5.1.1 Datenschutzrichtlinie

Ziel

Diese Datenschutzrichtlinie gilt für die IT Manufactory GmbH und beruht auf global akzeptierten Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und das Ansehen der IT Manufactory GmbH als attraktiver Arbeitgeber. Die IT Manufactory GmbH verpflichtet sich im Rahmen Ihrer gesellschaftlichen Verantwortung zur internationalen Einhaltung von Datenschutzrechten. Die Datenschutzrichtlinie gewährleistet das von der Europäischen Datenschutzrichtlinie und den nationalen Gesetzen verlangte angemessene Datenschutzniveau für den grenzüberschreitenden Datenverkehr auch in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

Geltungsbereich

Diese Datenschutzrichtlinie gilt für die IT Manufactory GmbH 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.

Geltung staatlichen Rechts

Diese Datenschutzrichtlinie orientiert sich an den weltweit praktizierten 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. Die IT Manufactory GmbH ist für die Einhaltung dieser Datenschutzrichtlinie und der gesetzlichen Verpflichtungen verantwortlich. Bei Annahme, dass gesetzliche Verpflichtungen im Widerspruch zu den Pflichten aus dieser Datenschutzrichtlinie stehen, muss unverzüglich der Datenschutzbeauftragte darüber informieren werden.

Allgemeine Grundsätze

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.

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.

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.

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.

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 die die Daten ggfs. übermittelt werden.

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 nicht zutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

Löschung

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

Zulässigkeit der Datenverarbeitung

Personenbezogene Daten sind Einzelangaben über persönliche und sachliche Verhältnisse einer bestimmten oder bestimmbaren Person. Darunter fallen Informationen wie z.B. Ihr richtiger Vor- und Nachname, Ihre Anschrift, Ihre Telefon-, Telefax-, Mobilfunknummer, E-Mailadresse oder Ihr Geburtstag und etwaige weitere Daten. Informationen, die nicht direkt mit Ihrer Person in Verbindung gebracht werden, wie z.B. die Anzahl der Nutzer einer Webseite sind dagegen keine personenbezogenen Daten. 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 Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

Kundendaten

Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten oder Kunden dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die

Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages – also in der Vertragsanbahnungsphase – ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten, der Vorbereitung von Kaufanträgen oder zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche des Interessenten erlaubt. Interessenten dürfen während der Vertragsanbahnung unter Verwendung der Daten kontaktiert werden, die sie mitgeteilt haben. Eventuell vom Interessenten geäußerte Einschränkungen sind zu beachten.

Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an die IT Manufactory GmbH (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung der Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß IV.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 dokumentiert werden.

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.

Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der IT Manufactory GmbH 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.

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 Datenschutzbeauftragte im Vorfeld zu informieren.

Nutzerdaten und Internet

Wenn auf Webseiten personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen zu informieren. Die Datenschutzhinweise sind so zu integrieren, dass diese für die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

Mitarbeiterdaten

Datenverarbeitung für das Arbeitsverhältnis

Personenbezogene Daten dürfen für das Arbeitsverhältnis nur verarbeitet werden, wenn sie für die Begründung, Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet 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 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 Zusammenhang mit dem Arbeitsverhältnis stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

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.

Einwilligung in die Datenverarbeitung

Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung der Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Einwilligungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Ausnahmsweise kann die Einwilligung auch 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 IV.3. dieser Datenschutzrichtlinie informiert werden.

Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der IT Manufactory GmbH erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (z.B. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) 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 berechtigte 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. Informationsrechte der Betroffenen) berücksichtigt werden.

Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. 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. 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 Beauftragte für den Datenschutz im Vorfeld zu informieren.

Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Intranet 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 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 Netz der IT Manufactory GmbH 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 IT Manufactory GmbH 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 Regelungen der IT Manufactory GmbH.

Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der IT Manufactory GmbH oder an Empfänger innerhalb der IT Manufactory GmbH unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt V. 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 IT Manufactory GmbH in einem Drittstaat 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 IT Manufactory GmbH muss sichergestellt sein,

dass die Daten nur für die vorgesehenen Zwecke verwendet werden dürfen. Werden personenbezogene Daten von einer Gruppengesellschaft mit Sitz im Europäischen Wirtschaftsraum an eine Gruppengesellschaft 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 über- mittelten Daten zu beachten. Entsprechendes gilt für Datenübermittlungen durch Gruppengesellschaften aus anderen Staaten.

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 ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb der IT Manufactory GmbH eine Vereinbarung über eine Auftragsdatenverarbeitung 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.

- Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.
- Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
- Die vom Datenschutzbeauftragten bereitgestellten Vertragsstandards müssen beachtet werden.
- 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.
- Bei einer grenzüberschreitenden Auftragsdatenverarbeitung sind die jeweiligen nationalen Anforderungen für eine Weitergabe personenbezogener Daten ins Ausland zu erfüllen.

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.

- 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.
- Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.
- Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
- 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.

- 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. 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.

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. Zusätzlich sind sämtliche Daten der Human-Resource Abteilung und des Legal Department verschlüsselt. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Vorgesetze müssen ihre Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrung des Datengeheimnisses unterrichten. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

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 zu orientieren. 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.

Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Kontrollen überprüft. Die Durchführung obliegt dem Datenschutzbeauftragten oder beauftragten externen Prüfern. Die Ergebnisse der Datenschutzkontrollen sind dem Datenschutzbeauftragten mitzuteilen. Die Geschäftsführung 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.

Datenschutzvorfälle

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

In Fällen von:

- unrechtmäßiger Übermittlung personenbezogener Daten an Dritte,
- unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten,
- Verlust von personenbezogenen Daten

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

Verantwortlichkeiten und Sanktionen

Die Geschäftsführungen ist verantwortlich für die Datenverarbeitung in ihrem Verantwortungsbereich. Damit sind sie 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 Datenschutzkontrollen durch Behörden ist der Beauftragte für den Datenschutz umgehend zu informieren.

Das Verarbeitungsverzeichnis

Die IT Manufactory GmbH hat eine Dokumentation über alle Verarbeitungsvorgänge zu führen, bei denen personenbezogene Daten erfasst, verarbeitet oder gespeichert werden. Im engen Zusammenhang mit dem Informationssicherheitsmanagementsystem sind die Verantwortlichkeiten klar geregelt, die benötigten Informationen der jeweils betroffenen Abteilung zusammenzustellen und dem Datenschutzbeauftragten zukommen zu lassen. Dieser wird die Informationen zusammentragen und entsprechend der Anforderungen des Art. 30 DS-GVO in einem Verarbeitungsverzeichnis dokumentieren. Auf Anfrage stellt das Unternehmen der zuständigen Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Geschäftsführung ist hierfür der Datenschutzbeauftragte zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

Der Datenschutzbeauftragte

Die IT Manufactory GmbH hat nach Massgabe des Artikels 37 DS-DVO einen internen, freiwiligen, nebenamtlichen Datenschutzbeauftragten benannt und in die Unternehmenskultur eingegliedert. Der Beauftragte für den Datenschutz als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin.

Aufgaben:

- Beratung bei datenschutzrechtlichen Fragen
- Überwachung und Einhaltung der datenschutzrechtlichen Vorschriften (DSGVO, BDSG sowie weitere Rechtsvorschriften) sowie der unternehmenseigenen Datenschutzbestimmungen und Schulung von Mitarbeitern.

- Kommunikation mit der Datenschutzaufsichtsbehörde,
- Ansprechpartner für betroffene Personen und Mitarbeiter zu allen mit der Verarbeitung ihrer Daten und mit der Wahrnehmung ihrer Rechte zusammenhängenden Vorgänge.
- Unterstützung des Verantwortlichen bei der Etablierung von Prozessen bzw. Dokumentationen zur Erfüllung datenschutzrechtlicher Pflichten, Unterstützung bei der Meldepflicht- und Benachrichtigungspflicht bei Datenschutzverletzungen sowie Erfüllung der Betroffenenrechte (Recht aus Auskunft, Berichtigung, Einschränkung der Datenverarbeitung, und Löschen von Daten).
- Unterstützung bei der Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten.

Der Datenschutzbeauftragte wird von der Geschäftsführung der IT Manufactory GmbH bestellt.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden.
Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Kann der Datenschutzbeauftragte einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzrichtlinien nicht abstellen, muss er die Geschäftsführung einschalten.

Datenschutzbeauftragter:

Jürgen Sterr, D-94113 Tiefenbach, E-Mail: juergen.sterr@it-manufactory.com, Mobil: +49 (0) 151 648 129 25