

DATENSCHUTZRICHTLINIEN

der Frings Solutions Group und aller angebundenen Unternehmen

IHR ANSPRECHPARTNER:

Holger Haardt | Datenschutzbeauftragter der Frings

Tel. +49 (2103) 58 77 -110

E-Mail: datenschutzbeauftragter@frings-solutions.de

Frings Solutions Deutschland GmbH

Kleinhülsen 42 | 40721 Hilden | Deutschland

Tel. +49 (2103) 58 77 -105 | Fax -300

E-Mail: kontakt@frings-solutions.de

Inhalt

Vorwort	03
1.0 Ziel der Datenschutzrichtlinie	04
2.0 Geltungsbereich und Änderung der Datenschutzrichtlinie	04
3.0 Geltung staatlichen Rechts	04
4.0 Prinzipien für die Verarbeitung personenbezogener Daten	04
4.1 Fairness und Rechtmäßigkeit	04
4.2 Zweckbindung	05
4.3 Transparenz	05
4.4 Datenvermeidung und Datensparsamkeit	05
4.5 Löschung	05
4.6 Sachliche Richtigkeit und Datenaktualität	05
4.7 Vertraulichkeit und Datensicherheit	05
5.0 Zulässigkeit der Datenverarbeitung	05
5.1 Kunden- und Partnerdaten	06
5.2 Mitarbeiterdaten	07
6.0 Übermittlung personenbezogener Daten	10
7.0 Auftragsverarbeitung	11
8.0 Rechte des Betroffenen	12
9.0 Vertraulichkeit der Verarbeitung	12
10.0 Sicherheit der Verarbeitung	13
11.0 Datenschutzkontrolle	13
12.0 Datenschutzvorfälle	13
13.0 Verantwortlichkeiten und Sanktionen	13
14.0 Der Beauftragte für den Datenschutz	14
15.0 Begriff-Definitionen	15

Vorwort

Sehr geehrte Damen und Herren,

wir unterstützen mit unserem Wirken in verschiedensten Projekten, im Auftrag unserer Kunden, die Digitalisierung. Das setzt voraus, dass Daten erfasst und verarbeitet werden. Doch egal, ob im Marketing, im Projektmanagement oder im Service, für uns gilt der Grundsatz: Wo Daten gespeichert und verwendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit sichergestellt werden.

Dies gilt für Daten von Kunden, Interessenten und Geschäftspartnern, genauso wie für Mitarbeiterdaten. Denn Datenschutz ist Schutz der Persönlichkeitsrechte. Unser Anspruch ist es, dass die Frings Gruppe nicht nur erfolgreiche Projekte realisiert, sondern auch Standards beim Datenschutz setzt. Deshalb sehen wir es als unsere Pflicht an, als mittelständiges, eigentümergeführtes Unternehmen den gesetzlichen Anforderungen voll zu entsprechen, die mit der Erhebung und Verarbeitung personenbezogener Daten verbunden sind.

Oberste Priorität hat für uns, einen einheitlichen und gültigen Standard beim Umgang mit personenbezogenen Daten sicherzustellen. Denn die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu wahren, ist für uns die Basis für vertrauensvolle Geschäftsbeziehungen mit Ihnen. In unserer Richtlinie zum Datenschutz haben wir strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Geschäftspartnern und Mitarbeitern geregelt.

Diese entspricht den Anforderungen der Europäischen Datenschutzrichtlinie und stellt die Einhaltung der Prinzipien der weltweit geltenden nationalen und internationalen Datenschutzgesetze sicher.

Als Maßstab haben wir sieben Datenschutzgrundsätze festgelegt – darunter Transparenz, Datensparsamkeit und Datensicherheit. Unsere Führungskräfte und Mitarbeiter sind verpflichtet, diese Richtlinie zum Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren. Als Geschäftsführer trage ich dafür Sorge, dass die gesetzlichen Regelungen und Prinzipien zum Datenschutz in der Frings Solutions Group (und allen verbundenen Unternehmen) geachtet werden. Meine Mitarbeiter, unser Datenschutzbeauftragter und ich stehen Ihnen als Ansprechpartner bei Fragen zum Datenschutz und zur Datensicherheit gerne zur Verfügung.

Sven Frings
Geschäftsführer

1.0 Ziel der Datenschutzrichtlinie

Die Frings Solutions Group verpflichtet sich, im Rahmen seiner gesellschaftlichen Verantwortung, zur Einhaltung von Datenschutzrechten. Diese Datenschutzrichtlinie gilt für die gesamte Gruppe und beruht auf akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der Frings Gruppe als Arbeitgeber. Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für Datenübermittlungen zwischen den verbundenen Unternehmen der Frings Solutions Group.

2.0 Geltungsbereich und Änderung der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für alle angebundenen Unternehmen der Frings Solutions Group, d.h. für die Frings Building Solutions GmbH, die Frings Informatic Solutions GmbH, die Axxess Digital Solutions GmbH und die Frings Solutions Deutschland GmbH und alle von ihr abhängigen Gesellschaften sowie verbundenen Unternehmen und deren Mitarbeiter. Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, gilt diese Datenschutzrichtlinie auch in gleicher Weise für Daten juristischer Personen. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie. Die einzelnen Gesellschaften sind nicht berechtigt, von dieser Datenschutzrichtlinie abweichende Regelungen zu treffen. Weitere Richtlinien zum Datenschutz dürfen in Abstimmung mit dem Beauftragten für den Datenschutz dann erstellt werden, wenn dies nach dem jeweiligen nationalen Recht erforderlich ist. Eine Änderung dieser Datenschutzrichtlinie findet in Abstimmung mit dem Beauftragten für den Datenschutz innerhalb des für die Änderung von Richtlinien vorgegebenen Verfahrens statt. Die Änderungen werden den Unternehmen innerhalb des für die Änderung von Richtlinien vorgegebenen Verfahrens unverzüglich gemeldet. Die aktuellste Version der Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf den einzelnen Internetseiten der Frings Solutions Group unter Datenschutz, z.B. www.frings-solutions.de/en/unternehmen/datenschutz.html abgerufen werden.

3.0 Geltung staatlichen Rechts

Diese Datenschutzrichtlinie beinhaltet die weltweit akzeptierten Datenschutzprinzipien, ohne dass bestehendes staatliches Recht ersetzt wird. Sie ergänzt das jeweilige nationale Datenschutzrecht. Das jeweilige staatliche Recht geht vor, wenn es Abweichungen von dieser Datenschutzrichtlinie erfordert oder weitergehende Anforderungen stellt. Die Inhalte dieser Datenschutzrichtlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt. Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen müssen beachtet werden. Jedes Unternehmen der Frings Solutions Group ist für die Einhaltung dieser Datenschutzrichtlinie und der gesetzlichen Verpflichtungen verantwortlich. Hat es Grund zu der Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutzrichtlinie stehen, hat das betroffene Unternehmen unverzüglich den Beauftragten für den Datenschutz zu informieren. Im Falle einer Kollision zwischen nationaler Rechtsvorschrift und der Datenschutzrichtlinie wird die Frings Solutions Group gemeinsam mit dem betroffenen Schwesterunternehmen nach einer praktikablen Lösung im Sinne der Ziele der Datenschutzrichtlinie suchen.

4.0 Prinzipien für die Verarbeitung personenbezogener Daten

4.1. Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

4.2. Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

4.3. Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens Folgendes erkennen können oder entsprechend informiert werden über:

- » Die Identität der verantwortlichen Stelle
- » Den Zweck der Datenverarbeitung
- » Dritte oder Kategorien von Dritten, an welche die Daten gegebenenfalls übermittelt werden

4.4. Datenvermeidung und Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte oder statistische Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

4.5. Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

4.6. Sachliche Richtigkeit und Datenaktualität

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

4.7. Vertraulichkeit und Datensicherheit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

5.0 Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

5.1 Kunden- und Partnerdaten

5.1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Anbahnung/Begründung, zur Durchführung und zur Beendigung eines Geschäftsvorfalles verarbeitet werden. Dies umfasst auch die Akquise des Geschäftspartners, sofern dies im Zusammenhang mit dem geplanten Geschäftsvorfall steht. Im Vorfeld eines Geschäftsvorfalles – also in der Anbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Leads, Verkaufschancen, Angeboten, der Vorbereitung von Geschäftsabschlüssen oder zur Erfüllung sonstiger auf einen Geschäftsabschluss hin gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Geschäftsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten. Für darüber hinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter Punkt 5.1.2 beachtet werden.

5.1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen der Frings Solutions Group (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig. Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher 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, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung des Betroffenen in die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können (Einwilligung siehe Absatz 5.1.3). Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig und sie müssen für diese Zwecke gesperrt werden. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke sind zu beachten.

5.1.3 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß Abschnitt 4, Absatz 4.3 dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss allerdings genau dokumentiert werden.

5.1.4 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

5.1.5 Datenverarbeitung Aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der Frings Solutions Group erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen). Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

5.1.6 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dies gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Beauftragte für den Datenschutz im Vorfeld zu konsultieren.

5.1.7 Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen muss die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden. Zur Vermeidung von Fehlentscheidungen muss eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährleistet werden.

5.1.8 Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und ggf. Cookie-Hinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind. Werden zur Auswertung des Nutzungsverhaltens von Webseiten und Apps Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out). Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

5.2 Mitarbeiterdaten

5.2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbei-

tet werden. Nach 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 auch für eine Verwendung der Daten für weitere Bewerbungsverfahren oder vor der Weitergabe der Bewerbung an andere Konzerngesellschaften erforderlich. Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift. Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen. Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

5.2.2 Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen die schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

5.2.3 Kollektivregelung für Datenverarbeitungen

Geht eine Verarbeitung über den Zweck der Vertragsabwicklung hinaus, so ist sie auch dann zulässig, wenn sie durch eine Kollektivregelung gestattet wird. Kollektivregelungen sind Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

5.2.4 Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben die Umstände dies ausnahmsweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung muss in jedem Fall ordnungsgemäß dokumentiert werden. Bei einer informierten, freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß 4.3 dieser Datenschutzrichtlinie informiert werden.

5.2.5 Datenverarbeitung Aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der Frings Solutions Group erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlich (z.B. Bewertung von Unternehmen) begründet. Eine

Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechnete Interesse des Unternehmens und die möglichen schutzwürdigen Interessen der Mitarbeiter müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem müssen ggf. nach staatlichem Recht bestehende weitere Anforderungen (z.B. Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

5.2.6 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige, personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die verantwortliche Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrechts nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in die Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Konzernbeauftragte für den Datenschutz im Vorfeld zu konsultieren.

5.2.7 Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (z.B. im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein. Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter muss außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

5.2.8 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet und Internet sowie interne soziale Netzwerke werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das jeweils nationale geltende Telekommunikationsrecht zu beachten, soweit diese Anwendung finden. Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das Frings-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der Frings Solutions Group erfolgen. Diese Kontrollen dürfen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips erfolgen. Die jeweiligen nationalen Gesetze sind ebenso zu beachten wie die hierzu bestehenden Konzernregelungen.

6.0 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der Frings Solutions Group oder an Empfänger innerhalb der Frings Solutions Group unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 5. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden. Im Falle einer Datenübermittlung an einen Empfänger außerhalb der Frings Solutions Group muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Eine solche gesetzliche Verpflichtung kann sich aus dem Recht des Sitzlandes der Gesellschaft, welche die Daten übermittelt, ergeben oder das Recht des Sitzlandes der Gesellschaft erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an. Im Falle einer Datenübermittlung von Dritten an Unternehmen der Frings Gruppe muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen. Werden personenbezogene Daten von einer Gesellschaft mit Sitz im Europäischen Wirtschaftsraum an eine Gesellschaft mit Sitz außerhalb des Europäischen Wirtschaftsraums (Drittstaat) übermittelt, so ist die datenimportierende Gesellschaft verpflichtet, bei allen Anfragen der für die datenexportierende Gesellschaft zuständigen Aufsichtsbehörde mit dieser zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die übermittelten Daten zu beachten. Entsprechendes gilt für Datenübermittlungen durch Konzerngesellschaften aus anderen Staaten. Nehmen sie an einem internationalen Zertifizierungssystem für verbindliche Unternehmensregelungen zum Datenschutz teil, müssen sie die dort vorgesehene Kooperation mit den entsprechenden Prüfungsstellen und Behörden sicherstellen. Die Teilnahme an derartigen Zertifizierungssystemen ist mit dem Konzernbeauftragten für den Datenschutz abzustimmen.

Im Fall eines von einem Betroffenen behaupteten Verstoßes gegen diese Datenschutzrichtlinie durch eine datenimportierende Gesellschaft mit Sitz in einem Drittstaat verpflichtet sich die datenexportierende Gesellschaft mit Sitz im Europäischen Wirtschaftsraum, den Betroffenen, dessen Daten im Europäischen Wirtschaftsraum erhoben worden sind, sowohl bei der Sachverhaltsaufklärung zu unterstützen als auch die

Durchsetzung seiner Rechte gemäß dieser Datenschutzrichtlinie gegenüber der datenimportierenden Gesellschaft sicherzustellen. Darüber hinaus ist der Betroffene berechtigt, seine Rechte auch gegenüber der datenexportierenden Gesellschaft geltend zu machen. Bei einem behaupteten Verstoß muss die datenexportierende Gesellschaft gegenüber dem Betroffenen den Nachweis erbringen, dass der datenimportierenden Gesellschaft in einem Drittland bei einer Weiterverarbeitung der erhaltenen Daten ein Verstoß gegen diese Datenschutzrichtlinie nicht zuzurechnen ist. Im Fall einer Übermittlung personenbezogener Daten von einer Gesellschaft mit Sitz im Europäischen Wirtschaftsraum an eine Gesellschaft mit Sitz in einem Drittstaat hat die datenübermittelnde Stelle den Betroffenen, dessen personenbezogene Daten im Europäischen Wirtschaftsraum erhoben worden sind, bei zurechenbaren Verstößen der Gesellschaft mit Sitz in einem Drittstaat gegen diese Datenschutzrichtlinie haftungsrechtlich so zu stellen, als hätte die datenübermittelnde Stelle den Verstoß begangen. Gerichtsstand ist das zuständige Gericht am Sitz der datenexportierenden Stelle.

7.0 Auftragsverarbeitung

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer im Auftrag eines Verantwortlichen personenbezogene Daten verarbeitet. Eine Verarbeitung liegt vor, sofern die entsprechende Begriffsbestimmung im Artikel 4 Absatz 2 DSGVO zutreffend ist. Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines Vertrags. Daher ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb der Frings Gruppe eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind die nachfolgenden Vorgaben einzuhalten; der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

- 7.1 Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
- 7.2 Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
- 7.3 Die vom Beauftragten für den Datenschutz bereitgestellten Vertragsstandards müssen beachtet werden.
- 7.4 Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.
- 7.5. Bei einer grenzüberschreitenden Auftragsverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere darf die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum in einem Drittstaat nur stattfinden, wenn der Auftragnehmer ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:
 - a. Vereinbarung der EU-Standardvertragsklauseln zur Auftragsverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
 - b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.
 - c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

8.0 Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen.

- 8.1. Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind. Falls im Arbeitsverhältnis nach dem jeweiligen Arbeitsrecht weitergehende Einsichtsrechte in Unterlagen des Arbeitgebers (z.B. Personalakte) vorgesehen sind, so bleiben diese unberührt.
- 8.2. Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
- 8.3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
- 8.4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.
- 8.5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
- 8.6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.
- 8.7. Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.
- 8.8. Der Betroffene hat ein Beschwerderecht bei einer Aufsichtsbehörde.

Darüber hinaus kann jeder Betroffene die in den Ziffern III. Abs. 2, IV., V., VI., IX., X, und XIV. Abs. 3 eingeräumten Rechte als Drittbegünstigter geltend machen, wenn ein Unternehmen, das sich zur Einhaltung der Datenschutzrichtlinie verpflichtet hat, deren Vorgaben nicht beachtet und er dadurch in seinen Rechten verletzt ist.

9.0 Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip: Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten. Mitarbeiter dürfen personenbezogene Daten nicht für eigene, private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetzte müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

10.0 Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten (ggf. ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Der verantwortliche Fachbereich muss dazu insbesondere seinen Informationssicherheitsbeauftragten (ISO) und auf jeden Fall den betrieblichen Datenschutzbeauftragten zu Rate ziehen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des gruppenweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

11.0 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Beauftragten für den Datenschutz und weiteren, mit Auditrechten ausgestatteten Unternehmensbereichen oder beauftragten externen Prüfern.

Die Ergebnisse der Datenschutzkontrollen sind dem Beauftragten für den Datenschutz mitzuteilen. Der Geschäftsführer der Frings Solutions Group ist im Rahmen der jeweiligen Berichtspflichten über wesentliche Ergebnisse zu informieren. Auf Antrag werden die Ergebnisse von Datenschutzkontrollen der zuständigen Datenschutzaufsichtsbehörde zur Verfügung gestellt. Die zuständige Datenschutzaufsichtsbehörde kann im Rahmen der ihr nach staatlichem Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Richtlinie durchführen.

12.0 Datenschutzvorfälle

Jeder Mitarbeiter soll seinem jeweiligen Vorgesetzten oder dem Beauftragten für den Datenschutz unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden. Die für die Funktion oder die Einheit verantwortliche Führungskraft ist verpflichtet, den zuständigen Beauftragten für den Datenschutz umgehend über Datenschutzvorfälle zu unterrichten.

In Fällen von:

- » unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- » unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
- » bei Verlust personenbezogener Daten sind die im Unternehmen vorgesehenen Meldungen (Information Security Incident Management) unverzüglich vorzunehmen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

13.0 Verantwortlichkeiten und Sanktionen

Der Geschäftsführer der Gesellschaften ist verantwortlich für die Datenverarbeitung in seinem Verantwortungsbereich. Damit ist er verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe der Führungskräfte, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutz-

kontrollen durch Behörden ist der Beauftragte für den Datenschutz umgehend zu informieren. Die Geschäftsführer sind verpflichtet, den Beauftragten für den Datenschutz in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Beauftragten für den Datenschutz rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Beauftragte für den Datenschutz schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Die Führungskräfte müssen sicherstellen, dass ihre Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder andere Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen. Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtlichen Sanktionen führen.

14.0 Der Beauftragte für den Datenschutz

Der Beauftragte für den Datenschutz als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Der Beauftragte für den Datenschutz wird vom Geschäftsführer der Gesellschaft bestellt. Alle Mitarbeiter unterrichten den Beauftragten für den Datenschutz zeitnah über Datenschutzrisiken. Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Beauftragten für den Datenschutz wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Der betriebliche Datenschutzbeauftragte unterliegt der Schweigepflicht. Die Entscheidungen des Beauftragten für den Datenschutz zur Abhilfe der Datenschutzverletzung sind durch den Geschäftsführer zu berücksichtigen. Anfragen von Aufsichtsbehörden sind immer auch dem Beauftragten für den Datenschutz zur Kenntnis zu bringen.

Der Beauftragte kann wie folgt erreicht werden:

Frings Solutions Deutschland GmbH

Herr Holger Haardt

Beauftragter für den Datenschutz

Kleinhülsen 42, 40721 Hilden

E-Mail: datenschutzbeauftragter@frings-solutions.de

Telefon: +49 (2103) 58 77 -110

15.0 Begriff-Definitionen

- » Ein **angemessenes Datenschutzniveau** von Drittstaaten wird von der EU Kommission dann anerkannt, wenn der Kernbestand der Privatsphäre, so wie er in den Mitgliedstaaten der EU übereinstimmend verstanden wird, im Wesentlichen geschützt wird. Die EU Kommission berücksichtigt bei ihrer Entscheidung alle Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Dies schließt die Beurteilung staatlichen Rechts sowie der jeweiligen geltenden Landesregeln und Sicherheitsmaßnahmen ein.
- » **Anonymisiert** sind **Daten** dann, wenn ein Personenbezug dauerhaft und von niemandem mehr hergestellt werden kann bzw. wenn der Personenbezug nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wiederhergestellt werden könnte.
- » **Besonders schutzwürdige Daten** sind Daten aus denen die rassische und ethnische Herkunft, politische

Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervor gehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet werden.

- » **Betroffener** im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.
- » **Datenschutzvorfälle** sind alle Ereignisse, bei denen der begründete Verdacht besteht, dass personenbezogene Daten rechtswidrig ausgespäht, erhoben, verändert, kopiert, übermittelt oder genutzt wurden. Das kann sich sowohl auf Handlungen durch Dritte als auch Mitarbeiter beziehen.
- » **Dritter** ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
- » **Drittstaaten** im Sinne der Datenschutzrichtlinie sind alle Staaten außerhalb der Europäischen Union/EWR. Ausgenommen sind Staaten, deren Datenschutzniveau von der EU Kommission als angemessen anerkannt worden ist.
- » **Einwilligung** ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.
- » **Erforderlich** ist die Verarbeitung personenbezogener Daten, wenn der zulässige Zweck oder das berechtigte Interesse ohne die jeweiligen personenbezogenen Daten nicht oder nur mit unverhältnismäßig hohem Aufwand zu erreichen ist.
- » Der **Europäische Wirtschaftsraum** (EWR) ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.
- » **Personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
- » Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.
- » **Verarbeitung personenbezogener Daten** ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang zur Erhebung, Speicherung, Organisation, Aufbewahrung, Veränderung, Abfrage, Nutzung, Weitergabe, Übermittlung, Verbreitung oder der Kombination und der Abgleich von Daten. Dazu gehört auch das Entsorgen, Löschen und Sperren von Daten und Datenträgern.
- » **Verantwortliche Stelle** ist diejenige juristisch selbständige Gesellschaft der Frings Gruppe, deren Geschäftsaktivität die jeweilige Verarbeitungsmaßnahme veranlasst.
- » **Verantwortlicher** ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.