Datenschutzleitlinie

- Umgang mit personenbezogenen Daten -

Inhalt

1 Ziel der Datenschutzleitlinie

IDF verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung der Datenschutzrechte. Diese Datenschutzleitlinie gilt europaweit für IDF und beruht auf europaweit akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen sowie das Image von IDF.

Die Datenschutzleitlinie schafft eine der notwendigen Rahmenbedingungen für internationale Datenübermittlungen[1]. Sie gewährleistet das von der Europäischen Datenschutzrichtlinie[2] und den nationalen Gesetzen verlangte angemessene Datenschutzniveau, auch für den grenzüberschreitenden Datenverkehr in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau[3] besteht.

2 Geltungsbereich und Änderung der Datenschutzleitlinie

Diese Datenschutzleitlinie gilt für das Unternehmen IDF und deren Mitarbeiter. Die Datenschutzleitlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten[4].

Anonymisierte[5] Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzleitlinie.

Weitere Richtlinien und Erklärungen zum Datenschutz dürfen in Abstimmung mit dem Geschäftsinhaber dann erstellt werden, wenn dies nach dem jeweiligen nationalen Recht erforderlich ist.

Änderungen der Datenschutzleitlinie dürfen unter Einhaltung der Datenschutzrechte sowie mit Zustimmung des Geschäftsinhabers vorgenommen werden.

Die aktuellste Version der Datenschutzleitlinie kann unter den Datenschutzhinweisen auf der Internetseite von IDF, www.idf-managementsystseme.de, abgerufen werden.

3 Geltung staatlichen Rechts

Diese Datenschutzleitlinie 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 Datenschutzleitlinie erfordert oder weitergehende Anforderungen stellt. Die Inhalte dieser Datenschutzleitlinie sind auch dann zu beachten, wenn es kein entsprechendes staatliches Recht gibt.

Die aufgrund staatlichen Rechts bestehenden Meldepflichten für Datenverarbeitungen werden beachtet. IDF ist für die Einhaltung dieser Datenschutzleitlinie und der gesetzlichen Verpflichtungen verantwortlich.

Hat ein Mitarbeiter Grund zu der Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutzleitlinie stehen, hat dieser Mitarbeiter unverzüglich den Geschäftsinhaber zu informieren. Im Falle einer Kollision zwischen nationaler Rechtsvorschrift und der Datenschutzleitlinie sucht der Geschäftsinhaber, ggf. gemeinsam mit den Mitarbeitern, nach einer praktikablen Lösung im Sinne der Ziele der Datenschutzleitlinie.

---

[1] Siehe 15
[2] Siehe 15
[3] Siehe 15
[4] Siehe 15
[5] Siehe 15

4 Prinzipien für die Verarbeitung personenbezogener Daten

4.1 Rechtmäßigkeit, Treu und Glauben, Transparenz

Bei der Verarbeitung personenbezogener Daten werden die Persönlichkeitsrechte des Betroffenen[6] gewahrt. Personenbezogene Daten werden auf rechtmäßige Weise, nach Treu und Glauben und in einer verständlichen, transparenten und nachvollziehbaren Weise erhoben und verarbeitet.

4.2 Zweckbindung

Die Erhebung personenbezogener Daten erfolgt ausschließlich für festgelegte, eindeutige und legitime Zwecke. Eine Weiterverarbeitung erfolgt nur in einer mit diesen Zwecken zu vereinbarenden Weise. Nachträgliche Änderungen der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.

4.3 Datenminimierung

Personenbezogene Daten werden dem Zweck angemessen erhoben sowie auf das notwendige Maß beschränkt, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Sofern es möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, werden anonymisierte oder statistische Daten verwendet. Personenbezogene Daten werden nur dann für potentielle zukünftige Zwecke gespeichert, wenn dies durch staatliches Recht vorgeschrieben oder erlaubt ist.

4.4 Richtigkeit und Datenaktualität

Personenbezogene Daten werden sachlich richtig, vollständig und, soweit erforderlich, auf dem aktuellen Stand gespeichert. Unrichtige, unvollständige und veraltete Daten werden gelöscht, berichtigt, ergänzt oder aktualisiert.

4.5 Speicherbegrenzung

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich[7] sind, werden gelöscht.

Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, bleiben die Daten weiter gespeichert, bis das schutzwürdige Interesse rechtlich geklärt wurde oder der Geschäftsinhaber den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnte.

4.6 Vertraulichkeit und Datensicherheit

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

5 Zulässigkeit der Datenverarbeitung

Personenbezogene Daten werden nur dann verarbeitet, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Verarbeitung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

[6] Siehe 15
[7] Siehe 15

5.1 Kunden- und Partnerdaten

5.1.1 Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung[8] des Betroffenen stattfinden. Vor der Einwilligung wird der Betroffene gemäß 9.3 dieser Datenschutzleitlinie informiert. Die Einwilligungserklärung erfolgt grundsätzlich schriftlich oder elektronisch und kann unter Umständen auch mündlich erteilt werden, z.B. bei telefonischer Beratung. Die Erteilung wird dokumentiert.

5.1.2 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners werden zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

Im Vorfeld eines Vertrages erfolgt die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteten Wünsche des Interessenten.

Interessenten werden während der Vertragsanbahnung unter Verwendung der durch sie angegebenen Daten kontaktiert. Eventuell vom Interessenten geäußerte Einschränkungen werden beachtet.

Für darüber hinausgehende Werbemaßnahmen werden die folgenden Voraussetzungen unter 5.1.4 beachtet.

5.1.3 Datenverarbeitung aufgrund rechtlicher Verpflichtung

Die Verarbeitung personenbezogener Daten erfolgt auch dann, 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.

5.1.4 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an IDF, 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 wird über die Verwendung seiner Daten für Zwecke der Werbung informiert.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so erfolgt keine weitere Verwendung seiner Daten für diese Zwecke und sie werden für diese Zwecke gesperrt. Darüber hinaus bestehende Beschränkungen einiger Länder bezüglich der Verwendung von Daten für Werbezwecke werden beachtet.

5.1.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten erfolgt auch dann, wenn dies zur Verwirklichung eines berechtigten Interesses von IDF erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung von offenen Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen).

[8] Siehe 15

Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses erfolgt nicht, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen das Interesse an der Verarbeitung überwiegen. Die schutzwürdigen Interessen werden für jede Verarbeitung geprüft.

5.1.6 Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger[9] personenbezogener Daten erfolgt nur dann, 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, wird der Geschäftsinhaber im Vorfeld informiert.

5.1.7 Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (z.B. Kreditwürdigkeit) bewertet werden, bilden keine ausschließliche Grundlage für Entscheidungen. Dem Betroffenen werden die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben. Zur Vermeidung von Fehlentscheidungen werden eine Kontrolle und eine Plausibilitätsprüfung durch einen Mitarbeiter gewährt.

5.1.8 Nutzerdaten und Internet

Werden auf der Webseite personenbezogene Daten erhoben, verarbeitet und genutzt, werden die Betroffenen hierüber in Datenschutzhinweisen und Cookie-Hinweisen informiert. Die Datenschutzhinweise und Cookie-Hinweise sind so integriert, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

5.2 Mitarbeiterdaten

5.2.1 Datenverarbeitung für das Arbeitsverhältnis

Für das Arbeitsverhältnis werden die personenbezogenen Daten verarbeitet, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses werden personenbezogene Daten von Bewerbern verarbeitet. Nach Ablehnung werden die Daten des Bewerbers, unter Berücksichtigung beweisrechtlicher Fristen, gelöscht, 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 erforderlich.

Im bestehenden Arbeitsverhältnis ist die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen, 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[10] erforderlich, werden die jeweiligen nationalen gesetzlichen Anforderungen berücksichtigt. Im Zweifel wird eine Einwilligung des Betroffenen eingeholt.

Die Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, ursprünglich jedoch nicht der Erfüllung des Arbeitsvertrages dienen, erfolgt nur, wenn dafür eine rechtliche Legitimation vorliegt. Dies können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

[9] Siehe 15
[10] Siehe 15

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 sind für die gesetzlich zulässige Datenverarbeitung erforderlich und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, werden die schutzwürdigen Interessen des Mitarbeiters berücksichtigt.

5.2.3 Kollektivregelungen für Datenverarbeitungen

Eine Verarbeitung, die über den Zweck der Vertragsabwicklung hinausgeht, ist 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 erstrecken sich dabei auf den konkreten Zweck der gewünschten Verarbeitung 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 wird aus Beweisgründen grundsätzlich schriftlich oder elektronisch eingeholt.

Die Einwilligung kann unter besonderen Umständen mündlich erteilt werden. Ihre Erteilung wird in jedem Fall ordnungsgemäß dokumentiert.

Gibt der Betroffene freiwillig personenbezogene Daten über sich an, wird eine Einwilligung angenommen, wenn das nationale Recht keine explizite Einwilligung vorschreibt.

Vor der Einwilligung wird der Betroffene gemäß 4.3 dieser Datenschutzleitlinie informiert.

5.2.5 Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten erfolgt auch dann, wenn dies zur Verwirklichung eines berechtigten Interesses seitens IDF 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 erfolgt nicht, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass die schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen wird für jede Verarbeitung geprüft.

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

5.2.6 Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten werden nur unter bestimmten Voraussetzungen verarbeitet. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein.

Daten, die Straftaten betreffen, werden nur unter besonderen, von staatlichem Recht aufgestellten Voraussetzungen verarbeitet. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit IDF ihre Rechte 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, wird der Geschäftsinhaber im Vorfeld informiert.

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), stellt eine solche automatisierte Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen.

Um Fehlentscheidungen zu vermeiden, wird in automatisierten Verfahren gewährleistet, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist.

Dem betroffenen Mitarbeiter werden außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben.

5.2.8 Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen und Internet 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 wird das Fernmeldegeheimnis und das jeweils national geltende Telekommunikationsrecht beachtet, soweit diese Anwendung finden.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Internet-Nutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer sind Schutzmaßnahmen an den Übergängen in das IDF-Netz implementiert, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren.

Aus Gründen der Sicherheit wird die Nutzung der Telefonanlagen, der E-Mail-Adressen und Internets zeitlich befristet protokolliert. Personenbezogene Auswertungen dieser Daten erfolgen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien. Diese Kontrollen erfolgen nur durch ermittelnde Bereiche unter Wahrung des Verhältnismäßigkeitsprinzips. Die jeweiligen nationalen Gesetze werden ebenso beachtet wie die hierzu bestehenden Regelungen von IDF.

6 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb oder innerhalb von IDF unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 5. Der Empfänger der Daten wird darauf verpflichtet, diese nur zu den festgelegten Zwecken zu verwenden.

Im Falle einer Datenübermittlung an einen Empfänger außerhalb von IDF in einem Drittstaat[11] muss dieser ein zu dieser Datenschutzleitlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt.

Im Falle einer internen Datenübermittlung von Dritten wird gewährleistet, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

7 Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen wird mit den externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abgeschlossen. Dabei behält IDF als Auftraggeber 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; IDF stellt ihre Umsetzung sicher.

1. Der Auftragnehmer wird nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen ausgewählt.
2. Der Auftrag wird in Textform zu erteilt. Dabei werden die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers dokumentiert.
3. Die vom Geschäftsinhaber bereitgestellten Vertragsstandards werden beachtet.
4. Der Auftraggeber überzeugt sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung wird die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig wiederholt.
5. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung wird darauf geachtet, die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen. Insbesondere findet die Verarbeitung personenbezogener Daten aus dem Europäischen Wirtschaftsraum[12] in einem Drittstaat nur statt, wenn der Auftragnehmer ein zu dieser Datenschutzleitlinie gleichwertiges Datenschutzniveau nachweist. Geeignete Instrumente können sein:
    a. Vereinbarung der EU-Standardvertragsklauseln zur Auftragsdatenverarbeitung in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern.
    b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus.

[11] Siehe 15
[12] Siehe 15

c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutz-Aufsichtsbehörden.

8 Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung wird umgehend durch IDF bearbeitet und führt für den Betroffenen zu keinerlei Nachteilen.

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.
2. Werden personenbezogene Daten an Dritte übermittelt, wird auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben.
3. Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
4. Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke werden die Daten gesperrt.
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 werden beachtet.
6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das berücksichtigt wird, 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.

9 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 erhalten nur Zugang zu personenbezogenen Daten, 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. Der Geschäftsinhaber unterrichtet seine Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

10 Sicherheit der Verarbeitung

Personenbezogene Daten werden jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen Verlust, Verfälschung oder Zerstörung geschützt. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, werden technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festgelegt und umgesetzt. Diese Maßnahmen orientieren sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten.

Die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten werden kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst.

11 Datenschutzkontrolle

Die Einhaltung der Datenschutzleitlinie und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem Geschäftsinhaber, Qualitätsmanagementbeauftragten und weiteren, mit Auditrechten ausgestatteten Mitarbeitern oder beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen werden dem Geschäftsinhaber mitgeteilt. 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 Datenschutzvorfälle

Jeder Mitarbeiter meldet dem Geschäftsinhaber unverzüglich Fälle von Verstößen gegen diese Datenschutzleitlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle[13]). In Fällen von

» unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,

» unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder

» bei Verlust personenbezogener Daten

werden die im Unternehmen vorgesehenen Meldungen unverzüglich vorgenommen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

13 Verantwortlichkeiten und Sanktionen

Der Geschäftsinhaber ist verantwortlich für die Datenverarbeitung in seinem Verantwortungsbereich. Damit ist er verpflichtet, sicherzustellen, dass die gesetzlichen und die in der Datenschutzleitlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Managementaufgabe des Geschäftsinhabers, 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 Datenschutzkontrollen durch Behörden wird der Geschäftsinhaber umgehend informiert.

[13] Siehe 15

Der Geschäftsinhaber ist Ansprechpartner für den Datenschutz. Er kann Kontrollen durchführen und vertraut die Mitarbeiter mit den Inhalten der Datenschutzleitlinie. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen informieren den Geschäftsinhaber rechtzeitig über neue Verarbeitungen personenbezogener Daten. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, wird der Geschäftsinhaber schon vor Beginn der Verarbeitung beteiligt. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Der Geschäftsinhaber stellt sicher, dass seine 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 Der Geschäftsinhaber

Der Geschäftsinhaber 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.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Geschäftsinhaber wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt.

Anfragen von Aufsichtsbehörden werden immer auch dem Geschäftsinhaber zur Kenntnis gebracht.

15 Definitionen

[1] Datenübermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.

[2] RL 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/law/index_de.htm#richtlinie

[3] 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 Standesregeln und Sicherheitsmaßnahmen ein.

[4] Personenbezogene Daten sind alle Informationen über eine bestimmte oder bestimmbare natürliche Person. Bestimmbar ist eine Person z. B. dann, wenn der Personenbezug durch eine Kombination von Informationen mit auch nur zufällig vorhandenem Zusatzwissen hergestellt werden kann. Die 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.

[5] 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.

[6] Betroffener im Sinne dieser Datenschutzleitlinie ist jede natürliche Person, über die Daten verarbeitet werden. In einigen Ländern können auch juristische Personen Betroffener sein.

[7] 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.

[8] Eine Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.

[9] Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. 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.

[10] Dritter ist jeder außerhalb des Betroffenen und der für die Datenverarbeitung verantwortlichen Stelle. Auftragsdatenverarbeiter sind innerhalb der EU nicht Dritte im Sinne des Datenschutzrechtes, da sie gesetzlich der verantwortlichen Stelle zugeordnet sind.

[11] 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.

[12] Der Europäische Wirtschaftsraum (EWR) ist ein mit der EU assoziierter Wirtschaftsraum, dem Norwegen, Island und Liechtenstein angehören.

[13] 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.