Datenschutzleitlinie der Elabs AG

Betreff	Datenschutzleitlinie der Elabs AG
Erstellt:	11.11.2021
Bearbeitet:	06.07.2022
Version:	1.3
Autor:	Christian Stenger | Elabs AG
Freigegeben durch:	Information Security Officer (ISO)
Anwendungsbereich:	Gesamtes Unternehmen
Zuständigkeiten:	Datenschutzbeauftragter (DSB)

Datum	*Version*	*Autor*	*Änderung*
11.11.2021	***1.0***	***DSB***	***Initiale Version / Draft***
15.12.2021	***1.1***	***DSB***	***Anpassungen und Formulierungen***
24.02.2022	***1.2***	***DSB***	***Anpassungen***
06.07.2022	***1.3***	***DSB***	***Neu hinzugefügt Vorwort***

Vorwort

Sehr geehrte Damen, Herren und Diverse,

wir bieten unseren Kunden neben den klassischen Kontaktmöglichkeiten auch die Möglichkeit, digital mit uns zu kommunizieren. Das setzt voraus, dass Daten erfasst und verarbeitet werden. Hierbei gilt für uns der Grundsatz: Wo Daten gespeichert und gesendet werden, muss ein hohes Maß an Datenschutz und Datensicherheit gewährleistet sein. Dies gilt für Daten von Kunden und Bewerbern (fällt im Folgenden unter Kunden), Interessenten und Geschäftspartnern genauso wie für unsere Mitarbeiterdaten.

Unser Anspruch ist es, dass die Elabs AG nicht nur für qualitativ hochwertige Dienstleistungen und Vermittlung steht, sondern auch die gesetzlichen Anforderungen des Datenschutzes einhält. Die Persönlichkeitsrechte und die Privatsphäre eines jeden Einzelnen zu wahren, ist für uns die Basis für vertrauensvolle Geschäftsbeziehungen.

Wir haben strenge Voraussetzungen für die Verarbeitung personenbezogener Daten von Kunden, Interessenten, Geschäftspartnern und Mitarbeitern geschaffen. Diese richten sich nach den Anforderungen der Europäischen Datenschutzrichtlinie und stellen die Einhaltung der geltenden nationalen Datenschutzgesetze sicher. Im Folgenden stellen wir unsere Datenschutzleitlinie dar. Unsere Mitarbeiter sind verpflichtet den Datenschutz einzuhalten und die jeweiligen Datenschutzgesetze zu wahren.

Inhaltsverzeichnis

1 Ziel der Datenschutzleitlinie

Die Elabs AG verpflichtet sich, im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzleitlinie gilt für die Elabs AG und beruht auf Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation als attraktiver Arbeitgeber bzw. Dienstleister der Personalbranche.

Die Datenschutzleitlinie schafft eine der notwendigen Rahmenbedingungen für Datenübermittlungen zwischen Partnern, Kunden und Mitarbeitern. Sie gewährleistet das von der Europäischen Datenschutzrichtlinie und den nationalen Gesetzen verlangte angemessene Datenschutzniveau für den Datenverkehr auch mit solchen Ländern, in denen gesetzlich kein angemessenes Datenschutzniveau besteht.

2 Geltungsbereich

Diese Datenschutzleitlinie gilt für die Elabs AG, Hanauer Landstrasse 172, 60314 Frankfurt am Main, sowie für alle Mitarbeiter, die unmittelbar und mittelbar in den Diensten der Elabs AG stehen.

Die Datenschutzleitlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. In Ländern, in denen Daten juristischer Personen in gleicher Weise wie personenbezogene Daten geschützt werden, gilt diese Datenschutzleitlinie auch in gleicher Weise für Daten juristischer Personen. Anonymisierte Daten, z.B. für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzleitlinie.

Weitere Richtlinien zum Datenschutz dürfen in Abstimmung mit dem internen bzw. externen Unternehmensbeauftragten für den Datenschutz dann erstellt werden, wenn dies nach dem jeweiligen nationalen Recht erforderlich ist. Die aktuellste Version der Datenschutzleitlinie kann auf der Seite https://www.elabs.de unter dem Punkt „Datenschutz“ eingesehen werden.

3 Unsere Datenschutzgrundsätze

Unsere Grundsätze des Datenschutzes richten sich, wie im weiteren Verlauf dargestellt, streng nach den Anforderungen geltender Rechtsvorschriften.

Die folgende sieben Punkte sind uns besonders wichtig:

1. Zweckbindung

Die Zweckbindung ist ein wesentlicher Bestandteil des Gesetzes. Werden Daten für einen bestimmten Zweck erhoben bzw. gespeichert, dann dürfen diese Daten auch nur für diesen Zweck verwendet werden. Daten, die z.B. für die Erfüllung eines Vertrages gespeichert werden, dürfen auch nur für diesen Vertrag genutzt werden. Die Nutzung der Daten für einen anderen Zweck ist verboten! Hierbei achtet die Elabs AG sehr genau auf diese Zweckbindung.

2. Verbot bei Erlaubnisvorbehalt

Grundsätzlich ist die Erfassung bzw. Speicherung von personenbezogenen Daten verboten. Es sei denn, man hat die Erlaubnis der betroffenen Person bzw. des Unternehmens. Die Erlaubnis liegt zum Beispiel vor, wenn Daten für die Abwicklung eines Vertrages gespeichert werden müssen. Die Datenspeicherung ist immer an den Zweck gebunden (siehe oben: Zweckbindung).

3. Direkterhebung

Daten sollten immer direkt bei der betroffenen Person erhoben werden. Das bedeutet, dass personenbezogene Daten in der Regel direkt von der betroffenen Person erfragt werden müssen. Wir verwenden keine Daten aus anderen „Quellen“.

4. Datensparsamkeit

Wir speichern Daten nur so lange, wie diese an den Zweck gebunden sind oder andere vorrangige Gesetze eine Löschung verhindern. Ist die gesetzliche Aufbewahrungsfrist abgelaufen, werden Daten in jedem Fall zur Löschung freigegeben.

5. Datenvermeidung

Wir speichern nur Daten, die für den angegebenen Zweck erforderlich sind. Zusätzliche Datenbestände werden hierbei vermieden.

6. Transparenz

Jede betroffene Person soll wissen, welche Daten über sie gespeichert werden. Dies bedeutet, dass Daten nicht weitergegeben werden. (siehe oben: Direkterhebung). Ist die Weitergabe der Daten erforderlich, werden betroffene Person von der Datenweitergabe unterrichtet und eine Einwilligungserklärung eingeholt. Weiterhin besteht jederzeit ein Auskunftsrecht für betroffene Personen. Mit Hilfe dieses Auskunftsrechts kann man Einsicht in die gespeicherten Daten verlangen.

7. Erforderlichkeit

Daten dürfen nur gespeichert werden, wenn die Speicherung der Daten für die Erreichung des Zwecks (siehe oben: Zweckbindung) erforderlich ist.

Wie Sie erkennen können, sind diese sieben Grundprinzipien eng miteinander verknüpft und ergänzen bzw. bedingen sich gegenseitig. Im weiteren Verlauf erläutern wir detailliert Grundsätze, Prinzipien und Verarbeitungsrichtlinien des Datenschutzes in seiner aktuellen gesetzlichen Fassung.

4 Prinzipien für die Verarbeitung personenbezogener Daten

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

Der Betroffene kann jederzeit verlangen, über den Umgang mit seinen Daten informiert zu werden und die Löschung seiner Daten verlangen. 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 potenzielle zukünftige Zwecke gespeichert werden, es sei denn, dies ist durch staatliches Recht vorgeschrieben, erlaubt oder durch den Rechteinhaber der personenbezogenen Daten genehmigt.

Personenbezogene Daten, die nach Ablauf von gesetzlichen oder geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen oder für eine historische Bedeutung dieser Daten, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde oder die Unternehmensarchive den Datenbestand auf seine Archivwürdigkeit für historische Zwecke bewerten konnten. Personenbezogene Daten sind richtig, vollständig und soweit erforderlich auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.

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.

6 Kunden-, Interessenten und Partnerdaten

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.

2. Datenverarbeitung zur Vermittlung

Personenbezogene Daten des betroffenen Interessenten oder Bewerbers werden zur Beschaffung von Dokumenten, die für eine erfolgreichen Vermittlung eines Arbeitsplatzes erforderlich sind, erfasst und verarbeitet. Darunter fallen Dokumente und Daten, wie z.B.: eine Aufenthaltserlaubnis, eine Arbeitsgenehmigung, Bewerbungsunterlagen oder die Anerkennung von Zeugnissen und Abschlüssen, die Steuer- und Sozialversicherungsnummer, eine Wohnmeldebescheinigung etc..

Zu diesem Zwecke ist es notwendig die Daten an Behörden und Ämter, sowie potenzielle Arbeitgeber zu leiten. Dies geschieht im Rahmen einer Einwilligung der betroffenen Person und liegt vollständig in dessen Interesse.

3. Datenverarbeitung zu Werbezwecken

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

Kundenbindungs- oder Werbemaßnahmen bedürfen weitere rechtliche Voraussetzungen. Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder der Markt- und Meinungsforschung ist zulässig, sofern sich dies mit dem Zweck, für den die Daten ursprünglich erhoben wurden, vereinbaren lässt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung zu informieren. Sofern Daten ausschließlich für Werbezwecke erhoben werden, ist deren Angabe durch den Betroffenen freiwillig. Der Betroffene soll über die Freiwilligkeit der Angabe von Daten für diese Zwecke informiert werden. Im Rahmen der Kommunikation mit dem Betroffenen soll eine Einwilligung des Betroffenen für die Verarbeitung seiner Daten zu Werbezwecken eingeholt werden. Der Betroffene soll im Rahmen der Einwilligung zwischen den verfügbaren Kontaktkanälen wie Post, elektronische Post und Telefon wählen können (Einwilligung siehe unten 4. Einwilligung in die Datenverarbeitung). 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.

4. Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß dieser Datenschutzleitlinie 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. 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.

6. Datenverarbeitung aufgrund berechtigten Interesses

Die Verarbeitung personenbezogener Daten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses der Elabs AG 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 an der Verarbeitung überwiegen. Die schutzwürdigen Interessen sind für jede Verarbeitung zu prüfen.

7. Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten, wie z.B. personenbezogene Informationen über die rassische und ethnische Herkunft, politische Meinungen, religiöse Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, genetische oder biometrische 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 Unternehmensbeauftragte für den Datenschutz im Vorfeld zu informieren.

8. Nutzerdaten und Internet

Wenn auf Webseiten 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. Wird zur Auswertung des Nutzungsverhaltens von Webseiten Nutzungsprofile erstellt (Tracking), so müssen die Betroffenen darüber in jedem Fall in den Datenschutzhinweisen informiert werden. Ein personenbezogenes Tracking darf nur erfolgen, wenn das nationale Recht dies zulässt oder der Betroffene eingewilligt hat. Erfolgt das Tracking unter einem Pseudonym, so soll dem Betroffenen in den Datenschutzhinweisen eine Widerspruchsmöglichkeit eröffnet werden (Opt-out). Werden bei Webseiten oder Apps in einem registrierungspflichtigen Bereich Zugriffe auf personenbezogene Daten ermöglicht, so sind die Identifizierung und Authentifizierung der Betroffenen so zu gestalten, dass ein für den jeweiligen Zugriff angemessener Schutz erreicht wird.

7 Mitarbeiterdaten

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 erforderlich.

Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein, sofern nicht einer der nachfolgenden Erlaubnistatbestände für die Datenverarbeitung eingreift.

Ist während der Anbahnung des Arbeitsverhältnisses oder im bestehenden Arbeitsverhältnis die Erhebung weiterer Informationen über den Bewerber bei einem Dritten erforderlich, sind die jeweiligen nationalen gesetzlichen Anforderungen zu berücksichtigen. Im Zweifel ist eine Einwilligung des Betroffenen einzuholen.

Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht originär der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

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.

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 Tarifverträge oder Vereinbarungen zwischen Arbeitgeber und Arbeitnehmervertretungen im Rahmen der Möglichkeiten des jeweiligen Arbeitsrechts. Die Regelungen müssen sich auf den konkreten Zweck der gewünschten Verarbeitung erstrecken und sind im Rahmen des staatlichen Datenschutzrechts gestaltbar.

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 dem Abschnitt Kunden- und Partnerdaten Punkt 4 dieser Datenschutzrichtlinie informiert werden.

5. Datenverarbeitung aufgrund berechtigten Interesses

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

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

Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn dazu eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch bei Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahme (z.B. Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das 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.

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. 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 Unternehmensbeauftragte für den Datenschutz im Vorfeld zu informieren.

7. Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, Internet sowie interne 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. 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 können Schutzmaßnahmen an den Übergängen in das Unternehmens-Netz implementiert werden, die technisch schädigende Inhalte blockieren oder die Muster von Angriffen analysieren. Aus Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen und des Internets, sowie der internen Netzwerke zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien der Elabs AG 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 Unternehmensregelungen.

8 Übermittlung personenbezogener Daten

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der Elabs AG oder an Empfänger innerhalb der Elabs AG unterliegt den Zulässigkeitsvorraussetzungen der Verarbeitung personenbezogener Daten. 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 Elabs AG 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 des Unternehmens, welche die Daten übermittelt, ergeben oder das Recht des Sitzlandes des Unternehmens erkennt das mit der gesetzlichen Verpflichtung eines Drittstaats verfolgte Ziel der Datenübermittlung an. Im Falle einer Datenübermittlung von Dritten an die Elabs AG muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

Werden personenbezogene Daten eines Unternehmens mit Sitz im Europäischen Wirtschaftsraum an ein Unternehmen mit Sitz außerhalb des Europäischen Wirtschaftsraums (Drittstaat) übermittelt, so ist die datenimportierende Gesellschaft verpflichtet, bei allen Anfragen der für die datenexportierende Gesellschaft zuständigen Aufsichtsbehörde mit dieser zu kooperieren und die Feststellungen der Aufsichtsbehörde im Hinblick auf die übermittelten Daten zu beachten. Entsprechendes gilt für Datenübermittlungen durch Unternehmen aus anderen Staaten. Nehmen sie an einem internationalen Zertifizierungssystem für verbindliche Unternehmensregelungen zum Datenschutz teil, müssen sie die dort vorgesehene Kooperation mit den entsprechenden Prüfungsstellen und Behörden sicherstellen. Die Teilnahme an derartigen Zertifizierungssystemen ist mit dem Unternehmensbeauftragten für den Datenschutz abzustimmen.

9 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 mit externen Auftragnehmern 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.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.

3. Die vom Datenschutzbeauftragten bzw. der Elabs AG bereitgestellten Vertragsstandards müssen beachtet werden.

4. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflichten des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle gegebenenfalls während der Vertragslaufzeit regelmäßig zu wiederholen.

5. 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:

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.

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

10 Auskunftspflicht

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 Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

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, muss auch über die Identität des Empfängers oder über die Kategorien von Empfängern Auskunft gegeben werden.

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 müssen die Daten gesperrt werden.

5. Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder weggefallen ist. Gleiches gilt für den Fall, dass der Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.

6. Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse an der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

11 Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Es gilt das Need-to-know-Prinzip:

Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen von Berechtigungskonzepten.

Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. 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.

12 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 (ermittelt durch den Prozess zur Informationsklassifizierung) zu orientieren.

13 Datenschutzkontrolle

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

14 Datenschutzvorfälle

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

15 Verantwortlichkeiten und Sanktionen

Die Geschäftsführung der Gesellschaft ist verantwortlich für die Datenverarbeitung in ihrem Unternehmen. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzleitlinie 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 Unternehmensbeauftragte für den Datenschutz umgehend zu informieren.

Der Unternehmensbeauftragte für den Datenschutz kann Kontrollen durchführen, um Mitarbeiter mit den Inhalten der Datenschutzrichtlinien vertraut zu machen. Hierbei ist der Unternehmensbeauftragte für den Datenschutz vollumfänglich weisungsbefugt. Die Geschäftsführung ist verpflichtet, den Unternehmensbeauftragte für den Datenschutz in seiner Tätigkeit zu unterstützen. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Unternehmensbeauftragte für den Datenschutz schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. 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.

16 Der Unternehmensbeauftragte für den Datenschutz

Der Beauftragte für den Datenschutz als internes, fachlich weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Der Beauftragte für den Datenschutz wird von der Geschäftsleitung bestellt. Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Beauftragten für den Datenschutz wenden. Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt. Anfragen von Aufsichtsbehörden sind immer an den Beauftragten für den Datenschutz zur Kenntnis zu bringen. Sollte die Elabs AG keinen als Datenschutzbeauftragten benannt haben, so gilt die Geschäftsführung als Datenschutzverantwortlicher.

17 Kontakt

Elabs AG

Hanauer Landstrasse 172

60314 Frankfurt am Main

Vorstand: Thomas Keck (Vorsitzender)

Sitz der Gesellschaft: Frankfurt am Main

Registergericht: Amtsgericht Frankfurt am Main HRB52696

WEEE-Register-Nr.: DE 436 603 10

Ust-IdNr.: DE 813 208 789

Homepage: www.elabs.de

E-Mail: info@elabs.de