Datenschutzrichtlinie

der x-GmbH Stand: Januar xxxx

Inhalt

Vorwort der Geschäftsführung

Die x-GmbH produziert seit vielen Jahren Materialien zum Sprachenlernen, - übersetzen und -anwenden in allen medialen Formen.

Unsere Kunden verlassen sich auf die fremdsprachliche Kompetenz des Unternehmens und Rechtstreue als Teil eines der größten Bildungsunternehmen.

Im Mai 2018 trat die EU-Datenschutz-Grundverordnung vollumfänglich in Kraft. Sie ist - neben einigen wenigen nationalen Regelungen - die Grundlage für die Verarbeitung von personenbezogenen Daten für alle Bewohner der Europäischen Union

Die vorliegende Datenschutzrichtlinie für die x-GmbH soll Mitarbeiterinnen und Mitarbeitern ermöglichen sich bei der Verarbeitung von personenbezogenen Daten sicher zu bewegen und die Risiken für die Betroffenen richtig einzuschätzen.

Gabriele Schmidt (Geschäftsführerin x-GmbH)

Geltungsbereich und Ziele

Die X-Gmbh verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten der Bundesrepublik Deutschland, der Europäischen Union und weltweit.

Diese Datenschutzrichtlinie gilt für alle Mitarbeiter der X-Gmbh.

Sie beruht auf den europäischen Grundprinzipien zum Datenschutz und 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, zum Beispiel für statistische Auswertungen oder Untersuchungen, unterliegen nicht dieser Datenschutzrichtlinie.

Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der x-GmbH als attraktivem Arbeitgeber. Die Datenschutzrichtlinie schafft darüber hinaus notwendige Rahmenbedingungen für weltweite Datenübermittlungen zwischen der X-Gmbh und deren Partnern.

Sie gewährleistet das von der EU-Datenschutz-Grundverordnung (DSGVO) und den nationalen Gesetzen (BDSG-neu) verlangte angemessene Datenschutzniveau auch für den grenzüberschreitenden Datenverkehr in solche Länder, in denen gesetzlich kein angemessenes Datenschutzniveau besteht

Eine Änderung dieser Datenschutzrichtlinie findet in Abstimmung mit dem Datenschutzbeauftragten statt.

Die aktuellste Version der Datenschutzrichtlinie kann im internen Laufwerk unter G:\ALLE\Datenschutz jederzeit abgerufen werden.

Die Datenschutzrichtlinie regelt den allgemeinen Umgang mit personenbezogenen Daten im Unternehmen. Sie wird sukzessive ergänzt um konkrete Richtlinien zur Wahrung des Datenschutzes in speziellen Situationen.

Kommentiert [St.1]: Wohl kaum, wenn damit auch personenbezogene Daten gemeint sein sollten, was leider offen bleibt.

Kommentiert [St.2]: Siehe vorherigen Kommentar. Höchst missverständliche und gefährliche Behauptung, da sie für personenbezogene Daten keinesfalls gilt.

Kommentiert [St.3]: Es bleibt unklar, ob sich diese RL an die AN wendet, damit diese
-gegenüber Kunden
-gegenüber Mitarbeitern
-gegenüber sich selbst
den Datenschutz korrekt anwenden.
Dadurch kommt es zu Verallgemeinerungen und irreführenden Aussagen, die der Sache abträglich sind.

Begriffe und Abkürzungen

Die Begriffe werden gemäß den Definitionen der einzelnen geltenden Gesetze (insbesondere Art. 4 DSGVO) verwendet. Die wichtigsten Begriffe sind hier aufgeführt:

Begriff	Erklärung
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person" oder „Betroffener") beziehen. Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, welche Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
Verarbeitung	Jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung. Der Begriff der Verarbeitung wird den Begriffen Prozess und Verfahren gleichgeschaltet.
Profiling	Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.
Pseudonymisierung	Die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt, werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
Verantwortlicher	Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise

Kommentiert [St.4]: Es bleibt unklar, ob hier gesetzliche Definitionen unverfälscht zitiert werden oder ob es sich die X-GmbH erlaubt, diese lediglich als Grundlage für eigene Definitionen zu nutzen. Daran ändert sich auch nichts, wenn ich das jetzt einzeln durchprüfe (was ich nicht tue), denn es geht um den Eindruck gegenüber dem Leser. Es ist wissenschaftlich unseriös, hier nicht klar und transparent (insbesondere diese wird von der DSGVO als hohes Gut eingestuft) darzustellen, wie man vorgeht.

	die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
Auftragsverarbeiter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Empfänger von Daten	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung. Nicht zu verwechseln mit dem Paketempfänger. Dieser ist im Sinne des Datenschutzes Betroffener der Datenverarbeitung.
Dritter	Eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Steile, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.
In der Richtlinie werden folgende Abkürzungen verwendet:	
Abkürzung	Erklärung
BDSG-neu	Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG - EU) - die nationalen Datenschutzgesetze zur Umsetzung der Öffnungsklauseln aus der DSGVO
EU-DSGVO oder DSGVO	Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung)

Organisation des Datenschutzes bei der X-Gmbh

Der Datenschutzbeauftragte der X-Gmbh stellt ein fachlich weisungsunabhängiges Organ des Unternehmens dar und wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht deren Einhaltung. Seine genauen Aufgaben sind in Art. 37 DSGVO geregelt. Der Datenschutzbeauftragte wird von der Geschäftsführung bestellt.

Zur Unterstützung des Datenschutzbeauftragten ist ein Datenschutzkoordinator bestimmt worden.

Datenschutzkoordinatoren unterstützen die verantwortliche Stelle und vor allem den Datenschutzbeauftragten im Bereich des Datenschutzes. Der Datenschutzkoordinator wird als Schnittstelle zwischen Unternehmen und dem (externen) Datenschutzbeauftragten eingesetzt, er kommuniziert innerhalb des Unternehmens und aus dem Unternehmen mit dem Datenschutzbeauftragten und verbessert so entscheidend die Kommunikation.

Der Datenschutzkoordinator unterstützt den Datenschutzbeauftragten bei seinen Aufgaben, indem er beispielsweise

- relevante Informationen (aus den Fachabteilungen) einholt
- bei einfachen datenschutzrelevanten Fragestellungen als Ansprechpartner vor Ort zur Verfügung steht
- die Datenschutzdokumente verwaltet, aktualisiert, pflegt oder ggf. vorbereitet
- auf die Einhaltung der Datenschutzrichtlinie hinwirkt, um ein gewisses
- Datenschutzniveau aufrecht zu erhalten, beispielsweise durch Mitarbeitersensibilisierungen
- die Datenschutzkontrolle und Einhaltung datenschutzrechtlicher Vorgaben unterstützt

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit dem Datenschutz oder der Datensicherheit bei personenbezogenen Datenverarbeitungen an den Datenschutzbeauftragten oder den Datenschutzkoordinator wenden.

Anfragen und Beschwerden werden auf Wunsch vertraulich behandelt und können direkt an den Datenschutzbeauftragten gestellt werden. Die Entscheidungen des Datenschutzbeauftragten zur Abhilfe der Datenschutzverletzung sind durch die Geschäftsführung zu berücksichtigen.

Anfragen von Aufsichtsbehörden und Betroffenen sind immer dem Datenschutzbeauftragten zur Kenntnis zu bringen.

Der Datenschutzbeauftragte kann wie folgt erreicht werden:

X-Gmbh

c/o Datenschutzbeauftragter Musterstraße 11

11111 Musterstadt

E-Mail: datenschutz@xgmbh.de

Kommentiert [St.5]: Das ist sachlich falsch und bedeutet eine Korruption des Amtes des bDSB, da er neutral und weisungsfrei zu sein hat. Beides ist nicht möglich, wenn er sich in betriebsverfassungsrechtliche Angelegenheiten zwischen AG und AN einmischt.

Kommentiert [St.6]: Wertung, die hier nicht hingehört

Kommentiert [St.7]: Der bDSB ist also ein Anonymus. Das geht nicht. Er ist als Person zu benennen. Stichwort: Transparenz.

Grundsätze der Verarbeitung personenbezogener Daten

- Rechtmäßigkeit und Verarbeitung nach Treu und Glauben

Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten dürfen nur auf rechtmäßige Weise und nach Treu und Glauben verarbeitet werden. Der Datenschutzbeauftragte muss jede Verarbeitung auf ihre Rechtmäßigkeit prüfen.

- Transparenz

Personenbezogene Daten müssen in einer für den Betroffenen nachvollziehbaren Art und Weise verarbeitet werden. Betroffene müssen über die Art und Auswirkung der Datenverarbeitung angemessen und in klaren und verständlichen Worten informiert werden.

- Zweckbindung

Personenbezogene Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.

- Datenminimierung

Die Verarbeitung personenbezogener Daten muss dem Zweck angemessen und auf das dafür notwendige Maß beschränkt sein.

- Richtigkeit

Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein. Es sind angemessene Maßnahmen zu treffen, dass unrichtige Daten unverzüglich gelöscht oder berichtigt werden können.

- Speicherbegrenzung

Personenbezogene Daten dürfen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Für alle Verarbeitungen sind deshalb Aufbewahrungs- oder Löschfristen zu definieren und einzuhalten.

- Vertraulichkeit und Datensicherheit

Personenbezogene Daten dürfen nur so verarbeitet werden, dass eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist. Dies schließt den Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch die Auswahl geeigneter technischer und organisatorischer Maßnahmen mit ein.

Zulässigkeit der Datenverarbeitung

Hauptprozesse

- Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten zu Kunden, Partnern und deren Angestellten oder deren Ansprechpartnern dürfen nur zur Durchführung eines bestehenden oder angehenden Vertragsverhältnisses verarbeitet werden. Potenzielle Interessenten dürfen zur Vertragsanbahnung nur unter den personenbezogenen Daten kontaktiert werden, die sie mitgeteilt haben.

Angaben zu Sendungsinhalten, Empfängern und Zustellhinweisen dürfen nur im Rahmen der Postgesetze und nur für erforderliche Zwecke verarbeitet werden, es sei denn, es liegen entsprechend nachweisbare Einwilligungserklärungen der Betroffenen vor.

Wendet sich der Betroffene mit einem Informationsanliegen (zum Beispiel mit dem Wunsch nach Zusendung von Informationsmaterial zu einem Produkt oder Service) an das Unternehmen, so ist die Datenverarbeitung für die Erfüllung dieses Anliegens zulässig.

- Datenverarbeitung zu Werbezwecken

Kundenbindungs- oder Werbemaßnahmen bedürfen weiterer rechtlicher Voraussetzungen.

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

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung, so ist eine weitere Verwendung seiner Daten für diese Zwecke unzulässig; die Daten müssen für diese Zwecke gesperrt werden.

- Einwilligung in die Datenverarbeitung

Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene ausreichend und nachweislich informiert werden.

Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, zum Beispiel bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden, ihre Erteilung muss dokumentiert werden.

Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. Der Betroffene muss über jede neue Art der Verarbeitung oder zu jedem einzelnen Zweck der Verarbeitung informiert werden und dieser einzeln zustimmen (Verkettungsverbot für Einwilligungen).

- Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Kommentiert [St.8]: Das kann wohl kaum auf AN abgewälzt werden und hat daher in einer RL nichts verloren. Hier geht es um Haftungsverantwortung der verantwortlichen Stelle. Sie hat die Abläufe bereits technisch, mindestens aber organisatorisch im Einzelfall festzulegen und zu prüfen, bevor sie sie in die Hände einzelner AN legt.

Kommentiert [St.9]: Verwechslung der Chronologie: zuerst werden die Daten erhoben, dann werden sie verwendet. Dadurch Verharmlosung der gesetzlichen Pflichten.

Kommentiert [St.10]: Äußerst missverständlich. Hier werden ggf. Ursache und Wirkung verwechselt.

Kommentiert [St.11]: Nein, er „ist“.

Kommentiert [St.12]: „ist“

Kommentiert [St.13]: Das ist chronologisch der erste Gedanke und nicht der letzte. Hinweis auf Widerrufsmöglichkeit ist gesetzlich vorgeschrieben und fehlt.

Kommentiert [St.14]: Hinweis auf Zweckinformation und Widerruf fehlt.

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 X-Gmbh oder einem Dritten erforderlich ist. Berechtigte Interessen sind in der Regel rechtlicher Art (zum Beispiel Durchsetzung von offenen Forderungen) oder wirtschaftlicher Art (zum Beispiel 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 einzeln zu prüfen.

Die Gründe für die berechtigten Interessen sind zu dokumentieren und sowohl bei der Verarbeitungsübersicht als auch bei der Information zur jeweiligen Datenverarbeitung (Datenschutzerklärung im Internet oder auf Formularen) anzugeben.

- Verarbeitung besonders schutzwürdiger Daten

Die Verarbeitung besonders schutzwürdiger personenbezogener Daten nach Art. 9 DSGVO 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.

Zu den besonders schutzwürdigen Daten zählen alle Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

- Automatisierte Einzelentscheidungen

Automatisierte Verarbeitungen personenbezogener Daten, durch die einzelne Persönlichkeitsmerkmale (zum Beispiel die Kreditwürdigkeit) bewertet werden, dürfen nicht die ausschließliche Grundlage für Entscheidungen mit negativen rechtlichen Folgen oder erheblichen Beeinträchtigungen für den Betroffenen sein. Dem Betroffenen müssen die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit zu einer Stellungnahme gegeben werden.

- Nutzerdaten und Internet

Wenn auf Webseiten oder in Apps personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber mit Datenschutzhinweisen und gegebenenfalls Cookie-Hinweisen zu informieren. Die Datenschutzhinweise und gegebenenfalls Cookie-Hinweise sind so zu integrieren, dass sie 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

Kommentiert [St.15]: Das ist falsch. Nicht alle gesetzlichen Erlaubnistatbestände verlangen inzident eine „Erforderlichkeit“; sie ist auch keine vorgeschaltete ungeschriebene Tatbestandsvoraussetzung. Selbst, wenn sie es wäre, könnte ein einzelner Mitarbeiter sie nicht prüfen.

Kommentiert [St.16]: Hier wird der falsche Eindruck erweckt, dies sei eine zu allen anderen Erlaubnistatbeständen alternative Erlaubnis. Tatsächlich ist sie in vielen Fällen gerade im Arbeitsleben nicht anwendbar, da sie durch speziellere Tatbestände verdrängt wird.

Kommentiert [St.17]: Ich glaube, hier weiß jemand nicht, was ein cookie ist. Dieser Begriff passt hier nicht her.

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.

Kommentiert [St.18]: Das kann wohl kaum auf AN abgewälzt werden und hat daher in einer RL nichts verloren. Hier geht es um Haftungsverantwortung der verantwortlichen Stelle.

Kommentiert [St.19]: s.o.

Kommentiert [St.20]: s.o.

Datenverarbeitung im Rahmen des Arbeitsverhältnisses

Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für die Begründung, Durchführung und Beendigung des Arbeitsvertrags 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 oder Partner erforderlich.

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

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 Arbeitsvertrags dienen, muss jeweils eine rechtliche Legitimation vorliegen. Das können gesetzliche Anforderungen, Kollektivregelungen mit Arbeitnehmervertretungen, eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

- 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.

- 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 Datenschutzrechts gestaltbar.

- 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.

- Datenverarbeitung aufgrund berechtigten Interesses

Kommentiert [St.21]: Das ist sachlich falsch. Es gibt zahlreiche Spezialgesetze, die ausschließlich der Erfüllung des Arbeitsverhältnisses dienen und entsprechende Datenverarbeitungen legitimieren.

Kommentiert [St.22]: Das ist sachlich falsch. Es gibt im arbeitsrechtlichen Datenschutz keine Regelung, die die berechtigten Interessen des Unternehmens genügen lassen. Es handelt sich hier um eine verdeckte Anspielung auf Art. 6 I f, der für den Arbeitnehmerdatenschutz nicht anwendbar ist.

Kommentiert [St.23]: Falsch, s.o.

Kommentiert [St.24]: Das mag so sein. Jedoch unterliegt alles bis hierher Gesagte im Abschnitt „Datenverarbeitung im Rahmen des Arbeitsverhältnisses“ der Mitbestimmung, was verschwiegen wird.

Die Verarbeitung personenbezogener Mitarbeiterdaten kann auch erfolgen, wenn dies zur Verwirklichung eines berechtigten Interesses des Unternehmens erforderlich ist. Berechtigte Interessen sind in der Regel rechtlicher Art (zum Beispiel Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche) oder wirtschaftlicher Art (zum Beispiel Bewertung von Unternehmen).

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 (zum Beispiel Einhaltung rechtlicher Bestimmungen und unternehmensinterner Regeln) müssen gegen ein mögliches schutzwürdiges Interesse des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden. Die Kontrollmaßnahmen 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 gegebenenfalls nach staatlichem Recht bestehende weitere Anforderungen (zum Beispiel Mitbestimmungsrechte der Arbeitnehmervertretung und Informationsrechte der Betroffenen) berücksichtigt werden.

- Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden.

Zu den besonders schutzwürdigen Daten zählen alle Angaben, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung einer natürlichen Person.

Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft oder der Inhalt der Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichem Recht auf gestellten 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.

- Automatisierte Entscheidungen

Soweit im Beschäftigungsverhältnis personenbezogene Daten automatisiert verarbeitet werden, durch die einzelne Persönlichkeitsmerkmale bewertet werden (etwa im Rahmen der Personalauswahl oder der Auswertung von Fähigkeitsprofilen), darf eine solche automatisierte

Kommentiert [St.25]: Das ist falsch, siehe bereits den Kommentar oben.

Kommentiert [St.26]: Falsch. Es bedarf immer einer gesetzlichen Regelung, einer Einwilligung oder einer BV (als „gesetzliche“ Regelung).
Möglicherweise eine verdeckte Anspielung auf § 26 I S. 2 BDSG, der dies davon abhängig macht, dass „zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat“; die Anspielung wäre dann ebenfalls sachlich falsch.

Kommentiert [St.27]: Eingriff in die Mitbestimmung. Diese Fragen sind der Regelung in einer BV vorbehalten.

Kommentiert [St.28]: Eben. Darum s.o. – es ist unzulässig, ein Thema, das mitbestimmt ist, parallel individualrechtlich zu regeln, solange nicht der BR dem zumindest zugestimmt hat oder eben eine BV dazu mit dem AG abgeschlossen hat.

Kommentiert [St.29]: Es ist rätselhaft, warum hier eine andere Formulierung gewählt wird, als oben zur selben Rubrik. Die gesetzlichen Aussagen sind identisch.

Verarbeitung nicht die ausschließliche Grundlage für Entscheidungen mit negativen Folgen oder erheblichen Beeinträchtigungen für die betroffenen Mitarbeiter sein.

Um Fehlentscheidungen zu vermeiden, muss in automatisierten Verfahren gewährleistet sein, dass eine inhaltliche Bewertung des Sachverhalts durch eine natürliche Person erfolgt und diese Bewertung Grundlage für die Entscheidung ist. Dem betroffenen Mitarbeiter müssen außerdem die Tatsache und das Ergebnis einer automatisierten Einzelentscheidung mitgeteilt und die Möglichkeit einer Stellungnahme gegeben werden.

- Telekommunikation und Internet

Telefonanlagen, E-Mail-Adressen, 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 und Internetnutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer können Schutzmaßnahmen an den Übergängen in das X- 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 Internets sowie der internen sozialen Netzwerke zeitlich befristet protokolliert werden.

Kommentiert [St.30]: Das ist mitbestimmungspflichtig.

Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze oder Richtlinien des Unternehmens 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.

Kommentiert [St.31]: Siehe vorhergehenden Kommentar.

- Videoüberwachung und Zutrittskontrolle

Der Zutritt zum Gebäude wird mittels Transponder und einem Zutrittssystem geregelt. Außerhalb der Arbeitszeiten (Nachts, an Wochenenden und Feiertagen) werden die Eingangsbereiche kameraüberwacht.

Übermittlung personenbezogener Daten

Kommentiert [St.32]: Ist das jetzt wieder allgemeine Aussage, als eine, die nicht speziell für das Arbeitsrecht gelten soll ? Struktur ist intransparent.

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb oder innerhalb des Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten, wie sie im vorausgegangenen Abschnitt zu Kunden, Partnern und Mitarbeitern beschrieben wurden.

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 Unternehmens in einem Drittstaat, d.h. außerhalb des Europäischen Wirtschaftsraums, muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung - beispielsweise zur Erfüllung der Zustellung von Paketen - erfolgt und dazu zwingend erforderlich ist.

Kommentiert [St.33]: Das ist eine missverständliche und extrem verkürzte Aussage, die so schon wieder falsch ist, weil sie wesentliche Elemente weglässt.

Im Falle einer Datenübermittlung von Dritten an das Unternehmen muss sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

Kommentiert [St.34]: Unverständlich.

Auftragsverarbeitung und gemeinsame Verantwortung

Eine Auftragsverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne dass ihm die Verantwortung für den zugehörigen Geschäftsprozess übertragen wird. Hierbei greift Art. 28 DSGVO. In diesen Fällen ist mit den externen Auftragnehmern eine Vereinbarung über eine Auftragsverarbeitung abzuschließen. Dabei behält die X-Gmbh die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung, deren Kontrolle sowie die Wahrnehmung der Rechte der von der Verarbeitung betroffenen Personen.

Sofern zwei oder mehrere verantwortliche Stellen die Mittel und die Zwecke einer Datenverarbeitung jedoch gemeinsam bestimmen, liegt eine Datenverarbeitung nach Art. 26 DSGVO vor, die dann ebenfalls einer besonderen vertraglichen Vereinbarung bedarf. Dies ist bei der X-Gmbh im Verhältnis zum Stuttgarter Verlagskontor (SVK) der Fall.

- Auftragsverarbeitung nach Art. 28 DSGVO

Bei einer Auftragsverarbeitung nach Art. 28 DSGVO darf der Auftragnehmer personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrags sind deshalb 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 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 Daten Sicherheit 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 Auftragsverarbeiturg in Drittstaaten mit dem Auftragnehmer und möglichen Subunternehmern
   b. Teilnahme des Auftragnehmers an einem von der EU anerkannten Zertifizierungssystem zur Schaffung eines angemessenen Datenschutzniveaus (beispielsweise Privacy Shield)
   c. Anerkennung verbindlicher Unternehmensregeln des Auftragnehmers zur Schaffung eines angemessenen Datenschutzniveaus durch die zuständigen Datenschutzaufsichtsbehörden

- Verarbeitung nach Art. 26 DSGVO (gemeinsam für die Verarbeitung Verantwortliche)

Bei einer gemeinsamen Verarbeitung im Rahmen des Art. 26 DSGVO legen die Vertragsparteien in einer schriftlichen Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß DSGVO erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Personen angeht, und wer welchen Informationspflichten gemäß Art. 13 und 14 DSGVO nachkommt, sofern

Kommentiert [St.35]: So aufgrund Weglassung falsch. Sie müssen auch geeignete Garantien bieten.

Kommentiert [St.36]: Teilweise falsche, teilweise entstellende Wiedergabe des Gesetzestextes. (Auch) Hier stellt sich die Frage nach dem Sinn des gesamten Papiers: wenn es eine Richtlinie ist, dann hat sie Weisungscharakter. Wie soll eine unzutreffende Wiedergabe von Gesetzestext in Weisung erwachsen ? Warum gibt man nicht gleich den Gesetzestext her ?
Oder noch deutlicher:
Wenn man eine Weisung kreieren will, dann sollte man den Gesetzestext bzw. den Arbeitsvertrag ausfüllen, anstatt ihn falsch, fragmentarisch oder gar nicht abzubilden.
Kurz: es ist sinnlos.
Und noch weiter: wie schon oben gesagt, hat keiner der „normalen“ AN auch nur im Ansatz die Befugnis oder gar die Pflicht, sich Gedanken über juristische Fachfragen zur Auslandsdatenverarbeitung zu machen. Das ist Aufgabe des AG – er hat die technisch-organisatorischen Maßnahmen zu treffen, um AN vor der Konfrontation mit solchen Fragen zu schützen. Dazu gehört, dass der bDSB und die entsprechenden Fachjuristen diese Fragen klären, Abläufe dazu festlegen und dafür haften. Nichts davon ist Aufgabe eines normalen MA.
Wenn man dann eine Weisung erteilen will, dann kann sie sich auf die konkreten Ausgestaltungsergebnisse der GF zu den o.g. Aufgaben beziehen. Was hier passiert, ist untaugliche Regelungswut ohne die Klärung der Frage, was man damit eigentlich erreichen will und innerhalb welcher rechtlichen Rahmenbedingungen und Grenzen (z.B. der Mitbestimmung) man sich bewegt.
Das ganze Papier folgt hauptsächlich einem Zweck: „Herr Lehrer, ich weiß was“.

und soweit die jeweiligen Aufgaben der Verantwortlichen nicht durch Rechtsvorschriften der EU oder der Mitgliedstaaten, denen die Verantwortlichen unterliegen, festgelegt sind.

Die Vereinbarung muss beinhalten:

1. die Angaben zu einer Anlaufstelle für die betroffenen Personen;
2. die jeweiligen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen.

Kommentiert [St.37]: Siehe vorhergehenden Kommentar: hier noch krasser – das Thema geht den MA absolut nichts an. Er hat auch nichts davon, dass es hier steht.

Datenschutzfreundliche Technik und Voreinstellungen

Sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen zu treffen, die dafür ausgelegt sind, die Datenschutzgrundsätze wirksam umzusetzen. Dabei sind der Stand der Technik, die Implementierungskosten und Art, Umfang, Umstände und Zwecke der Verarbeitung sowie die unterschiedlichen Eintrittswahrscheinlichkeiten und die Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheitert natürlicher Personen zu berücksichtigen. Außerdem sind die notwendigen Garantien in die Verarbeitung aufzunehmen, um die Rechte der betroffenen Personen zu schützen und den Anforderungen der DSGVO gerecht zu werden.

Die X-Gmbh ergreift geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich personenbezogene Daten nur dann verarbeitet werden, wenn dies für den jeweiligen Verarbeitungszweck erforderlich ist.

Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Dazu zählen unter anderem die Verarbeitung nur von pseudonymisierten Daten, der Einsatz besonderer Authentifizierungsmaßnahmen (Zwei-Faktor-Authentifizierung), die Vorbelegung mit datenschutzfreundlichen Grundeinstellungen in Checkboxen oder das Kennzeichnen von zu erhebenden Informationen als freiwillig.

Kommentiert [St.38]: Was sagt mir das als MA ? Nichts.

Rechte des Betroffenen

Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DSGVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und 21 DSGVO Gebrauch, so erfolgt die Bearbeitung durch die GL und den Datenschutzbeauftragten. Die Auskünfte sind binnen einer Frist von vier Wochen zu erteilen.

Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalverwaltung erfüllt.

Es ist sicherzustellen, dass dem Betroffenen seine Daten auf Wunsch in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt werden können. Welcher Standard diesen Anforderungen genügt, ist im Vorfeld einvernehmlich durch den Datenschutzbeauftragten und die GL festzulegen. Dabei müssen nur solche Daten bereitgestellt werden, die vom Betroffenen auch an die X-Gmbh übermittelt wurden.

Auskünfte sind generell schriftlich an die X-Gmbh bekannte Adresse zu erteilen. Zur Sicherstellung der Identität des Auskunftssuchenden muss mindestens die Adresse und Geburtsdatum erfragt werden. Elektronische Auskünfte werden nur erteilt, wenn der Postweg bestätigt wurde. Bei Zweifeln an der Richtigkeit der Angaben muss ein sicheres Verfahren (z.B. Post-ID Verfahren) zur Bestätigung der Angaben verwendet werden.

Vertraulichkeit der Verarbeitung

Personenbezogene Daten unterliegen der Vertraulichkeit. 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. Dieses Prinzip ist sowohl durch die eigene IT als auch in Auftragsverarbeitungs- oder Softwareentwicklungsprozessen sicherzustellen.

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

Kommentiert [St.39]: O.k., das ist ausnahmsweise mal Weisungstext. Allerdings unterschreiben alle MA das sowieso im Zuge ihrer Vertraulichkeitsverpflichtung. Daher hier überflüssig.

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 an dem Stand der Technik, den vor der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren.

Der verantwortliche Fachbereich kann dazu den Datenschutzkoordinator zurate ziehen. Die technisch-organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des unternehmensweiten Informationssicherheitsmanagements und müssen kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst werden.

Datenschutzfolgeabschätzung

Hat eine Form der Verarbeitung personenbezogener Daten, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so muss vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchgeführt werden (Art. 35 EU-DSGVO).

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

Die Verantwortung für die Durchführung der Datenschutzfolgeabschätzung haben der Datenschutzbeauftragte und der Datenschutzkoordinatoren. Die Datenschutzfolgeabschätzung ist entsprechend zu dokumentieren.

Datenschutzkontrolle

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

Die zuständige Aufsichtsbehörde der X-Gmbh ist aktuell: Landesbeauftragten für Datenschutz und Informationsfreiheit, Musterstraße 11 , D-11111 Musterstadt

Datenschutzvorfälle

Jeder Mitarbeiter muss dem Datenschutzkoordinator, Datenschutzbeauftragten und dem Geschäftsführer unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder andere Vorschriften zum Schutz personenbezogener Daten melden.

Beispiele für solche Vorfälle sind:

a) unrechtmäßige Übermittlung personenbezogener Daten an Dritte,
b) unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten oder
c) Verlust personenbezogener Daten.

Verantwortlichkeiten und Sanktionen

Die Geschäftsführung des Unternehmens ist verantwortlich für die Datenverarbeitung. Damit ist sie verpflichtet, sicherzustellen, dass die gesetzlichen und die in der Datenschutzrichtlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (zum Beispiel nationale Meldepflichten), was sie durch organisatorische, personelle und technische Maßnahmen sicherstellt.

Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.

Kommentiert [St.40]: Das ist falsch. Fraglich ist allerdings, warum hier mal von „Maßnahmen“ und mal von „Vorgaben“ die Rede ist. Es bleibt rätselhaft, was damit geeint sein soll (eventuell sogar dasselbe ?). Auf diese Weise kann keine Haftung begründet werden.

Die für Geschäftsprozesse und Projekte fachlich Verantwortlichen müssen den Datenschutzkoordinator und den Datenschutzbeauftragten rechtzeitig über neue Verarbeitungen personenbezogener Daten informieren. Bei Datenverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte 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.

Musterstadt, den xxxxx gez.

Name Geschäftsführerin X-Gmbh