Richtlinie Datenschutzmanagementsystem (DSMS)

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

Fassung gemäß Vorstandsbeschluss vom 05.08.2021

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Richtlinie Datenschutzmanagementsystem
Version	21.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft
Erstmalige Freigabe	09.05.2018
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
18.0	09.05.2018	Ersterstellung	Daniel Fürdauer
19.0	11.04.2019	Jährliches Review, Einführung Datenschutzexperten	Daniel Fürdauer
20.0	29.07.2020	Jährliches Review, Redaktionelle Änderungen	Daniel Fürdauer
21.0	29.07.2021	Jährliches Review	Daniel Fürdauer

Art der Freigabe – VHV Konzern

Version	Datum	Wesentliche Änderungen	Bestätigt von
18.0	23.04.2018	Nein	Sina Rintelmann
19.0	10.04.2019	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-MANAGEMENTSYSTEM (DSMS) VERSION 21.0“ DER VHV GRUPPE

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

Die Bezeichnung URCF ist ein Synonym für die Risikomanagementfunktion.

Kapitel 4.3

Die Gesellschaft ernennt keine Verantwortlichen für Verarbeitungstätigkeiten.
Stattdessen werden dezentrale Datenschutz-Verantwortliche ernannt. Die Bestimmungen zu den Dezentralen Datenschutz-Verantwortlichen werden in der Richtlinie Dezentrale Datenschutz-Verantwortliche geregelt.

Kapitel 4.4

Die Unterrichtung und Beratung erfolgt hinsichtlich der Rechte und Pflichten nach der Datenschutzgrundverordnung (DSGVO) sowie der sonstigen Datenschutzvorschriften der Europäischen Union und der Republik Österreich.

Kapitel 4.5

Die Datenschutzexperten werden vom Datenschutz-Beauftragten in Abstimmung mit dem jeweiligen Vorgesetzten festgelegt und bleiben organisatorisch und disziplinar in Ihrer Abteilung bzw. Stabstelle.
Die konkreten Aufgaben der Datenschutzexperten werden direkt mit dem Datenschutz-Beauftragten abgestimmt. Die Aufgaben der Datenschutzexperten können auch andere Abteilungen betreffen.
Der Datenschutz-Beauftragte wird zusätzlich durch die externe Unternehmensberatung Secur-Data unterstützt.

Kapitel 4.6

In der VAV Versicherungs-Aktiengesellschaft ist der Datenschutz-Beauftragte in der Stabstelle Datenschutz und Informationssicherheit und berichtet unmittelbar an den Vorstandsvorsitzenden.

KONZERNRICHTLINIE

DATENSCHUTZMANAGEMENTSYSTEM (DSMS)

KONZERNDATENSCHUTZ UND INFORMATIONSSICHERHEIT
KLASSIFIKATION: INTERN
VERSION 21.0

VHV GRUPPE

Dokumenteneigenschaften

Typ	Konzernrichtlinie
Geltungsbereich	Siehe Kapitel „Geltungsbereich“
Erstmalige Freigabe	11.12.2017
Verabschiedet durch (Datum)	VHV Vereinigte Hannoversche Versicherung a.G. (11.02.2021) VHV Holding AG (11.02.2021) VHV Allgemeine Versicherung AG (13.11.2017) Hannoversche Lebensversicherung AG (28.11.2017) WAVE Management AG (19.12.2017) Pensionskasse der VHV Versicherungen
Klassifikation	Intern
Dokumentenverantwortlicher Verantwortliche Abteilung	Ulrich Lintker (Abteilungsleiter KDI) Konzerndatenschutz und Informationssicherheit (KDI)
Fachlicher Ansprechpartner	Roman Lemke
Letztes Review	Februar 2021

Historie

Version	Freigabedatum	Beschreibung der Änderung
17.0	25.09.2017	Initiale Erstellung
19.0	30.01.2019	Jährliches Review; Anpassung der Versionierung
20.0	28.01.2020	Jährliches Review; Anpassung der Versionierung
21.0	15.02.2021	Jährliches Review; Anpassung der Versionierung und des Dokumentenverantwortlichen

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

Abbildungsverzeichnis

1 Zielsetzung des Datenschutzmanagementsystems

Das Datenschutzmanagementsystem (im Folgenden: DSMS) hat die Zielsetzung, den datenschutzkonformen Ablauf der in den Unternehmen der VHV Gruppe vorhanden Tätigkeiten, Systeme, Prozesse und Maßnahmen sicherzustellen. Das DSMS beschreibt neben den einzuhaltenden Grundsätzen des Datenschutzes, einen Regelprozess zur Erkennung, Bewertung, Behebung, Dokumentation und Berichterstattung von datenschutzrelevanten Verarbeitungstätigkeiten der VHV Gruppe. Die nach dem DSMS geforderten Maßnahmen werden in der Konzernrichtlinie Datenschutz sowie in Arbeitsrichtlinien für die Mitarbeiter konkretisiert. Die Verfolgung dieser Ziele soll praxisnah und im jeweils erforderlichen Maß erfolgen.

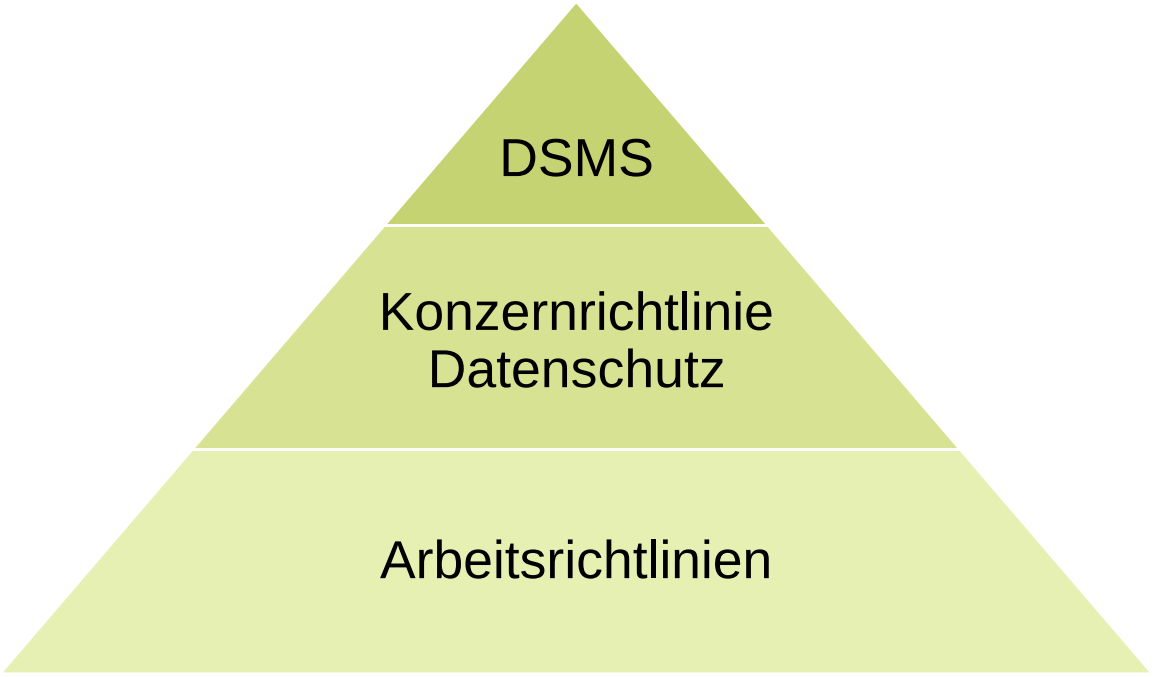

Abbildung 1: DSMS-Pyramide

2 Geltungsbereich

Das DSMS 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

3 Grundsätze des Datenschutzes

Die VHV Gruppe hält sich bei der Verarbeitung von personenbezogenen Daten an das geltende Datenschutzrecht. Aus den gesetzlichen Anforderungen des europäischen und nationalen Datenschutzrechts (insbesondere DS-GVO, BDSG) sowie den Verhaltensregeln für den Umgang mit personenbezogenen Daten durch die deutsche Versicherungswirtschaft (kurz: CoC) ergeben sich zehn Grundsätze des Datenschutzes:

3.1 Rechtmäßigkeit

Eine Datenverarbeitung ist nur zulässig, soweit diese rechtmäßig ist. Dabei gilt das sogenannte Verbot mit Erlaubnisvorbehalt, d. h. das Gesetz sieht eine Datenverarbeitung grundsätzlich als rechtswidrig an, es sei denn, diese ist erlaubt. Alle Verarbeitungsvorgänge der VHV Gruppe müssen daher auf einer Rechtsgrundlage basieren. Das sind entweder eine rechtsgeschäftliche Einwilligung oder gesetzliche Erlaubnistatbestände.

3.2 Zweckbindung und Nichtverkettbarkeit

Die VHV Gruppe verarbeitet personenbezogene Daten nur für zuvor festgelegte, eindeutige und legitime Zwecke. Eine zweckändernde Verarbeitung ist nur dann zulässig, wenn der Weiterverarbeitungszweck im Einklang mit dem ursprünglichen Erhebungszweck steht, d. h. die Zwecke miteinander kompatibel sind.

3.3 Transparenz und Informationspflichten

Die VHV Gruppe verarbeitet personenbezogene Daten nach dem Grundsatz der Transparenz. Dies setzt voraus, dass alle erforderlichen Hinweise, Informationen und Mitteilungen sowie Benachrichtigungen (Meldung von Verletzungen des Schutzes personenbezogener Daten) zur Verarbeitung von personenbezogenen Daten erteilt werden und leicht zugänglich, verständlich und in klarer einfacher Sprache verfasst sind. Der Betroffene soll dadurch die Möglichkeit haben, die Verarbeitung von Anfang bis Ende nachvollziehen zu können.

3.4 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 die betroffene Person eine Vorstellung davon bekommt, wer seine Daten verarbeitet, für welche Zwecke die Daten verarbeitet und an wen seine Daten weitergegeben werden.

3.5 Intervenierbarkeit und Betroffenenrechte

Die VHV Gruppe gewährleistet, dass die betroffenen Personen ihr gegenüber ihre datenschutzrechtlichen Betroffenenrechte ausüben können. Sie gewährleistet daher insbesondere die Einhaltung folgender Rechte:

- Recht auf Auskunft bzw. Erhalt einer Datenkopie
- Recht auf Berichtigung
- Recht auf Vergessenwerden bzw. Löschung
- Recht auf Datenübertragbarkeit bzw. Datenportabilität
- Recht auf Einschränkung der Datenverarbeitung
- Widerspruchsrechte

3.6 Datenminimierung und Speicherbegrenzung

Die VHV Gruppe verarbeitet 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 personenbezogene Daten wenn möglich nur solange gespeichert werden, wie dies zur Erfüllung des jeweiligen Speicherzwecks erforderlich ist. Diese Ziele werden durch die Pseudonymisierung, Anonymisierung oder das Löschen von personenbezogenen Daten gewährleistet.

3.7 Richtigkeit der Datenverarbeitung

Die personenbezogenen Daten der VHV Gruppe werden durch angemessene Maßnahmen sachlich richtig und erforderlichenfalls auf dem neuesten Stand gehalten. Der Grundsatz der Richtigkeit der Datenverarbeitung wird durch den Anspruch auf Berichtigung und Vervollständigung von unrichtigen bzw. unvollständigen Daten gestützt.

3.8 Vertraulichkeit, Verfügbarkeit und Integrität

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

3.9 Privacy by Default

Die VHV Gruppe gestaltet die Grundeinstellungen neuer und bestehender Verarbeitungstätigkeiten so, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

3.10 Privacy by Design

Die VHV Gruppe sieht bereits bei der Planung von neuen Verarbeitungstätigkeiten geeignete technische und organisatorische Maßnahmen in Systemen und Prozessen vor, um die Einhaltung der vorstehenden Grundsätze zu gewährleisten.

4 Rollen und Verantwortlichkeiten

Zum Betrieb und zur Aufrechterhaltung des DSMS hat die VHV Gruppe folgende Rollen und Verantwortlichkeiten etabliert:

4.1 Gesamtvorstand der VHV Holding AG / VHV a.G.

Der Gesamtvorstand der VHV Holding AG / VHV a.G. trägt die Verantwortung für die Einrichtung, die angemessene Ausgestaltung, die Wirksamkeit und die laufende Überwachung des DSMS auf Gruppenebene. Er verabschiedet das DSMS sowie die weiteren zum Betrieb eines DSMS erforderlichen Richtlinien.

4.2 Geschäftsleitung der Einzelgesellschaften

Jede Gesellschaft innerhalb der VHV Gruppe ist verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und Richtlinien. Der Vorstand bzw. die Geschäftsführung der Einzelgesellschaft trägt die Verantwortung für die Einrichtung, die angemessene Ausgestaltung, die Wirksamkeit und laufende Überwachung des DSMS aus Sicht der Einzelgesellschaft. Zudem gibt die Geschäftsleitung Strategien und Richtlinien zum Datenschutz in den Einzelgesellschaften vor.

4.3 Verantwortliche für Verarbeitungstätigkeiten

Jede Gesellschaft hat Verantwortliche für Verarbeitungstätigkeiten benannt. In den operativen Bereichen sind dies in der Regel die Spartenverantwortlichen. In den NVT-Bereichen sind dies grds. die Abteilungsleiter der jeweiligen Querschnittsfunktion. Die Namen sind in den Verarbeitungsverzeichnissen hinterlegt. Die Verantwortlichen für Verarbeitungstätigkeiten sind für die Meldung bestehender und neuer Verarbeitungstätigkeiten, in denen personenbezogene Daten verarbeitet werden sowie die Meldung der für das Verzeichnis von Verarbeitungstätigkeiten notwendigen Informationen an den Datenschutzbeauftragten, verantwortlich. Der Datenschutzbeauftragte führt die Verzeichnisse der Verarbeitungstätigkeiten in einem Datenschutzmanagement-Tool.

4.4 Datenschutzbeauftragter

Für die Einzelgesellschaften der VHV Gruppe ist ein Datenschutzbeauftragter bestellt, soweit dies gesetzlich erforderlich ist.

Der Datenschutzbeauftragte ist ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen einzubinden. Der Datenschutzbeauftragte übernimmt dabei folgende Aufgaben:

- Unterrichtung und Beratung der Geschäftsleitung der Unternehmen der VHV Gruppe sowie der dort Beschäftigten hinsichtlich der Rechte und Pflichten nach der DS-GVO sowie der sonstigen Datenschutzvorschriften der Europäischen Union und der Bundesrepublik Deutschland,
- Überwachung der Einhaltung aller einschlägigen Datenschutzvorschriften einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter und der diesbezüglichen Überprüfung,
- Auf Anfrage: Beratung bei der Datenschutz-Folgenabschätzung und Überwachung der Durchführung durch die hierfür Verantwortlichen,
- Zusammenarbeit mit den zuständigen Aufsichtsbehörden,
- Anlaufstelle für die zuständigen Aufsichtsbehörden für Fragen im Zusammenhang mit der Verarbeitung oder der Konsultation der Aufsichtsbehörde

Der Vorstand stattet den Datenschutzbeauftragten mit allen zur Durchführung der ihm übertragenen Aufgaben notwendigen Befugnissen und Kompetenzen aus. Der Datenschutzbeauftragte berichtet unmittelbar an die höchste Managementebene der jeweiligen Konzerngesellschaft.

4.5 Datenschutzexperten

Die Datenschutzexperten, die organisatorisch und disziplinarisch in den Versicherungssparten der Einzelgesellschaften angesiedelt sind, unterstützen den Datenschutzbeauftragten bei der Wahrnehmung seiner Aufgaben. Insbesondere werden die Datenschutzexperten als erste Ansprechpartner der Mitarbeiter bei Anfragen von Kunden (im Rahmen der Ausübung von Betroffenenrechten) tätig. Die konkreten Aufgaben der Datenschutzexperten sind in den Arbeitsrichtlinien der Sparten geregelt.

4.6 Informationssicherheitsbeauftragter und IT-Security-Management

Der Informationssicherheitsbeauftragte und das IT-Security-Management arbeiten eng mit dem Datenschutzbeauftragten zusammen, um die jeweiligen Anforderungen und Überwachungshandlungen aufeinander abzustimmen. Zur Nutzung von Synergien und um das Datenschutzmangementsystem möglichst eng mit dem Informationssicherheitsmanagementsystem zu verzahnen, sind diese Rollen und Funktionen in der Abteilung „Konzerndatenschutz und Informationssicherheit“ gebündelt. Die Aufgaben der Abteilung sind in der Geschäftsordnung näher spezifiziert.

5 DSMS-Regelprozess

Die VHV Gruppe hat zur Einhaltung des Datenschutzes im Unternehmen den folgenden Regelprozess etabliert:

Abbildung 2: DSMS-Regelprozess

Der Datenschutzbeauftragte unterstützt fachkundig und beratend beim Aufbau und bei der Koordination des Datenschutzmanagements und überwacht dessen Funktionsfähigkeit.

5.1 Planung und Konzeption

Die Planung und Konzeption jeder Verarbeitung von personenbezogenen Daten orientiert sich an den Grundsätzen des Datenschutzes (Kapitel 0). Die Grundsätze müssen bei der Planung und Konzeption jederzeit Berücksichtigung finden. Aus diesem Grunde sind die Mitarbeiter dazu angehalten, die konkreten Vorgaben und Prozesse, die in den Konzernrichtlinien Datenschutz und Informationssicherheit sowie den nachgelagerten Richtlinien enthalten sind, zu beachten. Vom Datenschutzbeauftragten erstellte Dokumentenvorlagen und Leitfäden sowie regelmäßige Schulungs- und Sensibilisierungsmaßnahmen sollen ferner dazu beitragen, den Datenschutzgrundsätzen bestmöglich Rechnung zu tragen. Sofern die Verarbeitung mit besonderen Risiken für den Betroffenen verbunden ist (z. B. durch den Einsatz neuer Technologien), ist durch den Risikoverantwortlichen unter bedarfsweiser Hinzuzuziehung des Datenschutzbeauftragten eine Datenschutzfolgenabschätzung gemäß den Vorgaben der Konzernrichtlinie Datenschutz durchzuführen. Auf Basis der Planung und Konzeption werden geeignete technische und organisatorische Maßnahmen unter Berücksichtigung der internen und externen Vorgaben ermittelt. Bei der Auswahl von geeigneten Maßnahmen werden neben dem Datenschutzbeauftragten, der Informationssicherheitsbeauftragte und das IT-Security-Management beratend tätig.

5.2 Umsetzung

Die jeweiligen Maßnahmen werden auf Basis der zuvor erfolgten Planung und Konzeption einschließlich der Risikobewertung und unter Berücksichtigung des Stands der Technik durch die Fachbereiche bzw. die Informatik umgesetzt. Diesbezüglich werden auch die Implementierungskosten sowie die Verhältnismäßigkeit zwischen Nutzen und Aufwand einer Maßnahme berücksichtigt.

5.3 Kontrolle und Überwachung

5.3.1 Kontrollen im Fachbereich

Neben den in den Richtlinien enthaltenden Kontrollverpflichtungen der Fachbereiche, die sich z. B. aus der Konzernrichtlinie Informationssicherheit ergeben, obliegt es den Risikoverantwortlichen, im Falle von datenschutz- und sicherheitsrelevanten Risiken geeignete und angemessene Kontrollen zu implementieren.

5.3.2 Überwachung durch den Datenschutzbeauftragten

Die Einhaltung der Datenschutzgrundsätze unterliegt der regelmäßigen Überwachung durch den Datenschutzbeauftragten. Externe Prüfer werden bedarfsweise für Prüfungshandlungen hinzugezogen. Soweit thematisch sinnvoll, werden die Überwachungshandlungen mit den Prüfungen des Informationssicherheitsbeauftragten abgestimmt. Der Datenschutzbeauftragte kommt seiner Überwachungsfunktion im Einzelnen wie folgt nach:

- Anlassbezogene Überwachungen finden insbesondere statt, sofern ein Sachverhalt bekannt wird, der einen Verstoß gegen die Grundsätze des Datenschutzes (Kapitel 0) darstellt.
- Es wird auf Basis eines jährlichen Überwachungsplanes eine regelmäßige Überwachung der Einhaltung des Datenschutzes gewährleistet. Der Überwachungsplan berücksichtigt, dass Schwerpunkte der Überwachung mit Blick auf die Schutzbedürftigkeit der Daten im Zusammenhang mit dem Risiko der jeweiligen Verarbeitungstätigkeit gesetzt werden können.
- Die Überwachungstätigkeit wird in geeigneter Form dokumentiert. Der Nachweis kann durch einen Tätigkeitsbericht erfolgen, den der Datenschutzbeauftragte dem Verantwortlichen jährlich zur Verfügung stellt (siehe Berichtspflichten).

5.3.3 Kontrollen durch die Interne Revision

Risikoorientierte Prüfungshandlungen der Internen Revision sorgen ferner dafür, die Funktionsfähigkeit und Wirksamkeit des Datenschutzmanagementssystems in Gänze sicherzustellen.

5.4 Anpassung und Verbesserung

Ergibt die Kontrolle und Überwachung der Verarbeitungstätigkeiten durch den Datenschutzbeauftragten eine Abweichung vom Soll-Zustand, wird der Risikoverantwortliche hierüber unverzüglich in Kenntnis gesetzt. Der Datenschutzbeauftragte empfiehlt unter Berücksichtigung der konkreten Risikosituation und unter Einbeziehung des Fachbereichs geeignete Maßnahmen, um die Abweichung zu beseitigen oder die bestehenden Risiken zu minimieren. Er überwacht die fristgemäße Umsetzung der Maßnahmen. Bestehende Restrisiken, die nicht kurzfristig kompensiert werden können, werden dem Leiter URCF mitgeteilt. Zur Berichterstattung im Übrigen vgl. unter Kapitel 7 – Berichtspflichten.

6 Dokumentations- und Rechenschaftspflichten

6.1 Verzeichnis von Verarbeitungstätigkeiten

Die Einzelgesellschaften der VHV Gruppe führen Verzeichnisse von Verarbeitungstätigkeiten, die personenbezogene Daten beinhalten. Die Verantwortlichen für die Verarbeitungstätigkeiten haben dem Datenschutzbeauftragten die hierfür erforderlichen Informationen zur Verfügung zu stellen sowie Änderungen von Verarbeitungstätigkeiten oder neue Verarbeitungsverfahren mitzuteilen. Die Verzeichnisse werden regelmäßig durch die Verantwortlichen für Verarbeitungstätigkeiten auf Aktualität überprüft. Der Datenschutzbeauftragte führt die gemeldeten Verzeichnisse der Verarbeitungstätigkeiten für die jeweiligen Einzelgesellschaften in einem Datenschutzmanagementtool.

6.2 Nachweis der Datenschutz- und Datensicherheitsmaßnahmen

Mit Blick auf die sog. Rechenschaftspflichten (Accountability) der Geschäftsleitung, muss es jederzeit möglich sein, die Rechtskonformität der Verarbeitung sowohl in rechtlicher als auch in technischer und organisatorischer Hinsicht nachzuweisen. Die Tätigkeiten der VHV Gruppe, welche im Rahmen der Planung, Umsetzung, Überprüfung und Anpassung von Datensicherheitsmaßnahmen erbracht werden, sind in geeigneter Weise durch die jeweils beteiligten Rollen zu dokumentieren.

7 Berichtspflichten

7.1 Jährlicher Bericht

Der Datenschutzbeauftragte erstellt einmal jährlich einen Tätigkeitsbericht für die Verantwortlichen (Geschäftsleitung). Zusätzlich zu den regelmäßigen und situativen Abstimmungen mit den Schlüsselfunktionen, enthalten die Leiter der Compliance-Funktion, der Leiter URCF und der Leiter der Internen Revision den Bericht des Datenschutzbeauftragten zur Kenntnis. Der Bericht des Datenschutzbeauftragten kann in den jährlichen Compliance-Bericht integriert werden.

7.2 Ad-hoc Bericht

Sofern bei einer Überprüfung sofortiger Handlungsbedarf festgestellt wird, der sich nicht ohne größeren Aufwand beseitigen lässt, berichtet der Datenschutzbeauftragte unverzüglich an den nach dem Geschäftsverteilungsplan zuständigen Fachvorstand oder Geschäftsführer der betroffenen Einzelgesellschaft. Eine Ad-hoc-Berichtspflicht besteht insbesondere in den folgenden Fällen, die keinen zeitlichen Aufschub dulden:

- Schwerwiegende, systematische oder wiederholte Verstöße gegen die datenschutzrechtlichen Vorgaben und Richtlinien, insbesondere gegen das geltende Datenschutzrecht,
- Anordnungen oder Anhörungen der Aufsichtsbehörden
- Konkret drohende Bußgelder oder Repuatationsschäden
- Klageverfahren von betroffenen Personen oder Verbraucherverbänden.

8 Änderungen

Redaktionelle Änderungen sowie Änderungen an dieser Arbeitsanweisung, die aufgrund veränderter rechtlicher Regelungen und Rahmenbedingungen notwendig geworden sind, dürfen durch den Datenschutzbeauftragten ohne vorherige Zustimmung der Geschäftsleitung der Einzelgesellschaften der VHV Gruppe vorgenommen werden.

Die Geschäftsleitung der Gesellschaften 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.