

Teufelberger Datenschutzrichtlinie

Inhaltsverzeichnis

1	Zweck.....	2
2	Geltungsbereich und Änderung der Datenschutzrichtlinie	2
3	Geltung staatlichen Rechts.....	2
4	Prinzipien für die Verarbeitung personenbezogener Daten	2
5	Zulässigkeit der Datenverarbeitung.....	3
6	Übermittlung personenbezogener Daten.....	7
7	Auftragsdatenverarbeitung	8
8	Rechte des Betroffenen	8
9	Vertraulichkeit der Verarbeitung	9
10	Sicherheit der Verarbeitung	9
11	Datenschutzkontrolle	9
12	Datenschutzvorfälle	10
13	Verantwortlichkeiten und Sanktionen	10
14	Der Konzernverantwortliche für den Datenschutz (KDSV).....	10
15	Definitionen	11

1 Zweck

Die Unternehmensgruppe Teufelberger verpflichtet sich, im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzrichtlinie gilt weltweit für den Teufelberger-Konzern. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation des Teufelberger-Konzerns als attraktiver Arbeitgeber. Die Datenschutzrichtlinie schafft eine der notwendigen Rahmenbedingungen für weltweite Datenübermittlungen¹ zwischen den Konzerngesellschaften. Sie gewährleistet das von der EU-Datenschutz-Grundverordnung (DSGVO) und den jeweiligen nationalen Gesetzen verlangte angemessene Datenschutzniveau für den grenzüberschreitenden Datenverkehr auch in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

2 Geltungsbereich und Änderung der Datenschutzrichtlinie

Diese Datenschutzrichtlinie gilt für alle Unternehmen des Teufelberger-Konzerns, d.h. für die Teufelberger Holding AG und alle verbundenen Unternehmen und deren Mitarbeiter.

Die Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten². Anonymisierte³ Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

Die einzelnen Konzerngesellschaften sind nicht berechtigt, von dieser Datenschutzrichtlinie abweichende Regelungen zu treffen. Weitere Richtlinien zum Datenschutz dürfen in Abstimmung mit dem Konzerndatenschutzverantwortlichen (KDSV) dann erstellt werden, wenn dies nach dem jeweiligen nationalen Recht erforderlich ist. Eine Änderung dieser Datenschutzrichtlinie findet in Abstimmung mit dem KDSV statt.

3 Geltung staatlichen Rechts

Diese Datenschutzrichtlinie beinhaltet die Vorgaben der DSGVO sowie der nationalen Umsetzungsgesetzgebung. Sie ergänzt und konkretisiert das jeweilige nationale Datenschutzrecht. 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 des Teufelberger-Konzerns 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 Konzernunternehmen unverzüglich den KDSV zu informieren. Im Falle einer Kollision zwischen nationaler Rechtsvorschrift und der Datenschutzrichtlinie wird die Teufelberger Holding AG gemeinsam mit dem betroffenen Konzernunternehmen nach einer praktikablen Lösung im Sinne der Ziele der Datenschutzrichtlinie suchen.

4 Prinzipien für die Verarbeitung personenbezogener Daten

4.1 Fairness und Rechtmäßigkeit

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen⁴ gewahrt werden. Personenbezogene Daten müssen auf rechtmäßige Weise und fair erhoben und verarbeitet werden.

¹ Siehe 15.1

² Siehe 15.2

³ Siehe 15.3

⁴ Siehe 15.4

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 Stelle⁵
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die 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 erforderlich⁶ 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 nicht zutreffende 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 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 Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

⁵ Siehe 15.5

⁶ Siehe 15.6

5.1 Kunden- und Partnerdaten

5.1.1 Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners 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. Für darüberhinausgehende Werbemaßnahmen müssen die folgenden Voraussetzungen unter 5.1.2 beachtet werden.

5.1.2 Datenverarbeitung zu Werbezwecken

Wendet sich der Betroffene mit einem Informationsanliegen an ein Unternehmen des Teufelberger Konzerns (z.B. Wunsch nach Zusendung von Informationsmaterial zu einem Produkt), so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

Unaufgeforderte 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.

Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung⁷ 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 s. 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 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 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 des Teufelberger-Konzerns erforderlich ist. Berechtigte Interessen sind in der

⁷ Siehe 15.7

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 schutzwürdiger⁸ 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 KDSV im Vorfeld zu informieren.

5.1.7 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.

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 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 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/Mitarbeiter 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

⁸ Siehe 15.8

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 Kollektivregelungen 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 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 des Teufelberger-Konzerns 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, ein verhältnismäßiges berechtigtes Interesse oder ein begründeter Anlass besteht. 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. 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 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. Ebenso dürfen Daten, die Straftaten betreffen, 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 KDSV im Vorfeld zu informieren.

5.2.7 **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 Teufelberger-Netzwerk implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren.

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Teufelberger-Konzerns 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 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb des Teufelberger-Konzerns oder an Empfänger innerhalb des Teufelberger-Konzerns 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 des Teufelberger-Konzerns in einem Drittstaat⁹ muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Im Falle einer Datenübermittlung von Dritten an Unternehmen des Teufelberger-Konzerns muss sichergestellt sein, dass die Daten nur für die vorgesehenen Zwecke verwendet werden.

Die Datenübermittlung innerhalb des Konzerns wird in einem gesonderten Rahmenvertrag für die Datenübermittlung vereinbart.

⁹ Siehe 15.9

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 ist sowohl mit externen Auftragnehmern als auch zwischen Unternehmen innerhalb des Teufelberger-Konzerns 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 schriftlich zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
- Der KSDV ist über jeden neuen Auftragsverarbeiter und jede Änderung zu Informieren.
- Die vom KSDV 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.
 - a. Bei einer grenzüberschreitenden Auftragsdatenverarbeitung 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: 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.
 - 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 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 kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung widersprechen. Für diese Zwecke müssen die Daten gesperrt werden.
- 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.

9 Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern im Teufelberger Konzern 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 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 vom KDSV 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 (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des konzernweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

11 Datenschutzkontrolle

Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft. Die Durchführung obliegt dem KSDV.

12 Datenschutzvorfälle

Jeder Mitarbeiter meldet seinem jeweiligen Vorgesetzten und dieser dem KDSV unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten (Datenschutzvorfälle¹⁰).

In Fällen von unbeabsichtigter oder unrechtmäßiger Zugriff/Übermittlung/Veränderung /Vernichtung/Verlust sind die im Unternehmen vorgesehenen Meldungen (Information Security Incident Management) unverzüglich durch den KDSV zu veranlassen, damit nach staatlichem Recht bestehende Meldepflichten von Datenschutzvorfällen erfüllt werden können.

13 Verantwortlichkeiten und Sanktionen

Der Vorstand und die Geschäftsführungen der Konzerngesellschaften sind 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, auf Basis der Vorgaben mittels organisatorischer, personeller und technischer Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes sicherzustellen.

Bei Datenschutzkontrollen durch Behörden ist der KDSV umgehend zu informieren. Die jeweiligen Geschäftsführungen und Werkleitungen müssen dem KDSV einen Datenschutzkoordinator benennen. Die Datenschutzkoordinatoren sind vor Ort Ansprechpartner für den Datenschutz. Sie können Kontrollen durchführen und haben die Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Die jeweiligen Geschäftsführungen sind verpflichtet, den KDSV und die Datenschutzkoordinatoren in ihrer Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen die Datenschutzkoordinatoren rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, bei denen personenbezogene Daten verarbeitet werden sollen, ist der Konzernverantwortliche für den Datenschutz schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten, in diesen Fällen ist eine Risikofolgenabschätzung durchzuführen. 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 Der Konzernverantwortliche für den Datenschutz (KDSV)

Der KDSV sorgt gemeinsam mit den jeweiligen Geschäftsführern und den Datenschutzkoordinatoren für die Einhaltung der nationalen und internationalen Datenschutzvorschriften. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Er wird vom Vorstand der Teufelberger AG bestellt. Er ist von den Datenschutzkoordinatoren regelmäßig zu informieren und bei wesentlichen Datenschutzthemen umgehend zu konsultieren.

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den KDSV oder an den für ihn zuständigen Datenschutzkoordinator wenden.

Kann der zuständige Datenschutzkoordinator einer Beschwerde nicht abhelfen oder einen Verstoß gegen Datenschutzrichtlinien nicht abstellen, muss er den KDSV einschalten. Die Entscheidungen des

¹⁰ Siehe 15.10

KDSV zur Abhilfe der Datenschutzverletzung sind durch die jeweiligen Geschäftsführungen zu berücksichtigen. Bei Anfragen von Aufsichtsbehörden ist stets auch der KDSV beizuziehen.

15 Definitionen

- 15.1 Übermittlung ist jede Bekanntgabe von geschützten Daten durch die verantwortliche Stelle an Dritte.
- 15.2 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.
- 15.3 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.
- 15.4 Betroffener im Sinne dieser Datenschutzrichtlinie ist jede natürliche Person, über die Daten verarbeitet werden.
- 15.5 Verantwortliche Stelle ist diejenige juristisch selbständige Gesellschaft des Teufelberger-Konzerns, deren Geschäftsaktivität die jeweilige Verarbeitungsmaßnahme veranlasst.
- 15.6 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.
- 15.7 Einwilligung ist eine freiwillige, rechtsverbindliche Einverständniserklärung in eine Datenverarbeitung.
- 15.8 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.
- 15.9 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.
- 15.10 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.