Datenschutzrichtlinie
Versicherungsmakler Frank Sußmann, Lessingstr. 12, 08491 Netzschkau, nachstehend VMFS genannt

22.5.2018

1. Grundsätze

Der Schutz personenbezogener Daten ist mir ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.
In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben. Außerdem beschreibe ich, mit welchen Maßnahmen ich die Sicherheit der Daten gewährleiste und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben. Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die bei VMFS bestehenden Verantwortlichkeiten.
Die Datenschutzrichtlinie richtet sich an alle Mitarbeiter, Kunden und Geschäftspartner des VMFS.
Alle Mitarbeiter von VMFS sind zur Einhaltung der Datenschutzrichtlinie verpflichtet.
Zur Zeit habe ich nur meine Ehefrau Larisa Sussmann im Rahmen eines Minijobs angestellt. Sie führt nur Reinigungs- und Hilfsarbeiten in meinem Beisein aus und hat somit keinen Zugang zu schützenwerten Daten. Sie kennt auch keinerlei Computerpasswörter.

Dabei gelten folgende Grundsätze – gilt für mich und Angestellte :

- Die DV-Hard- und Software sind für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke findet nicht statt.

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

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

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

2. Der betriebliche Datenschutzbeauftragte/Datenschutzkoordinatoren

2.1 Der VMFS hat nach Maßgabe des Artikels 37 DS-GVO keinen betrieblichen Datenschutzbeauftragten (DSB) bestellt. Bis dato übernimmt der Geschäftsinhaber (GI) die Rolle des Datenschutzkoordinators (DSK).
Die Kontaktdaten des Datenschutzkoordinators sind zu finden unter:

www.frank-susmann.de

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

2.2 Der DSK unterrichtet und berät die Beschäftigten und ggfls. die Geschäftspartner hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.
Im Falle risikoreicher Datenverarbeitungen steht der DSK dem Verantwortlichen beratend bei der Abschätzung des Risikos zur Seite.

2.3 Der DSK berichtet unmittelbar dem Geschäftsführer.

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

2.5 Soweit es sich aufgrund organisatorischer Gegebenheiten (z.B. bei unselbstständigen externen Filialbetrieben) als notwendig erweist, ernennt der GF für die jeweilige Fachabteilung einen Datenschutzkoordinator.
Der Koordinator ist also insoweit ein dem GI fachlich zugewiesener Mitarbeiter zur Einhaltung der für das Unternehmen geltenden Datenschutz-Vorschriften. Er informiert den DSK über vor Ort aufgetretene Datenschutzfragen.
Er erhebt die Angaben über in seinem Zuständigkeitsbereich gesondert eingesetzte Verfahren und gibt die Meldung an den DSK weiter.

2.6 Das Unternehmen hat ein Verzeichnis über alle Verarbeitungsvorgänge zu führen.
In jeder Fachabteilung wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DS-GVO zu dokumentieren.
Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen wird ein externer Datenschutzbeauftragter beratend hinzugezogen. Dem Datenschutzbeauftragten ist eine Kopie des Verfahrensverzeichnisses zu übergeben.
Auf Anfrage stellt das Unternehmen der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Unternehmensleitung ist hierfür der DSK zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

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

2.8 Der DSK berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel.

3. Beschaffung/Hard- und Software

3.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung des Geschäftsinhaber. Bereits bei der Auswahl von Hard-und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.

3.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der DSK rechtzeitig vorab von der anfordernden Stelle zu informieren (siehe hierzu Näheres in Ziff. 5.2). Der DSK berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die Durchführung einer Datenschutz-Folgenabschätzung erfolgt grundsätzlich.

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

3.4 VMFS führt ein Verzeichnis der eingesetzten Hardware und Software der verwendeten Anwendungsprogramme.

3.5 Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. ist GI unverzüglich zu informieren.

4. Verpflichtung / Schulung der Mitarbeiter

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

4.2 Die Verpflichtung erfolgt unter Verwendung des hierzu vorgesehenen Formulars und unter Aushändigung des von dem DSK und GI erstellten Merkblatts.

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

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

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

5. Transparenz der Datenverarbeitung

5.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt

VMFS Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO. Gleiches gilt für Veränderungen. Unabhängig von dieser Meldung ist der DSK bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren (vgl. Ziff. 6.3). Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Internet-Homepage etc.) ist der Erhebungsbogen etc. dem DSK zur Abstimmung vorzulegen.

5.3 Soweit der DSK feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgeabschätzung unterliegt, teilt er dies umgehend mit.
D as Verfahren darf erst nach Zustimmung des GI durchgeführt werden.

5.4 Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DSGVO Gebrauch, so erfolgt die zentrale Bearbeitung durch den DSK. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt. Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld festzulegen.
Ein öffentliches „Jedermann-Verzeichnis" existiert nach der DS-GVO nicht mehr. Ein Großteil der hierin enthaltenen Informationen werden den betroffenen Personen dennoch nach den Art. 13, 14 und 15 zur Verfügung gestellt.

6. Erhebung/Verarbeitung von personenbezogenen Daten

6.1 Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DSGVO zu beachten. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

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

6.3 Vor Einführung neuer Arten von Erhebungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Die im Rahmen der Zweckänderung genutzten Abwägungs-Kriterien sind einzeln zu prüfen.
Die Prüfung ist darüber hinaus auch zu einem ordnungsgemäßen Nachweis zu dokumentieren.
Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

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

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf in Netzwerk, auf mobilen Datenträgern oder Cloudspeichern (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch den DSK.

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

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

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

8. Externe Dienstleister / Auftragsverarbeitung / Wartung

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

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

9. Sicherheit der Verarbeitung

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

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

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

- Arbeitsanweisung zum datenschutzgerechten Versand von Datenträgern und zur Verschlüsselung von Daten
- Arbeitsanweisung zum Passwortverfahren
- Arbeitsanweisung zur Erteilung von Auskünften im Personalbereich
- Arbeitsanweisung zur PC- und Laptop-Nutzung
- Arbeitsanweisung Telearbeit/Home-Office

Diese Maßnahmen treten in Kraft, sobald Mitarbeiter eingestellt werden, die mit personenbezogenen Daten jeglicher Art arbeiten.

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