufwege und das Einkaufsverhalten nachverfolgen zu können.
11	Automatisierte Auswertung von Video- oder Audio-Aufnahmen zur Bewertung der Persönlichkeit von betroffenen Personen	Auswertung von Telefongesprächen mittels Algorithmen	Ein Callcenter wertet automatisiert die Stimmungslage der Anrufer aus.

#	MAßGEBLICHE BESCHREIBUNG DES VERARBEITUNGSVORGANGS	TYPISCHE EINSATZFELDER	BEISPIELE
12	Erhebung personenbezogener Daten über Schnittstellen persönlicher elektronischer Geräte, die nicht gegen ein unbefugtes Auslesen geschützt sind, das die betroffenen Personen nicht erkennen können	Erfassung des Kaufverhaltens unterschiedlicher Personenkreise zur Profilbildung und Kundenbindung unter Zuhilfenahme von Preisen, Preisnachlässen und Rabatten.	Ein Unternehmen verwendet Kundenkarten, welche das Einkaufsverhalten der Kunden erfassen. Als Anreiz zur Verwendung der Kundenkarte erhält der Kunde mit jedem Einkauf Treuepunkte. Mithilfe der gewonnenen Daten erstellt der Anbieter umfassende Kundenprofile.
13	Umfangreiche Anonymisierung von besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, falls diese (ggf. vermeintlich) anonymen Daten an Dritte weitergegeben oder zu nicht nur internen statistischen Zwecken verarbeitet werden sollen	Forschung mit medizinischen Daten	Umfangreiche besondere personenbezogene Daten werden durch ein Apothekenrechenzentrum oder eine Versicherung anonymisiert und zu anderen Zwecken selbst verarbeitet oder an Dritte weitergegeben.
14	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO – auch wenn sie nicht als „umfangreich“ im Sinne des Art. 35 Abs. 3 lit. b) anzusehen ist – sofern eine innovative Nutzung von digitalen Fernkommunikationsmitteln erfolgt.	Einsatz von Telemedizin-Lösungen zur detaillierten Bearbeitung von Krankheitsdaten	Ein Hausarzt bietet eine Telefonsprechstunde über ein Webportal oder eine App an.
15	Verarbeitung von Daten gemäß Art. 9 Abs. 1 und Art. 10 DSGVO – auch wenn sie nicht als „umfangreich“ im Sinne des Art 35 Abs. 3 lit. b) anzusehen ist – sofern die Daten durch die Anbieter neuer Technologien dazu verwendet werden, die Leistungsfähigkeit der Betroffenen zu bestimmen.	Zentrale Speicherung der Messdaten von Sensoren, die in Fitnessarmbändern oder Smartphones verbaut sind	Ein Unternehmen bietet einen Dienst an, mit dem Daten aus Fitnessarmbändern zur Verbesserung.

Tabelle 6: Liste von Verarbeitungsvorgängen