

Datenschutzrichtlinie HiSV
Version: 2.2

Erstelldatum: 01.11.2025
Ersteller: Oliver Thehos

Vithos IT-Services GbR
Martin-Schmeisser-
Weg 18
44227 Dortmund

Compliance & Organisation
Tel. +49 231 427888 11
E-Mail: thehos@vithos-it.de

CHANGE MANAGEMENT

Version	Datum	Kommentar
1.0	04.08.2022	Grundlagen- Dokument zur Trennung der übergeordneten ISO 27001 Richtlinie von der DSGVO Richtlinie (von 2017)
2.0	07.07.2024	Anpassung der Richtlinie zwecks Anpassung an der Geschäftsprozesse
2.1	15.07.2024	Aktualisierung der Richtlinie
2.2	01.11.2025	Anpassung Kontaktdaten

Inhaltsverzeichnis

Change Management.....	2
1 Einleitung.....	5
2 Zielsetzung der Datenschutzrichtlinie	5
3 Anwendungsbereich	6
4 Bezug zu gesetzlichen Vorgaben	7
5 Die Prinzipien für die Verarbeitung personenbezogener Daten.....	7
5.1 Rechtmäßigkeit	7
5.2 Gesetzliche Rahmenbedingungen Kunden- und Partnerdaten	8
5.2.1 Verarbeitung von Daten im Kontext vertraglicher Beziehungen	8
5.2.2 Datenverarbeitung zum Zwecke der Werbung	8
5.2.3 Einwilligung in die Verarbeitung personenbezogener Daten	9
5.2.4 Datenverarbeitung auf Basis einer gesetzlichen Erlaubnis oder Verpflichtung	9
5.2.5 Verarbeitung von Daten auf Grundlage berechtigten Interesses	9
5.3 Rechtsgrundlage Mitarbeiterdaten	9
5.3.1 Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses	9
5.3.2 Datenverarbeitung auf Grundlage gesetzlicher Erlaubnis oder Verpflichtung	10
5.3.3 Kollektivregelung für Datenvereinbarungen	10
5.3.4 Einwilligung in die Datenverarbeitung	11
5.3.5 Verarbeitung von Daten auf Grundlage berechtigten Interesses	11
5.4 Besonders schützwürdige Daten und deren Verarbeitung	12
5.5 Automatisierte Entscheidungen und Profiling	12
5.6 Telekommunikation, IT- Infrastruktur und Internet	13
5.7 Informationsverpflichtungen und Transparenz.....	14
5.8 Zweckbindung	14
5.9 Datenminimierung	14
6 Richtigkeit der Daten	15
6.1 Privacy by Design & Default	15
6.2 Einschränkungen der Verarbeitung und Löschung	15
6.3 Sicherheit der Daten und Verarbeitungsprozesse	16
6.4 Übermittlung personenbezogener Daten	16

6.4.1	Vereinbarung über EU-Standardvertragsklauseln 2021	17
6.4.2	EU akkreditierten Zertifizierungssystem zur Datenübermittlung	17
6.4.3	Anerkennung verbindlicher Unternehmensregelungen (BCR).....	18
6.4.4	Übermittlung an Behörden	18
7	Datenschutz- Folgeabschätzung	19
8	Verfahrensverzeichnis	19
9	Auftragsverarbeitung	19
9.1	Vorgaben für den Auftraggeber	20
9.2	Anforderungen an Auftragnehmer aus der Howden Gruppe.....	20
9.3	Anforderungen an übrige Auftragnehmer	21
10	Durchsetzbare Rechte für betroffene Personen.....	23
10.1	Rechte der betroffenen Person	23
10.2	Recht auf Beschwerde	24
11	Meldung von Datenschutzvorfällen.....	25
12	Datenschutzmanagement.....	25
12.1	Verantwortung der Geschäftsführung.....	25
12.2	Sensibilisierung.....	26
12.3	Organisation und Datenschutzbeauftragter	26
12.4	Kontrollmaßnahmen.....	27
12.5	Disziplinarische Maßnahmen	27
13	Aktualisierungen und Anpassungen der Datenschutzleitlinie	27
14	Veröffentlichung der Datenschutzrichtlinie.....	28
15	Kooperation mit Behörden	28
16	Hinweise zum Datenschutz auf unserer Webseite.....	28
16.1	Datenschutz.....	28
16.2	Verantwortliche Stelle/Diensteanbieter.....	29
16.3	Kontaktdaten des Datenschutzbeauftragten.....	29

1 EINLEITUNG

Die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG (nachstehend auch HiSV genannt) ist ein führendes Beratungsunternehmen für Sportversicherungen in Deutschland und Kontinentaleuropa.

HiSV wurde in den 50er Jahren von Erwin Himmelseher als Familienunternehmen gegründet. Die Kunden schätzen insbesondere die Qualität der Arbeit, den persönlichen, vertrauensvollen Kontakt zu ihren Ansprechpartnern und die stringenten Entscheidungsprozesse.

Das Vertrauen der Kunden in die außergewöhnliche Dienstleistung ist das Kapital von HiSV und alle aufgeführten Prozesse und Maßnahmen des Datenschutzes in dieser Leitlinie sowie der darüberhinausgehenden Selbstverpflichtung zur Umsetzung der ISO 27001 (Int. Norm zur Informationssicherheit) dienen dem Ziel, die Werte von HiSV und die ihnen anvertrauten personenbezogenen Daten ihrer Kunden und Partner zu schützen.

2 ZIELSETZUNG DER DATENSCHUTZRICHTLINIE

Die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG betrachtet die Wahrung der Persönlichkeitsrechte ihrer Mitarbeiter, Kunden und Partner als wesentlichen Bestandteil ihrer gesellschaftlichen und unternehmerischen Verantwortung.

Die Europäische Union hat, wie viele andere Länder auch, gesetzliche Standards zum Schutz personenbezogener Daten erlassen (EU-DSGVO). Zusammen mit dem ergänzenden deutschen Datenschutzgesetz (BDSG) und anderen verbindlichen Standards ergeben sich daraus Prozesse und Maßnahmen zum Schutz datenschutzrelevanter Informationen.

Dazu gehört beispielsweise, dass Daten nur dann in andere Länder übermittelt werden dürfen, wenn beim Empfänger ein angemessenes Datenschutzniveau gewährleistet ist oder dass personenbezogene Daten nur unter bestimmten Voraussetzungen erhoben oder verarbeitet werden dürfen.

Die vorliegende Datenschutzrichtlinie definiert ein einheitliches und hohes Schutzniveau für die Verarbeitung von datenschutzrelevanten Daten im Europäischen Wirtschaftsraum (im Weiteren als "EU/EWR" bezeichnet) sowie für die Erhebung, Verarbeitung sowie der Übermittlung von personenbezogenen Daten Konzerngesellschaften und Partner außerhalb der EU/EWR (inklusive deren anschließender dortiger Verarbeitung). Diese Datenschutzerklärung berücksichtigt insbesondere die Bestimmungen des Schweizer DSG, der EU-DSGVO und der UK GDPR. Die tatsächliche Anwendbarkeit der genannten Gesetze wird jeweils im Einzelfall geprüft und demensprechend umgesetzt.

Die Umsetzung der Richtlinie schafft hinsichtlich der HiSV anvertrauten Daten und Informationen angemessene Garantien für die Einhaltung der im Artikel 5 DSGVO aufgeführten Rechtsgrundsätze

- Rechtmäßigkeit der Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität
- Vertraulichkeit
- Rechenschaftspflicht

3 ANWENDUNGSBEREICH

Die vorliegende Datenschutzrichtlinie findet Anwendung auf die HiSV sowie deren Niederlassungen und sämtliche Mitarbeiter und Mitglieder der geschäftsführenden Organe.

Die vorliegende Richtlinie findet Anwendung auf die Verarbeitung personenbezogener Daten in Datei- und Ablagesystemen (auch in Papierform). Eine Differenzierung zwischen der automatisierten und nichtautomatisierten Verarbeitung erfolgt in der Regel nicht.

Die Richtlinie gilt für die Verarbeitung personenbezogener Daten für HiSV und ihre Niederlassungen, die ihren Standort innerhalb der EU/ EWR oder eines anderen Landes haben, auf die diese Richtlinie ausgedehnt werden kann.

Die vorliegende Richtlinie kann auf Länder außerhalb der EU/des EWR erstreckt werden. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, findet diese Richtlinie auch auf die Daten juristischer Personen in gleicher Weise Anwendung.

Die Bestimmungen dieser Richtlinie sind für die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG sowie deren Niederlassungen verbindlich, sofern diese im Anwendungsbereich tätig sind.

Neben den geltenden Vorschriften der Europäischen Union und der nationalen Datenschutzgesetze obliegt die Verantwortung für die Einhaltung dieser Richtlinie somit der Geschäftsführung sowie den Mitarbeitern der HiSV.

Abweichende Regelungen dürfen von den Niederlassungen nicht getroffen werden, sofern keine gesetzlichen Anforderungen entgegenstehen und diese Ausnahmen durch den Datenschutzbeauftragten und die Geschäftsführung der Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG schriftlich freigegeben wurden.

4 BEZUG ZU GESETZLICHEN VORGABEN

Die vorliegende Datenschutzrichtlinie stellt keinen Ersatz für geltendes Recht dar. Sofern in nationalen Datenschutzgesetzen oder der EU-DSGVO ein höheres Schutzniveau für personenbezogene Daten festgelegt ist, gehen diese Vorschriften der vorliegenden Richtlinie vor.

Die Richtlinie wird auch zur Anwendung gebracht, wenn auf nationaler Ebene (Drittländer) keine entsprechende Gesetzgebung existiert. Der Umgang in Bezug auf die Anwendung der Datenschutzrichtlinie in Drittländern ist in Abschnitt 16 beschrieben.

Im Falle einer Verletzung der nationalen Rechtsordnung durch die Einhaltung dieser Richtlinie oder der Notwendigkeit der Einführung divergierender Bestimmungen zur genannten Richtlinie ist dies dem Datenschutzbeauftragten zu melden.

Sollten Konflikte zwischen der nationalen Gesetzgebung und der vorliegenden Richtlinie auftreten, ist es Aufgabe des Datenschutzbeauftragten sowie der Geschäftsführung der HiSV mit der zuständigen Niederlassung eine praktische Lösung zu erarbeiten, welche dem Ziel dieser Richtlinie entspricht.

5 DIE PRINZIPIEN FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Alle in Ziffer 5 aufgeführten Pflichten sind für den Betroffenen drittbegünstigend.

5.1 Rechtmäßigkeit

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn sie auf rechtmäßige Weise und nach Treu und Glauben erfolgt. Die Datenverarbeitung muss sich daher auf eine angemessene Rechtsgrundlage stützen, die den jeweiligen Verarbeitungsvorgang erlaubt.

Diese Regelung gilt auch für die Datenverarbeitung zwischen den Niederlassungen der HiSV oder den Schwestergesellschaften der HiSV innerhalb der Howden Deutschland Gruppe.

Die Zugehörigkeit sowohl der übermittelnden als auch der empfangenden Gesellschaft zur Howden Deutschland Gruppe bzw. einer Niederlassung der HiSV begründet jedoch noch keinen Anspruch auf Datenverarbeitung.

Die Verarbeitung personenbezogener Daten ist u.a. gemäß Ziffer 5.2 oder 5.3 zulässig, sofern einer der dort genannten Erlaubnistatbestände gegeben ist. Dies gilt auch für den Fall, dass der Zweck der Verarbeitung personenbezogener Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

5.2 Gesetzliche Rahmenbedingungen Kunden- und Partnerdaten

5.2.1 Verarbeitung von Daten im Kontext vertraglicher Beziehungen

Die Verarbeitung personenbezogener Daten einer betroffenen Person, beispielsweise eines Interessenten, Kunden oder Partners, ist dann zulässig, wenn dies zur Begründung, Durchführung und Beendigung eines Vertrages erforderlich ist.

Dies umfasst, sofern dies im Zusammenhang mit dem Vertragszweck steht, auch die Betreuung des Kunden oder Partners.

Die Verarbeitung personenbezogener Daten vor dem Abschluss eines Vertrags ist zulässig, sofern sie der Erstellung von Angeboten, der Anbahnung des Vertrags oder der Erfüllung sonstiger Anfragen des Interessenten dient, die auf den Abschluss eines Vertrags abzielen.

Während der Anbahnung eines Vertrags darf der Interessent unter Verwendung der Daten kontaktiert werden, die er selbst mitgeteilt hat. Eventuell geäußerte Einschränkungen des Interessenten sind zu berücksichtigen.

5.2.2 Datenverarbeitung zum Zwecke der Werbung

Sofern sich der Betroffene mit einem Auskunftswunsch an HiSV wendet, beispielsweise mit dem Wunsch nach Zusendung von Informationsmaterial, ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Maßnahmen, mit denen Kunden gebunden oder beworben werden sollen, unterliegen weiteren rechtlichen Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbart lässt. Die betroffene Person ist vorab über die Verwendung seiner Daten für Zwecke der Werbung zu informieren.

Falls Daten ausschließlich für Werbezwecke erhoben werden, ist der Betroffene über die Freiwilligkeit der Angabe von Daten für diese Zwecke zu informieren. Im Rahmen der Kommunikation ist eine Einwilligung der betroffenen Person einzuholen.

Hinsichtlich der Einwilligung hat die betroffene Person die Möglichkeit, zwischen verschiedenen Kontaktkanälen, einschließlich elektronischer Kommunikation und Telefonanrufen, zu wählen (siehe Einwilligung, Abschnitt 5.2.3).

Widerspricht die betroffene Person der Verwendung ihrer Daten zu Werbezwecken, ist eine weitere Verwendung ihrer Daten zu Werbezwecken unzulässig. In diesem Fall sind die betreffenden Daten für Werbezwecke einzuschränken oder zu sperren.

Im Übrigen sind die Beschränkungen zu beachten, die sich aus den nationalen Rechtsvorschriften über die Verwendung von Daten zu Werbezwecken ergeben.

5.2.3 Einwilligung in die Verarbeitung personenbezogener Daten

Eine Datenverarbeitung kann auf Basis einer Einwilligung des Betroffenen erfolgen. Vor der Einwilligung ist der Betroffene gemäß dieser Datenschutzrichtlinie zu informieren.

Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. In Ausnahmefällen, beispielsweise bei einer telefonischen Beratung, kann die Einwilligung auch mündlich erteilt werden. Die Erteilung muss dokumentiert werden.

5.2.4 Datenverarbeitung auf Basis einer gesetzlichen Erlaubnis oder Verpflichtung

Unter der Voraussetzung, dass nationale Rechtsvorschriften die Verarbeitung personenbezogener Daten verlangen, voraussetzen oder gestatten, ist ebenfalls eine zulässige Datenverarbeitung gegeben.

Die Art und der Umfang der Datenverarbeitung müssen sich nach den für die gesetzlich zulässige Datenverarbeitung erforderlichen Kriterien richten und diesen entsprechen.

5.2.5 Verarbeitung von Daten auf Grundlage berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann ebenfalls erfolgen, sofern dies zur Durchsetzung eines berechtigten Interesses erforderlich ist.

Berechtigte Interessen lassen sich in der Regel zwei Kategorien zuordnen. Zum einen können sie rechtlicher Natur sein, beispielsweise im Kontext der Durchsetzung offener Forderungen. Zum anderen können sie wirtschaftlicher Natur sein, beispielsweise im Kontext der Vermeidung von Vertragsstörungen.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses ist unzulässig, sofern im Einzelfall die Interessen des Betroffenen am Schutz seiner Daten gegenüber den berechtigten Interessen an der Verarbeitung überwiegen.

Im Rahmen jeder Verarbeitung ist eine Prüfung der schutzwürdigen Interessen erforderlich.

5.3 Rechtsgrundlage Mitarbeiterdaten

5.3.1 Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses

Die Verarbeitung von personenbezogenen Daten, die für die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses erforderlich sind, ist im Rahmen des Arbeitsverhältnisses zulässig.

Im Rahmen der Entscheidungsfindung hinsichtlich der Begründung eines Arbeitsverhältnisses ist die Verarbeitung personenbezogener Daten von Bewerberinnen und Bewerbern zulässig.

Im Falle einer Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in eine weitere Speicherung für einen späteren Auswahlprozess eingewilligt.

Eine Einwilligung ist ebenfalls erforderlich, sofern die Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Mitglieder der Howden Deutschland Gruppe verwendet werden sollen.

Im Rahmen eines bestehenden Beschäftigungsverhältnisses ist die Verarbeitung von Daten stets auf den Zweck des Beschäftigungsverhältnisses zu beschränken, sofern nicht einer der nachfolgend dargestellten Erlaubnistatbestände für die Datenverarbeitung gegeben ist.

Falls im Verlauf der Anbahnung eines Arbeitsverhältnisses oder während eines bestehenden Arbeitsverhältnisses die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich ist, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Die Verarbeitung von personenbezogenen Daten, die im Kontext des Beschäftigungsverhältnisses stehen, jedoch nicht primär der Begründung oder Beendigung des Arbeitsverhältnisses dienen (Mitarbeiterdaten), ist nur zulässig, wenn eine der nachstehenden Rechtsgrundlagen vorliegt.

5.3.2 Datenverarbeitung auf Grundlage gesetzlicher Erlaubnis oder Verpflichtung

Die Verarbeitung von Mitarbeiterdaten ist ebenfalls zulässig, sofern nationale Rechtsvorschriften eine solche Datenverarbeitung verlangen, voraussetzen oder gestatten.

Art und Umfang der Datenverarbeitung müssen sich nach den gesetzlichen Erlaubnistatbeständen richten und für die gesetzlich erlaubte Datenverarbeitung erforderlich sein.

Sofern ein gesetzlicher Handlungsspielraum besteht, sind die schutzwürdigen Interessen des Mitarbeiters zu berücksichtigen.

5.3.3 Kollektivregelung für Datenvereinbarungen

Eine Verarbeitung, die über den Zweck der Vertragserfüllung hinausgeht, ist auch dann zulässig, sofern diese durch eine Kollektivregelung erlaubt ist.

Unter Kollektivregelungen werden Tarifverträge sowie Vereinbarungen zwischen Arbeitgebern und Arbeitnehmervertretungen verstanden, welche im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts getroffen werden.

Die betreffenden Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung beziehen und können im Rahmen des staatlichen Datenschutzrechts ausgestaltet werden.

Die betreffenden Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken. Dabei ist zu berücksichtigen, dass sie im Rahmen der Vorgaben der EU-Vorschriften und nationalen Gesetze gestaltbar sind.

5.3.4 Einwilligung in die Datenverarbeitung

Die Verarbeitung von Mitarbeiterdaten kann auf Basis einer freiwillig abgegebenen Einwilligungserklärung erfolgen. Dabei ist sicherzustellen, dass die Abgabe der Erklärung nicht unter Druck erfolgt und die betroffene Person vor Einwilligung ausreichend über seine Rechte belehrt wurde. Die Nichterteilung einer Einwilligung darf nicht zu Nachteilen für Mitarbeiter führen. Eine nicht freiwillig abgegebene Einwilligung ist unwirksam.

Aus Beweisgründen wird die Einwilligungserklärung grundsätzlich schriftlich oder elektronisch gespeichert. Sofern die Umstände dies ausnahmsweise nicht zulassen, kann die Einwilligung mündlich erteilt werden. Die Erteilung der mündlichen Einwilligung sowie die ausreichende Belehrung, auch mit dieser Datenschutzrichtlinie, ist in jedem Fall ordnungsgemäß zu dokumentieren.

5.3.5 Verarbeitung von Daten auf Grundlage berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann ebenfalls erfolgen, sofern dies zur Verwirklichung eines berechtigten Interesses seitens HiSV erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z. B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z. B. Beschleunigung von Betriebsabläufen, Bewertung von Unternehmen) begründet.

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses ist unzulässig, sofern im Einzelfall ein Anhaltspunkt dafür besteht, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Im Rahmen jeder Verarbeitung ist eine Prüfung vorzunehmen, ob schutzwürdige Interessen des Beschäftigten betroffen sind.

Die Verarbeitung von Mitarbeiterdaten, welche über die Durchführung des Arbeitsverhältnisses hinausgeht, beispielsweise im Rahmen einer Leistungskontrolle, ist nur zulässig, sofern eine gesetzliche Verpflichtung oder ein begründeter Anlass hierfür besteht. Selbst bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme einer kritischen Prüfung unterzogen werden.

Die Durchführung einer Kontrollmaßnahme durch HiSV ist grundsätzlich zulässig, sofern die damit verfolgten Ziele als berechtigt zu bewerten sind. Dazu zählt

beispielsweise die Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln. Allerdings muss im Rahmen einer Interessenabwägung auch das schutzwürdige Interesse des von der Maßnahme betroffenen Mitarbeiters berücksichtigt werden. Eine Kontrollmaßnahme darf demnach nur durchgeführt werden, wenn sie in diesem konkreten Anwendungsfall angemessen ist.

Im Rahmen der Entscheidungsfindung ist das Vorliegen eines berechtigten Interesses der Konzerngesellschaft sowie das Vorhandensein potenziell schutzwürdiger Interessen der Mitarbeitenden zu ermitteln und zu dokumentieren.

Des Weiteren sind gegebenenfalls weitere Anforderungen zu berücksichtigen, die sich aus dem geltenden nationalem Recht ergeben. Dazu zählen beispielsweise Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen.

5.4 Besonders schutzwürdige Daten und deren Verarbeitung

Die Verarbeitung von personenbezogenen Daten, die als besonders schutzwürdig eingestuft werden, ist nur unter bestimmten Voraussetzungen zulässig. Als besonders schutzwürdig werden Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeiten, die Gesundheit oder das Sexualleben einer Person betrachtet.

Darüber hinaus unterliegen Daten, die Straftaten betreffen, häufig besonderen, von staatlichem Recht auferlegten Verarbeitungsbedingungen.

Die Verarbeitung von Daten, die aufgrund ihrer Sensibilität einen besonderen Schutz benötigen, ist nur zulässig, wenn eine gesetzliche Grundlage hierfür besteht. Das heißt, die Verarbeitung ist entweder seitens des Gesetzgebers vorgeschrieben oder erlaubt, zum Beispiel um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben bzw. zu verteidigen oder um Rechten und Pflichten aus dem Arbeits- bzw. Sozialrecht zu entsprechen.

Die Verarbeitung von Daten ist darüber hinaus zulässig, sofern der Betroffene freiwillig und ausdrücklich in die Verarbeitung eingewilligt hat. Dies kann beispielsweise der Fall sein, wenn Daten verarbeitet werden, um ein Angebot zu erstellen, innerhalb einer Vertragsanbahnung oder zur Umsetzung des Vertrages.

Der Datenschutzbeauftragte ist vorab zu informieren, wenn die Verarbeitung besonders schutzwürdiger personenbezogener Daten geplant ist.

5.5 Automatisierte Entscheidungen und Profiling

Eine ausschließlich automatisierte Entscheidung, die für den Betroffenen rechtliche oder ähnlich nachteilige Auswirkungen hat, ist nur zulässig, wenn sie zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. In Einzelfällen kann eine automatisierte

Entscheidung mit einem Profiling verbunden sein, wobei durch die Verarbeitung personenbezogener Daten einzelne Persönlichkeitsmerkmale (beispielsweise die Kreditwürdigkeit von Kunden und Geschäftspartnern oder im Rahmen einer Personalauswahl die Erstellung oder Auswertung von Fähigkeitsprofilen) bewertet werden.

Sofern im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, ist sicherzustellen, dass die automatisierte Verarbeitung bzw. deren Schlussfolgerungen nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiterinnen und Mitarbeiter darstellt.

Generell ist der betroffenen Person sowohl die Tatsache als auch das Ergebnis einer automatisierten Einzelentscheidung mitzuteilen. Zudem ist ihr die Möglichkeit zu einer individuellen Prüfung durch einen Verantwortlichen zu eröffnen.

5.6 Telekommunikation, IT- Infrastruktur und Internet

Die Bereitstellung von Computer, Smartphones, Telefonanlage, E-Mail-Adressen, Intranet und Internet etc. sowie internen sozialen Netzwerken erfolgt primär durch das Unternehmen zur Erfüllung der betrieblichen Aufgabenstellung. Diese stellen Arbeitsmittel und Unternehmensressourcen dar, deren Nutzung im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien zulässig ist.

Eine allgemeine Überwachung der Telefon- und E-Mail-Kommunikation sowie der Intranet- und Internetnutzung findet statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer wurden Schutzmaßnahmen unter anderem an den Übergängen in das Netzwerk implementiert. Die Funktion dieser Schutzmaßnahmen besteht in der Blockierung technisch schädigender Inhalte sowie der Analyse von potentiellen Angriffsmustern.

Die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke wird aus Gründen der Sicherheit und Nachvollziehbarkeit protokolliert.

Die Auswertung personenbezogener Daten ist nur bei konkretem, begründetem Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens zulässig. Dabei ist das Prinzip der Verhältnismäßigkeit zu wahren. Es ist zu berücksichtigen, dass die nationalen Gesetzgebungen Geltung besitzen. Die Auswertungen dienen nicht der Leistungserfassung und werden lediglich nach Rücksprache mit dem Datenschutzbeauftragten sowie der Geschäftsführung durch mehrere Personen durchgeführt.

5.7 Informationsverpflichtungen und Transparenz

Die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG ist dazu verpflichtet, die Betroffenen über die Zwecke und Umstände der Verarbeitung ihrer personenbezogenen Daten gemäß Artikel 13 und 14 DSGVO zu informieren. Die Informationen sind in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie in einer klaren und einfachen Sprache zu vermitteln.

Es ist sicherzustellen, dass die Vorgaben des Datenschutzes jederzeit Beachtung finden. Die vorliegende Information ist daher grundsätzlich zum Zeitpunkt der ersten Erhebung der personenbezogenen Daten zu vermitteln.

Die Information ist grundsätzlich zum Zeitpunkt der ersten Erhebung der personenbezogenen Daten zu erteilen. Im Falle der Weitergabe der personenbezogenen Daten durch HiSV an einen Dritten ist die Information den Betroffenen in angemessener Frist nach Erlangung der Daten durch den Dritten mitzuteilen.

Sofern die betroffene Person bereits über die relevanten Informationen verfügt, die Erteilung dieser Informationen sich als unmöglich erweist oder der Aufwand zur Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde, ist eine weitergehende Informationspflicht nicht gegeben. Sollte einer der Ausnahmen zur Anwendung kommen, ist dies schriftlich oder elektronisch zu dokumentieren.

5.8 Zweckbindung

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn sie für den Zweck erfolgt, der vor der Datenerhebung definiert wurde. Eine nachträgliche Änderung des Verarbeitungszwecks ist nur unter der Voraussetzung zulässig, dass die Verarbeitung mit den Zwecken vereinbar ist, für die die personenbezogenen Daten ursprünglich erhoben wurden.

5.9 Datenminimierung

Die Verarbeitung personenbezogener Daten hat in einer Weise zu erfolgen, die sowohl eine quantitative als auch eine qualitative Beschränkung gewährleistet. Diese Beschränkung soll sicherzustellen, dass die Daten lediglich in einem Umfang verarbeitet werden, der für die Erreichung der festgelegten Zwecke notwendig ist.

Dieser Aspekt ist bereits bei der Konzeption der Datenerhebung zu berücksichtigen. Sofern der Zweck dies zulässt und der Aufwand in einem angemessenen Verhältnis zu dem verfolgten Ziel steht, sollte die Verwendung anonymisierter oder statistischer Daten in Betracht gezogen werden.

6 RICHTIGKEIT DER DATEN

Die vorgehaltenen personenbezogenen Daten müssen sachlich richtig und aktuell sein. HiSV ist verpflichtet, angemessene Maßnahmen zu ergreifen, um sicherzustellen, dass falsche oder unvollständige Daten gelöscht, korrigiert, ergänzt oder aktualisiert werden.

6.1 Privacy by Design & Default

Das Prinzip „Privacy by Design“ sieht vor, dass HiSV nach dem Stand der Technik interne Strategien festlegt und alle erforderlichen Maßnahmen ergreift, um die Datenschutzprinzipien von Anfang an in die Spezifikation und Architektur von Geschäftsmodellen und Prozessen sowie von IT-Systemen für den Zweck der Datenverarbeitung zu berücksichtigen oder zu integrieren. Dies erfolgt unter Berücksichtigung der Datenschutzprinzipien, welche als grundlegende Elemente bereits in der Konzeptions- und Designphase zu Beachtung gefunden haben.

Der Grundsatz „Privacy by Design“ besagt, dass die Verfahren und Systeme zur Verarbeitung personenbezogener Daten so gestaltet sein müssen, dass ihre initialen Einstellungen auf die für die Erfüllung des Zwecks erforderliche Datenverarbeitung beschränkt sind (Prinzip „Privacy by Default“). Dies umfasst sowohl den Verarbeitungsumfang, die Speicherdauer als auch die Zugänglichkeit.

Weitere Maßnahmen können in der möglichst zeitnahen Pseudonymisierung oder Anonymisierung personenbezogener Daten, der Schaffung von Transparenz hinsichtlich der Funktionen und der Verarbeitung personenbezogener Daten, der Gewährleistung von Entscheidungsfreiheit des Betroffenen bezüglich der Verarbeitung seiner personenbezogenen Daten sowie der Ermöglichung der Entwicklung und kontinuierlichen Verbesserung von Sicherheitsfunktionen durch den Betreiber von Verfahren oder Systemen bestehen.

Die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG implementiert für den gesamten Lebenszyklus ihrer Verarbeitungsprozesse geeignete technische und organisatorische Maßnahmen, um die Einhaltung der genannten Grundsätze zu gewährleisten. Diese Maßnahmen werden über den gesamten Lebenszyklus aufrechterhalten und dokumentiert.

6.2 Einschränkungen der Verarbeitung und Löschung

Die Speicherung und Verarbeitung von personenbezogenem Daten ist lediglich so lange zulässig, wie es für den jeweils damit verfolgten Zweck erforderlich ist. Dies bedeutet, dass eine Löschung der Daten erfolgen muss, sobald der Zweck ihrer Verarbeitung erfüllt ist oder die Notwendigen Erlaubnistatbestände anderweitig erloschen sind.

Bestehen gesetzliche Aufbewahrungspflichten und eine Speicherung der Daten muss weiterhin erfolgen, ist eine Einschränkung der Verarbeitung oder eine Anonymisierung der Daten umzusetzen.

Die für die einzelnen Verfahren Verantwortlichen haben sicherzustellen, dass die Lösch- und Anonymisierungsroutinen für ihre Verfahren umgesetzt und ggf. schriftlich oder elektronisch dokumentiert werden.

6.3 Sicherheit der Daten und Verarbeitungsprozesse

Es ist sicherzustellen, dass personenbezogene Daten, unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt, vor dem Zugriff durch Unbefugte, einer unrechtmäßigen Verarbeitung oder Weitergabe sowie vor einem versehentlichen Verlust, einer Veränderung oder Zerstörung geschützt werden.

Vor der Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme und einhergehenden Prozessen, ist eine Definition und Umsetzung technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten erforderlich. Diese Maßnahmen müssen auf dem aktuellen Stand der Technik, den Risiken der Verarbeitung und dem Schutzbedarf der Daten basieren.

Im Rahmen der Datenschutz-Folgenabschätzung und des Verfahrensverzeichnisses sind die datenschutzrelevanten technischen und organisatorischen Maßnahmen von den Verantwortlichen zu dokumentieren.

Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten stellen einen integralen Bestandteil des unternehmensweiten Informationssicherheits- und Datenschutz-Managements dar.

Die kontinuierliche Anpassung an technische Entwicklungen, organisatorische Veränderungen sowie gesetzliche Neuerungen und die Berücksichtigung der Bedrohungslage für IT-Infrastrukturen und Datenverarbeitung sind unerlässlich.

Um die Erfüllung dieser Anforderungen zu gewährleisten, kooperiert HiSV mit internen und externen, interdisziplinär arbeitenden Expertinnen und Experten. In gemeinsamer Arbeit werden die implementierten Maßnahmen und Prozesse kontinuierlich weiterentwickelt.

6.4 Übermittlung personenbezogener Daten

Die Übermittlung von personenbezogenen Daten an Empfänger außerhalb von HiSV oder an Empfänger innerhalb der Howden Gruppe unterliegt den in Ziffer 5 dargelegten Zulässigkeitsvoraussetzungen für die Verarbeitung personenbezogener Daten. Der Empfänger der Daten ist zu verpflichten, diese nur zu festgelegten Zwecken zu verwenden.

Im Falle einer grenzüberschreitenden Übermittlung personenbezogener Daten (einschließlich der Gewährung des Zugriffs aus einem anderen Land) sind die einschlägigen nationalen Anforderungen für die Weitergabe personenbezogener Daten ins Ausland zu erfüllen.

Die Datenübertragung innerhalb des EWR ist rechtlich genehmigungsfrei, da das Schutzniveau für die Datenübermittlung in diesen Ländern einheitlich geregelt ist.

Eine Verarbeitung personenbezogener Daten aus der EU/dem EWR in einem Drittland außerhalb des Unternehmens ist jedoch nur zulässig, wenn der Empfänger nachweislich über einen Datenschutzstandard verfügt, der dieser Richtlinie entspricht. Als geeignete Instrumente kommen in Betracht:

6.4.1 Vereinbarung über EU-Standardvertragsklauseln 2021

Im Falle der Übermittlung personenbezogener Daten an nicht-europäische Drittländer ist seitens HiSV eine geeignete Rechtsgrundlage gemäß der Datenschutzgrundverordnung (DSGVO) für den Datentransfer nachzuweisen. Zusätzlich muss sichergestellt werden, dass der Empfänger der Daten ein angemessenes Schutzniveau gewährleistet.

Die EU-Standardvertragsklauseln stellen Musterverträge der Europäischen Kommission dar, welche beide Vertragsparteien zur Einhaltung eines mit der EU vergleichbaren Datenschutzniveaus verpflichten.

Die EU-Kommission evaluiert, ob in Drittländern außerhalb Europas ein angemessenes Schutzniveau gewährleistet ist. Sofern ein angemessener Schutz der Daten gewährleistet ist, erfolgt seitens der Kommission die Erteilung eines Angemessenheitsbeschlusses.

Die Genehmigungsfreiheit bei der Verwendung der Standardvertragsklauseln findet lediglich Anwendung, sofern diese ohne Modifikationen verwendet werden. Diese Regelung findet jedoch keine Anwendung auf die Auswahl eines Moduls oder die Ergänzung oder Aktualisierung von Informationen in der Anlage.

Des Weiteren besteht für die Vertragsparteien die Möglichkeit, die Standardvertragsklauseln in einen umfassenderen Vertrag zu integrieren. Sofern jedoch weitere Klauseln oder zusätzliche Garantien in den Vertrag aufgenommen werden, dürfen diese weder unmittelbar noch mittelbar im Widerspruch zu den Standardvertragsklauseln stehen, noch dürfen sie die Grundrechte oder Grundfreiheiten der betroffenen Personen beschneiden.

6.4.2 EU akkreditierten Zertifizierungssystem zur Datenübermittlung

Die Zertifizierung stellt ein Instrument der DSGVO (Art. 42, 43) dar, durch welches die Einhaltung der Datenschutzbestimmungen in zuverlässiger Weise nachgewiesen werden soll. Ein genehmigter Zertifizierungsmechanismus kann, durch seine rechtsverbindlichen und durchsetzbaren Verpflichtungen zur Einhaltung der Garantien einschließlich der Betroffenenrechte (Art. 46 Abs. 2 lit. f, 42 Abs. 2 DSGVO), als adäquate Gewährleistung dafür dienen, dass bei einer Datenübermittlung in ein Drittland hinlänglicher Schutz für personenbezogene Daten gewährleistet ist.

6.4.3 Anerkennung verbindlicher Unternehmensregelungen (BCR)

Die Übermittlung von Daten in Drittländer ohne angemessenes Datenschutzniveau kann auf Grundlage verbindlicher interner Datenschutzvorschriften, sogenannter Binding Corporate Rules (BCR), erfolgen, sofern den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. Die BCR müssen darüber hinaus von einer zuständigen Aufsichtsbehörde genehmigt worden sein. Folglich unterliegen konkrete Übermittlungen, für die die BCR gelten, keiner gesonderten Genehmigung.

BCR betreffen Unternehmensgruppen oder Gruppen von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben. Eine Unternehmensgruppe ist gemäß Art. 4 Nr. 19 DS-GVO eine Gruppe, die aus einem herrschenden Unternehmen und von diesem abhängigen Unternehmen besteht. Die erforderlichen Mindestinhalte für BCR sind in Art. 47 DS-GVO geregelt.

Die BCR können in zwei Typen eingesetzt werden:

Vorschriften für Verantwortliche: Controller BCR (BCR-C)

Diese Vorschriften gelten für Daten, die Verantwortliche in Ländern der EU an andere Verantwortliche oder Auftragsverarbeiter außerhalb der EU schicken. Dabei gehören die beteiligten Unternehmen alle zu einer Gruppe.

Dieses Instrument ist für Unternehmensgruppen oder Gruppen von Unternehmen geeignet, in denen viele Daten ausgetauscht werden. Die Unternehmen erstellen Regeln zum Datenschutz für alle Personen, deren Daten im Konzern verarbeitet werden. Diese Regeln können sich auch nur auf bestimmte Bereiche beschränken, zum Beispiel auf die Verarbeitung von Personaldaten.

Vorschriften für Auftragsverarbeiter: Processor BCR (BCR-P)

Diese Regeln gelten für Auftragsverarbeiter. Sie betreffen Daten, die von einem Verantwortlichen, der kein Mitglied der Gruppe ist, erhalten werden und anschließend von den Mitgliedern der Gruppe als Auftragsverarbeiter und/oder Unterauftragsverarbeiter verarbeitet werden. Das kann zum Beispiel bei der Auslagerung von IT-Dienstleistungen passieren. Man kann diese Vorschriften auch "BCR für Daten Dritter" nennen.

6.4.4 Übermittlung an Behörden

Die Übermittlung personenbezogener Daten an eine Behörde ist nur unter der Voraussetzung zulässig, dass sie nicht massenhaft, unverhältnismäßig oder undifferenziert erfolgt. Im Falle von Konflikten zwischen diesen Vorgaben und den behördlichen Bestimmungen muss der Datenschutzbeauftragte in Zusammenarbeit mit der Geschäftsleitung eine praktikable Lösung finden, die dem Zweck dieser Richtlinie entspricht.

7 DATENSCHUTZ- FOLGEABSCHÄTZUNG

Im Rahmen der Einführung neuer Verarbeitungsvorgänge sowie bei einer wesentlichen Änderung bestehender, bereits geprüfter Verarbeitungsvorgänge erfolgt durch HiSV bzw. des Datenschutzbeauftragten eine vorangehende Analyse, ob die Verarbeitung ein signifikantes Risiko für die Privatsphäre der Betroffenen birgt.

Dies gilt insbesondere im Kontext der Verwendung neuer Technologien. In diesem Kontext ist insbesondere die Art, der Umfang, der Kontext sowie der Zweck der Datenverarbeitung zu berücksichtigen.

Im Rahmen dieser Risikoanalyse erfolgt durch den Datenschutzbeauftragten eine Bewertung der Auswirkungen der geplanten Verarbeitungen auf den Schutz personenbezogener Daten (Datenschutz-Folgenabschätzung). Sofern nach der Datenschutz-Folgenabschätzung und trotz der Anwendung geeigneter Maßnahmen zur Risikominderung ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht, aber der Verarbeitungsprozess zwingend für HiSV ist, wird nach Rücksprache mit der Geschäftsführung die zuständige Datenschutzaufsichtsbehörde durch den Datenschutzbeauftragten konsultiert.

8 VERFAHRENSVERZEICHNIS

HiSV ist dazu verpflichtet, die Verfahren, in denen personenbezogene Daten verarbeitet werden, in einem Verzeichnis zu dokumentieren. Dieses Verzeichnis muss in schriftlicher oder elektronischer Form vorliegen bzw. geführt werden. Auf Anfrage ist es der zuständigen Datenschutzaufsichtsbehörde zur Verfügung zu stellen.

9 AUFTRAGSVERARBEITUNG

Der Begriff der Auftragsverarbeitung umfasst die Verarbeitung personenbezogener Daten im Namen und nach Weisung des Auftraggebers durch einen Dienstleister. Dabei ist zwischen dem Dienstleister und dem Auftraggeber eine schriftliche Vereinbarung über die Auftragsverarbeitung zu schließen, welche den geltenden gesetzlichen Anforderungen genügt. Dabei behält der Auftraggeber die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung.

Die Bestimmungen der Ziffer 8.2 finden ebenfalls Anwendung bei Auftragnehmern, die Mitglieder der Howden Deutschland Gruppe sind.

9.1 Vorgaben für den Auftraggeber

Im Rahmen der Beauftragung zur Verarbeitung personenbezogener Daten sind die nachfolgenden Vorgaben zu berücksichtigen, wobei HiSV als Auftraggeber die Umsetzung gemäß den folgenden Anforderungen sicherzustellen hat.

Bei der Auswahl des Auftragnehmers ist darauf zu achten, dass dieser über die erforderliche Eignung verfügt, um die Anforderungen an die technischen und organisatorischen Schutzmaßnahmen zu gewährleisten.

Zudem sind die vom Datenschutzbeauftragten bereitgestellten Vertragsstandards zu berücksichtigen.

Der Auftrag zur Verarbeitung durch externe Dienstleister muss in Schrift- oder in elektronischer Form erteilt werden. Zusätzlich sind die Weisungen des Auftraggebers zur Datenverarbeitung sowie die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

Vor Beginn der Datenverarbeitung obliegt es dem Auftraggeber, sich durch geeignete Maßnahmen zu vergewissern, dass der Auftragnehmer die in diesem Kontext genannten Pflichten erfüllt. Ein Auftragnehmer kann die Einhaltung der Datenschutzanforderungen insbesondere durch eine entsprechende Zertifizierung eines adäquaten Informationssicherheitssystems nachweisen. Je nach Risiko der Datenverarbeitung sind während der Vertragslaufzeit regelmäßige Wiederholungen solcher Prüfungen erforderlich und die Ergebnisse zu dokumentieren.

9.2 Anforderungen an Auftragnehmer aus der Howden Gruppe

Auch Auftragnehmer innerhalb der Howden Gruppe dürfen personenbezogene Daten nur im Rahmen der DSGVO und nach Weisung durch HiSV verarbeiten.

Die Beauftragung anderer Schwester- oder Konzerngesellschaften oder Dritter, auch Unterauftragnehmer genannt, zwecks Verarbeitung personenbezogener Daten im eigenen (Unter-) Auftrag durch den Auftragnehmer bedarf der vorherigen Prüfung und Zustimmung der Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG.

Die Zustimmung erfolgt ausschließlich unter der Voraussetzung, dass der Auftragnehmer den Unterauftragnehmer vertraglich oder in einer vergleichbar rechtsverbindlichen Weise dazu verpflichtet, die gleichen Datenschutzpflichten zu erfüllen, die dem Auftragnehmer gemäß dieser Richtlinie gegenüber der HiSV und den Betroffenen obliegen. Zudem muss der Auftragnehmer zusichern, dass angemessene technische und organisatorische Schutzmaßnahmen getroffen werden.

Die Ausgestaltung der Zustimmung sowie die Informationspflichten bei Modifikationen im Rahmen des Unterauftragsverhältnisses sind im Dienstleistungsvertrag zu definieren.

Die Auftragnehmer sind dazu verpflichtet, HiSV als Auftraggeber angemessen bei der Einhaltung der für diesen geltenden Datenschutzbestimmungen zu unterstützen. Dies umfasst insbesondere die Bereitstellung aller für den Nachweis dieser Einhaltung erforderlichen Informationen. Dies betrifft insbesondere die Wahrung der folgenden Aspekte:

Die allgemeinen Grundsätze für die Verarbeitung (vgl. Ziffer 5), die Betroffenenrechte (vgl. Ziffer 10), die Meldepflichten des Auftraggebers (vgl. Ziffer 12), die Bestimmungen für Auftraggeber und Auftragnehmer (vgl. Ziffer 8) sowie die Handhabung von Anfragen und Untersuchungen von Aufsichtsbehörden sind ebenfalls zu berücksichtigen.

Sofern anwendbare Normen oder Rechtsbestimmungen dem Auftragnehmer eine weisungswidrige Verarbeitung vorschreiben oder ihn daran hindern, seinen Verpflichtungen aus dieser Richtlinie oder aus der Vereinbarung über die Auftragsverarbeitung nachzukommen, ist der Auftragnehmer verpflichtet, dies HiSV unverzüglich mitzuteilen, es sei denn, die betreffende Rechtsbestimmung untersagt eine entsprechende Mitteilung.

Diese Regelung findet ebenfalls Anwendung, sofern der Auftragnehmer aus anderen Gründen nicht in der Lage ist, die Weisungen seines Auftraggebers zu befolgen. In diesem Fall ist der Auftraggeber berechtigt, die Datenübermittlung auszusetzen und/oder den Auftragsverarbeitungsvertrag zu kündigen.

Jeder Auftragnehmer ist verpflichtet, den Auftraggeber über alle rechtsverbindliche Aufforderung einer Behörde zur Offenlegung personenbezogener Daten zu unterrichten, sofern dies nicht aus anderen Gründen untersagt ist.

Nach Beendigung der Leistungserbringung hat der Auftragnehmer alle von dem Auftraggeber überlassenen personenbezogenen Daten entweder zu löschen oder zurückzugeben. Die Wahl, welche der beiden Optionen vom Auftragnehmer zu erfüllen ist, obliegt dem Auftraggeber.

Die Auftragnehmer sind dazu verpflichtet, ihren Auftraggeber unverzüglich über geltend gemachte Ansprüche, Forderungen oder Beschwerden von Betroffenen in Kenntnis zu setzen.

Auch gruppeninterne Auftraggeber sind dazu verpflichtet, sicherzustellen, dass externe Auftragnehmer die vorstehenden Regelungen einhalten.

Die besonderen Pflichten des Auftragnehmers gegenüber dem Auftraggeber haben eine drittbegünstigende Wirkung.

9.3 Anforderungen an übrige Auftragnehmer

Die Verarbeitung personenbezogener Daten durch den Auftragnehmer hat ausschließlich in Übereinstimmung mit den Weisungen von HiSV als Auftraggebers zu erfolgen.

Die Beauftragung von Dritten, sogenannten Unterauftragnehmern, zur Verarbeitung personenbezogener Daten im eigenen Auftrag durch den Auftragnehmer ist nur mit vorherigem Einverständnis des Auftraggebers zulässig.

Eine Zustimmung zur Beauftragung von Dritten wird lediglich erteilt, sofern der Auftragnehmer dem Unterauftragnehmer – auf vertraglicher oder vergleichbarer Basis – die gleichen Datenschutzverpflichtungen auferlegt, welche ihm gemäß dieser Richtlinie gegenüber HiSV und den Betroffenen obliegen. Zudem müssen angemessene technische und organisatorische Schutzmaßnahmen gewährleistet werden.

Die Ausgestaltung der Zustimmung sowie die Informationspflichten bei Modifikationen im Rahmen des Unterauftragsverhältnisses sind im Dienstleistungsvertrag zu definieren.

Die Auftragnehmer sind dazu verpflichtet, den HiSV als Auftraggeber angemessen bei der Einhaltung der für diesen geltenden Datenschutzbestimmungen zu unterstützen. Dies umfasst insbesondere die Bereitstellung aller für den Nachweis dieser Einhaltung erforderlichen Informationen.

Die allgemeinen Grundsätze für die Verarbeitung (vgl. Ziffer 5), die Betroffenenrechte (vgl. Ziffer 10), die Meldepflichten des Auftraggebers (vgl. Ziffer 12), die Bestimmungen für Auftraggeber und Auftragnehmer (vgl. Ziffer 8) sowie die Handhabung von Anfragen und Untersuchungen von Aufsichtsbehörden sind ebenfalls zu berücksichtigen.

Sofern anwendbare Normen oder Rechtsbestimmungen dem Auftragnehmer eine weisungswidrige Verarbeitung vorschreiben oder ihn daran hindern, seinen Verpflichtungen aus dieser Richtlinie oder aus der Vereinbarung über die Auftragsverarbeitung nachzukommen, ist der Auftragnehmer verpflichtet, dies HiSV unverzüglich mitzuteilen, es sei denn, die betreffende Rechtsbestimmung untersagt eine entsprechende Mitteilung.

Jeder Auftragnehmer ist verpflichtet, den Auftraggeber über alle rechtsverbindliche Aufforderung einer Behörde zur Offenlegung personenbezogener Daten zu unterrichten, sofern dies nicht aus anderen Gründen untersagt ist.

Nach Beendigung der Leistungserbringung hat der Auftragnehmer alle von dem Auftraggeber überlassenen personenbezogenen Daten entweder zu löschen oder zurückzugeben. Die Wahl, welche der beiden Optionen vom Auftragnehmer zu erfüllen ist, obliegt dem Auftraggeber.

Die Auftragnehmer sind dazu verpflichtet, ihren Auftraggeber unverzüglich über geltend gemachte Ansprüche, Forderungen oder Beschwerden von Betroffenen in Kenntnis zu setzen.

Die spezifischen Pflichten des Auftragsnehmers gegenüber dem Auftraggeber sind für den Betroffenen drittbegünstigend.

10 DURCHSETZBARE RECHTE FÜR BETROFFENE PERSONEN

Alle in Ziffer 9 aufgeführten Rechte der Betroffenen sowie die Pflichten von HiSV sind für den Betroffenen drittbegünstigend ausgestaltet.

Die Anfragen und Beschwerden, die gemäß dieser Ziffer 9 eingereicht werden, müssen innerhalb eines Monats geprüft und bei Erfordernis beantwortet werden. Unter Berücksichtigung der Komplexität sowie der Anzahl der Anträge kann dieser Zeitraum von einem Monat um maximal zwei weitere Monate verlängert werden. Über diese Verlängerung ist die betroffene Person entsprechend zu informieren.

10.1 Rechte der betroffenen Person

Eine betroffene Person in der EU/EWR hat gegenüber HiSV oder – sofern HiSV als Auftragnehmer tätig ist – gegenüber dem Auftraggeber folgende Rechte, wie sie in den näheren Einzelheiten des EU-Rechts festgelegt sind:

- das Recht auf Information über die Umstände der Verarbeitung personenbezogener Daten ist zu gewährleisten. Dabei sind die Vorgaben des EU-Datenschutzbeauftragten zu berücksichtigen.
- die Ausübung des Rechts auf Auskunft beinhaltet die Möglichkeit, sich über die Art und Weise der Verarbeitung personenbezogener Daten sowie über die dem Betroffenen zustehenden Rechte zu informieren. Insofern in den jeweiligen arbeitsrechtlichen Bestimmungen spezifische Einsichtsrechte in Unterlagen des Arbeitgebers vorgesehen sind – als Beispiel sei hier die Personalakte genannt –, bleiben diese unberührt. Sofern dies seitens des bzw. der Betroffenen gewünscht wird, besteht die Möglichkeit eine Kopie der personenbezogenen Daten gegen eine angemessene Vergütung zur Verfügung zu stellen. Dies findet jedoch keine Anwendung, wenn dadurch schützenswerte Interessen Dritter beeinträchtigt werden.
- das Recht auf Berichtigung oder Ergänzung personenbezogener Daten besteht, sofern diese unrichtig oder unvollständig sind.
- das Recht auf Einschränkung der Verarbeitung personenbezogener Daten kann seitens des Betroffenen geltend gemacht werden, sofern die Richtigkeit der Daten von ihm bestritten wird, deren Verarbeitung durch das Unternehmen nicht länger erforderlich ist oder der Betroffene die Daten noch für die Wahrnehmung seiner Rechtsansprüche benötigt. Des weiteren hat der Betroffene das Recht, von dem Unternehmen zu verlangen, dass die Verarbeitung seiner Daten eingeschränkt wird. Dies

ist insbesondere dann der Fall, wenn das Unternehmen die Daten löschen müsste oder einen Widerspruch des Betroffenen prüft.

- das Recht auf Löschung der Daten besteht, sofern die Einwilligung widerrufen wird oder die Rechtsgrundlage für die Verarbeitung der Daten nicht länger gegeben ist. Die Löschung der Daten muss ebenfalls erfolgen, wenn der Zweck der Datenverarbeitung durch Ablauf von Fristen (z.B. Aufbewahrungsfristen) oder aus anderen Gründen entfallen ist. Im Falle einer bestehenden Aufbewahrungspflicht sowie entgegenstehender schutzwürdiger Interessen ist eine Löschung nicht zulässig.
- das Recht, die ihn betreffenden und von ihm bereitgestellten, legitim verarbeiteten personenbezogenen Daten in einem gängigen digitalen Format zu erhalten und dieses an einen Dritten zu übermitteln, sofern die Verarbeitung mithilfe automatisierter Verfahren erfolgt und technisch machbar ist.
- das Recht, jederzeit Marketing- und Werbemaßnahmen zu widersprechen, muss gewährleistet werden. Dazu ist ein entsprechendes Einwilligungs- und Widerspruchsprozess zu etablieren. Für diese Zwecke müssen diese Daten gesperrt sein.
- ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten ist zu berücksichtigen, sofern die schutzwürdigen Gründe der betroffenen Person, zum Beispiel seinen Interessen, Rechten und Freiheiten dem berechtigten Interesse an der Verarbeitung durch HiSV überwiegen. Dieses Recht findet jedoch keine Anwendung, sofern eine Rechtsvorschrift die Verarbeitung der Daten vorschreibt. Im Falle eines berechtigten Widerspruchs sind die betreffenden Daten jedoch fristgerecht zu löschen.

Darüber hinaus hat der Betroffene das Recht, seine Rechte auch gegenüber dem Daten importierenden Schwestergesellschaft innerhalb der Howden Gruppe in einem Drittland geltend zu machen.

10.2 Recht auf Beschwerde

Gemäß der EU-Datenschutzgrundverordnung (DSGVO) sind Betroffene dazu berechtigt, eine Beschwerde bei dem Datenschutzbeauftragten von HiSV einzureichen, sofern sie der Ansicht sind, dass gegen die vorliegende Richtlinie verstoßen wurde. Die Beschwerde kann per E-Mail an hisv@vithos-dsgvo.de oder telefonisch (Werkstags zwischen 09.00 Uhr- 16.30 Uhr) unter Tel: +49 231 42788811 eingereicht werden.

Sofern die Beschwerde berechtigt ist, ergreift die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG geeignete Maßnahmen, um die Einhaltung der vorliegenden Richtlinie sicherzustellen, und informiert die betroffene Person über die getroffenen Maßnahmen sowie ihre weiteren Rechte.

Sollte die Entscheidung von HiSV über die Einhaltung der Vorschriften seitens der betroffenen Person nicht akzeptiert werden (oder sollte aus anderen Gründen

eine Unzufriedenheit mit der Handhabung bestehen), besteht die Möglichkeit gegen diese Entscheidung oder dieses Verhalten rechtlich vorzugehen.

In diesem Kontext besteht die Möglichkeit, sich an die zuständige Aufsichtsbehörde zu wenden, wobei insbesondere der gewöhnliche Aufenthaltsort, der Arbeitsplatz oder der Ort des mutmaßlichen Verstoßes zur Bestimmung der Zuständigkeit dienen. Als weitere Handlungsoption kommt die Klageerhebung bei Gericht in Betracht. Weitergehende gesetzliche Rechte und Zuständigkeiten bleiben hiervon unberührt.

11 MELDUNG VON DATENSCHUTZVorfÄLLEN

Im Falle des potenziellen Verstoßes gegen die Maßgaben zur Datensicherheit – im Folgenden kurz Datenschutzvorfall genannt – unterliegt das Unternehmen Untersuchungs-, Informations- und Schadensminderungspflichten. Ein Datenschutzvorfall definiert sich als eine Datenschutzverletzung, wenn eine Verletzung der Datensicherheit vorliegt, welche unmittelbar zu einer Löschung, einer Änderung, einer unbefugten Offenlegung oder einer Nutzung personenbezogener Daten führt.

Sollte sich daraus ein Risiko für die Rechte und Freiheiten natürlicher Personen ableiten, sind entsprechende Ereignisse innerhalb eines Zeitraums von 72 Stunden, nachdem dem Unternehmen die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde mitzuteilen.

Darüber hinaus sind bei einer Datenschutzverletzung, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der Betroffenen zur Folge hat, die Betroffenen über die Datenschutzverletzung zu benachrichtigen.

Auftragnehmer im Sinne von Ziffer 8.2 und 8.3 sind verpflichtet, Datenschutzvorfälle unverzüglich ihrem Auftraggeber zu melden.

Im Falle einer Datenschutzverletzung ist eine entsprechende Dokumentation zu erstellen, welche auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen ist.

12 DATENSCHUTZMANAGEMENT

12.1 Verantwortung der Geschäftsführung

Die Geschäftsleitung ist für die Datenverarbeitung in ihrem Verantwortungsbereich zuständig. Sie ist verpflichtet sicherzustellen, dass die gesetzlichen (z. B. nationale Meldepflichten) und die in dieser Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt.

Die Verantwortung der Geschäftsleitung umfasst die Sicherstellung einer ordnungsgemäßen Datenverarbeitung unter Beachtung des Datenschutzes durch organisatorische, personelle und technische Maßnahmen.

Die Umsetzung der vorgegebenen Richtlinien obliegt den zuständigen Mitarbeitern. Im Falle von Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte und die Geschäftsführung umgehend zu informieren.

12.2 Sensibilisierung

Die Geschäftsführung muss sicherstellen, dass die Mitarbeiter von HiSV, soweit sie ständigen oder regelmäßigen Zugang zu personenbezogenen Daten haben, an der Erhebung von Daten oder an der Entwicklung von Instrumenten zur Verarbeitung personenbezogener Daten beteiligt sind, die Handhabung dieser Richtlinie verstehen und sie einhalten. Neben dieser Richtlinie dienen auch Handlungsvorgaben und regelmäßige Schulungen zum Thema Datenschutz und Informationssicherheit der Umsetzung der genannten Ziele.

12.3 Organisation und Datenschutzbeauftragter

Der Datenschutzbeauftragte ist in seiner Funktion als Datenschutzbeauftragter unabhängig von Weisungen hinsichtlich seiner Aufgabenerfüllung. Der Datenschutzbeauftragte als fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der Datenschutzvorschriften hin. Er ist dafür verantwortlich, dass die nationalen und internationalen Datenschutzbestimmungen eingehalten werden. Dazu zählt auch die Überwachung der Einhaltung als auch die Aktualisierung dieser Richtlinie.

Der Datenschutzbeauftragte ist berechtigt:

- auf die Beachtung der Datenschutzvorschriften und deren Einhaltung hinzuwirken
- Büroräume aus datenschutzrechtlichen Gesichtspunkten zu besichtigen und zu bewerten
- Stellungnahmen innerhalb der Abteilungen einzuholen
- Mitarbeiter über die Einhaltung des Datenschutzes zu belehren
- grob fahrlässige Zuwiderhandlungen gegen datenschutzrechtliche Bestimmungen unverzüglich der Geschäftsführung anzuzeigen

Der Datenschutzbeauftragte unterrichten die Geschäftsleitung zeitnah über Datenschutzrisiken und steht beratend zur Lösungsfindung zur Verfügung.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden.

Der Datenschutzbeauftragte steht somit allen Betroffenen jederzeit zur Verfügung, um Bedenken, Fragen, Informationsanfragen oder Beschwerden in Bezug auf Datenschutz oder Datensicherheit zu besprechen. Auf Wunsch werden Bedenken und Beschwerden vertraulich behandelt.

Die Kontaktdaten des Datenschutzbeauftragten lauten wie folgt:

Vithos IT-Services GbR
-Büro Dortmund-
Oliver Thehos
Martin-Schmeisser-Weg 18
44227 Dortmund

Telefonnummer: +49 231 427888 18
Mail: hisv@vithos-dsgvo.de

12.4 Kontrollmaßnahmen

Die Einhaltung dieser Richtlinie sowie der geltenden Datenschutzgesetze wird innerhalb des Unternehmens fortwährend mittels einer risikobasierten Überprüfung unterzogen. Die Verantwortung hierfür obliegt dem Datenschutzbeauftragten.

12.5 Disziplinarische Maßnahmen

Die Verarbeitung personenbezogener Daten ist in vielen Ländern durch entsprechende Gesetze geregelt, deren Nichtbeachtung zu rechtlichen Konsequenzen führt. Dazu zählen sowohl Ordnungsstrafen als auch zivilrechtliche Ansprüche auf Schadenersatz.

Die Verantwortung für die Einhaltung dieser Richtlinie liegt bei jedem einzelnen Mitarbeiter von HiSV. Verstöße gegen die Datenschutzrichtlinien, die von Mitarbeitern verursacht werden, können zu arbeitsrechtlichen Sanktionen führen. Die Ahndung von Verstößen erfolgt gemäß internen Regelungen.

13 AKTUALISIERUNGEN UND ANPASSUNGEN DER DATENSCHUTZLEITLINIE

In Abstimmung mit dem Datenschutzbeauftragten kann diese Richtlinie jederzeit geändert werden. Sollten Änderungen vorgenommen werden, die wesentliche Auswirkungen auf die Datenschutzrichtlinie haben oder das gewährte Schutzniveau möglicherweise beeinträchtigen, ist die Geschäftsführung umgehend zu informieren.

14 VERÖFFENTLICHUNG DER DATENSCHUTZRICHTLINIE

Für HiSV ist es von essenzieller Bedeutung, dass betroffene Personen leichten Zugang zu dieser Richtlinie haben. Aus diesem Grund ist eine aktuelle Version dieser Richtlinie auf der HiSV- Webseite abrufbar.

Diese Vorgabe ist für betroffene Personen drittbegünstigend.

15 KOOPERATION MIT BEHÖRDEN

Im Falle von Problemen, Anfragen oder sonstigen Verfahren, die sich aus der Verarbeitung personenbezogener Daten sowohl innerhalb der EU/ EWR als auch in Drittländern ergeben, ist HiSV verpflichtet, mit den zuständigen Aufsichtsbehörden zusammenzuarbeiten.

Dies verpflichtet HiSV, rechtskonforme Audits durch die zuständigen Aufsichtsbehörden zu akzeptieren und Anweisungen der Aufsichtsbehörden, die sich aus der Anwendung der DSGVO im Falle von Verarbeitungsprozessen innerhalb der EU/ EWR als auch in Drittländern ergeben oder aus Bestimmungen dieser Richtlinie ergeben, zu befolgen.

Die Bestimmungen der Ziffer 14 über die Zusammenarbeit mit den Behörden sind drittbegünstigend ausgestaltet.

16 HINWEISE ZUM DATENSCHUTZ AUF UNSERER WEBSEITE

16.1 Datenschutz

Auf der HiSV-Webseite informiert Sie die HiSV ausführlich darüber, welche personenbezogene Daten (im Folgenden kurz „Daten“ genannt) bei Ihrem Besuch unseres Internetauftritts erhoben und verarbeitet werden. Weiter erklären wir Ihnen welche Art von Daten wir bei unseren Kunden erheben, verarbeiten und schützen.

Beim Gebrauch spezifischer Begrifflichkeiten wie „Verantwortlicher“ oder „Verarbeitung“ etc. verweisen wir auf die Definitionen der DSGVO (z.B. Artikel 4).

16.2 Verantwortliche Stelle/Diensteanbieter

Verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG) und zugleich Diensteanbieter im Sinne des Digitale-Dienste-Gesetz (DDG) ist die Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG, vgl. Sie dazu das Impressum.

Erwin Himmelseher Assekuranz-Vermittlung GmbH & Co. KG
Theodor-Heuss-Ring 23
D-50668 Köln
Tel: +49 (0)221 888 25 – 100
E-Mail: hisv@himmelseher.com

16.3 Kontaktdaten des Datenschutzbeauftragten

Vithos IT-Services GbR
-Büro Dortmund-
Oliver Thehos
Martin-Schmeisser-Weg 18
44227 Dortmund

Telefonnummer: +49 231 427888 18
Mail: hisv@vithos-dsgvo.de