DATENSCHUTZRICHTLINIE

Datenschutzrichtlinie der KD GmbH und KD Europe

Um unsere Geschäftsprozesse zu ermöglichen und die damit verbundenen Pflichten zu erfüllen, muss KD nicht nur Geschäftsdaten verarbeiten, sondern auch Daten, die sich auf Einzelpersonen, vor allem unsere Mitarbeiter:innen, aber auch andere Personen, mit denen wir zusammenarbeiten, beziehen. Neben internen Personaldaten bedürfen die Daten unserer Kunden, Lieferanten, Geschäftspartner sowie Bewerber besonderen Schutz. Wir sind uns unserer Verantwortung im Bereich des Datenschutzes bewusst.

Grundsatzerklärung

Wir verpflichten uns stets alle führenden Datenschutz- und Sicherheitsstandards einzuhalten. Die gesetzlichen Vorschriften verlangen, dass personenbezogene Daten so verarbeitet werden, dass die Rechte der durch die Verarbeitung betroffenen Personen auf Vertraulichkeit und Integrität ihrer Daten gewährleistet werden. Bei der Erhebung, Speicherung, Verarbeitung oder Übertragung personenbezogener Daten (z. B. Name, Adresse, Telefonnummer, Geburtsdatum, Informationen über den Gesundheitszustand) von Mitarbeiter:innen, Kunden oder anderen Dritten achten wir daher auf größte Sorgfalt und strenge Vertraulichkeit. Wir achten somit das Recht auf Privatsphäre und erfüllen damit die Bestimmungen der EU-Datenschutz-Grundverordnung (EU-DS-GVO).

Hauptverantwortung für alle Themen in Bezug auf Datenschutz trägt die Geschäftsführung. Verantwortlichkeit im Tagesgeschäft tragen die jeweiligen Bereichsleiter.

Alle unsere Mitarbeiter:innen durchlaufen eine verpflichtende jährliche Online-Schulung zum Datenschutz.

Wir bei KD sind uns einig, dass Verstöße gegen diese Datenschutzrichtlinie zu arbeitsrechtlichen Konsequenzen für die zuwiderhandelnden Personen führen.

Verpflichtungen zu personenbezogenen Daten

Eine besondere Rolle in Bezug auf den Umgang mit Daten nehmen unsere Mitarbeitenden ein, da diese regelmäßig personenbezogene Daten verarbeiten. Unseren Mitarbeitenden ist es nur gestattet, personenbezogene Daten in dem Umfang und in der Weise zu verarbeiten, wie es zur Erfüllung der ihnen übertragenen Aufgaben erforderlich ist. Es ist ihnen untersagt, personenbezogene Daten unbefugt zu verarbeiten. Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Einwilligung bzw. eine gesetzliche Regelung die Verarbeitung erlauben oder eine Verarbeitung dieser Daten vorgeschrieben ist. Die Grundsätze der EU-DS-GVO für die Verarbeitung personenbezogener Daten sind in Art. 5 Abs. 1 EU-DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen:

Personenbezogene Daten müssen

a. auf rechtmäßige Weise und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden;

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

c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;

e. 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;

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit");

Diese Vorgaben zum Umgang mit personenbezogenen Daten gelten verpflichtend für Kunden- und Lieferantendaten, Daten von Geschäftspartnern, Personaldaten sowie Bewerbungsdaten.

Verpflichtung zur Aufbewahrungsfrist

Die Daten werden ausschließlich so lange aufbewahrt, bis der vertragliche Zweck erfüllt ist und auch keine gesetzliche Archivierungs- oder Aufbewahrungsvorgabe dem entgegensteht.

Zugriff auf die Daten

Betroffene Personen haben die Möglichkeit auf ihre Daten zuzugreifen, um personenbezogene Daten zu löschen, zu ergänzen oder zu ändern.

Daten zur Weitergabe an Dritte

Grundsätzlich verpflichtet sich KD dazu, Nutzerdaten nur zum zuvor angegebenen Zweck zu nutzen. Prinzipiell werden keine Kundendaten an Dritte weitergegeben. Sollten Daten an Dritte weitergeleitet werden, sind wir verpflichtet, die dritten Parteien zur Einhaltung der Unternehmensrichtlinie Datenschutz zu verpflichten und die Daten verschlüsselt zu übermitteln. Die Erhebung von Nutzerdaten erfolgt immer rechtmäßig und transparent mit ausdrücklicher Zustimmung der betroffenen Person.

Datenschutzmanagement und Sicherstellung der Einhaltung

Das Thema Datenschutzmanagement hat bei KD einen hohen Stellenwert und liegt daher in der Verantwortung direkt bei der Geschäftsführung. Die betrieblichen Datenschutzbeauftragten stehen den Mitarbeiter: innen für datenschutzrechtliche Fragestellungen zur Verfügung. Das Thema Datenschutz ist daher zentraler Bestandteil unserer Nachhaltigkeitsstrategie bei KD. Das Ziel, den Datenschutz kontinuierlich zu vertiefen sowie entsprechende Maßnahmen und Verantwortlichkeiten, sind in der Strategie konkret festgehalten.

Anhand der Datenschutzrichtlinie haben wir uns als KD konkrete Ziele gesetzt, die entsprechend kommuniziert werden. Zudem werden unsere Mitarbeiter:innen jährlich via Onlinekursen hierzu geschult. Unsere Mitarbeiter: innen berichten an den/die zuständige Abteilungsleitung, die wiederum an die Geschäftsführung berichten.

Verantwortung unserer Mitarbeitenden

Jede und jeder unserer Mitarbeitenden bei KD ist dafür verantwortlich, dass:

- die ihnen anvertrauten Daten, Datenträger und Ausdrucke unter Verschluss gehalten werden, wenn sie nicht unmittelbar daran arbeiten. Hierzu sind insbesondere Bildschirme und PCs bei Abwesenheit vom Arbeitsplatz zu sperren.

- sie nicht einfach mit der Antwortfunktion auf E-Mails mit vertraulichem Inhalt reagieren, sondern vorher Absenderlisten überprüfen. Dies gilt auch für die E-Mail-Empfänger im Allgemeinen, insbesondere bei der Verwendung der „CC"-Funktion. Dabei ist zu beachten, dass vertrauliche Informationen grundsätzlich nicht per E-Mail zu versenden sind, wenn keine Verschlüsselung möglich ist. Ferner ist auf die Virengefahr bei unbekannten E-Mail-Anhängen zu achten.

- keine vertraulichen Informationen per Fax verschickt werden. Falls sie dies doch in Ausnahmefällen tun müssen, werden Vorkehrungen getroffen (z. B. telefonische Absprache wegen Anwesenheit des Empfängers, Doppelkontrolle der Richtigkeit der Empfängernummer).

- das Passwort keinem Unbefugten zugänglich wird. Daher dürfen nur sichere Passwörter verwenden werden (z. B. mit Sonderzeichen, keine Namen) und diese müssen regelmäßig gewechselt werden.

- nicht mehr benötigte Datenträger und Ausdrucke so vernichtet werden, dass eine missbräuchliche Verwendung nicht möglich ist.

- Laptops und Notebooks und sonstige mobile Betriebsmittel bei Reisen sorgfältig gesichert und vor fremden Blicken geschützt werden; ein etwaiger Geräteverlust muss sofort der IT-Abteilung gemeldet werden.

- keine vertraulichen Telefonate vom Mobiltelefon aus in der Öffentlichkeit geführt werden, z. B. auf Reisen.

- sie nur Software und Apps verwenden, die vom Unternehmen freigegeben sind. Sie keine betriebsfremden Betriebsmittel, wie z. B. USB-Sticks, unbefugt verwenden.

- sie keine unternehmensinternen Informationen unbefugt im Internet verbreiten, insbesondere in sozialen Netzwerken.

- sie nur die personenbezogenen Daten verarbeiten, die sie für ihr Aufgabengebiet benötigen und regelmäßig prüfen, welche Daten sie nicht mehr benötigen und diese entsprechend den internen Löschvorgaben löschen.

- Betroffenenrechte wie Auskunfts- Berichtigungs- oder Löschansprüche sowie Widerspruchsrechte entsprechend der internen Regelungen unverzüglich an die verantwortliche Stelle weitergeleitet werden. Dies gilt auch für sog.

Datenpannen, d.h. wenn auf personenbezogene Daten unbefugt zugegriffen wird oder diese anderweitig abhandenkommen (z. B. Verlust).

Richtlinie für die Nutzung der Internet-Dienste am Arbeitsplatz

Die vom Gesetzgeber auferlegten Datenschutzbestimmungen und die für KD unabdingbare Sicherheit in der Informationsverarbeitung zwingen uns die nachfolgend aufgeführte Regelung einzuführen:

Im Rahmen dieser Maßgaben ist es anerkannt, dass die dienstlich motivierte gelegentliche Privatnutzung von E-Mail und der Internet-Dienste, unter Nutzung der technischen Einrichtungen der Firma bzw. der United Waterways Firmen E-Mail Adresse, gestattet ist. Dies umfasst z. B. private Mitteilungen aufgrund dienstlicher Anlässe (ähnlich der Telefonnutzung, z. B. Mitteilung über Arbeitsende) oder bzw. für den Fall der Privatnutzung in dem eine Verschiebung aus dienstlichen Gründen in die Freizeit nicht möglich ist.

Grundsätzlich gilt folgendes:

2.1. Der Internet-Zugang und die E-Mail-Dienste werden ausschließlich für die Erfüllung geschäftlicher Aufgaben genutzt.

2.2. Eine private Nutzung des Internet-Zugangs und der E-Mail-Dienste ist nicht zulässig.

2.3. Die bei der Nutzung der E-Mail- und Internet-Dienste anfallenden personenbezogenen Daten (Protokoll- oder Verbindungsdaten, d. h. Aufzeichnungen über Tag, Uhrzeit, Beginn und Dauer einschließlich der angefallenen Gebühreneinheiten, sowie der Absender- und Zieladressen) werden protokolliert. Personenbezogene Daten, die zur Sicherstellung eines ordnungsgemäßen Betriebes der E-Mail-Dienste erhoben und gespeichert werden, unterliegen der besonderen Zweckbindung nach § 31 Bundesdatenschutzgesetz (BDSG). Ein Zugriff auf diese Daten von Seiten des Unternehmens erfolgt bei Bedarf, so z.B. zur Klärung von Geschäftsprozessen, bei Viren usw. sowie zur Analyse und Behebung von technischen Fehlern, Gewährleistung der Systemsicherheit, Optimierung des Netzwerkes, außerdem zur Stichprobenkontrolle, zur ordnungsgemäßen Nutzung und zur Missbrauchskontrolle.

Eine Unterscheidung von dienstlicher und privater Nutzung der Internetdienste auf technischem Wege erfolgt nicht. Die Protokollierung und Kontrolle erstreckten sich auf jegliche Art der Nutzung.

2.4. Die vorstehende Regelung ermöglicht nicht den Zugriff auf die Daten von Einzelpersonen ohne Grund.

Benachrichtigung bei Änderungen in den Datenschutzvorgaben und Vorfällen

Wir verpflichten uns dazu betroffene Personen im Fall von Änderungen der Richtlinien und bei Datenschutzverletzungen sowie bei einem Datensicherheitsvorfall rechtzeitig zu benachrichtigen.

Vermutetes Fehlverhalten sowie tatsächliche oder potenzielle Verstöße gegen diese Grundsätze sind umgehend zu melden. Sollten Bedenken hinsichtlich des Datenschutzes aufkommen, haben betroffene Personen die Möglichkeit der Bereichsleitung und/oder Geschäftsführung Bedenken zu äußern. Betroffene Personen haben zudem die Möglichkeit, unsere Whistleblowing-Wege zu nutzen: Sollte uns an unserem eigenen Verhalten, dem von Kolleg:innen, oder am Verhalten Dritter etwas auffallen, was unter Umständen gegen eine der oben beschriebenen Regelungen verstößt, wenden wir uns an unsere Führungskraft oder an unsere Ombudsperson Frau Nicole Trebinger. Die Geschäftsführung garantiert, dass jede Meldung, die

in gutem Glauben und mit guter Absicht getätigt wurde, unter keinen Umständen negative Folgen für die Hinweisgeberin/den Hinweisgeber haben wird

Als Ombudsfrau, Rechtsanwältin und zertifizierte Mediatorin wird Frau Trebinger die absolute Anonymität des Hinweisgebers/der Hinweisgeberin zu jedem Zeitpunkt des Verfahrens wahren. Sie kann bei Bedarf eine erste juristische Einschätzung geben und weitere Schritte ausloten. Die Meldungen bei der Ombudsfrau müssen im guten Glauben und ohne Arglist erfolgen. Sie wird die Geschäftsführung oder die entsprechenden Führungskräfte über den jeweiligen Sachverhalt informieren und hinsichtlich des möglichen Handlungsbedarfs beraten. Frau Trebinger ist unter folgenden Kontaktdaten erreichbar:

DIGIT@ LAW® Rechtsanwälte
Mittelstraße 12-14, 50672 Köln,
02 21 17 73 87 90
hinweisgeber@digita-law.de

Folgen bei Nichteinhaltung

Verstöße gegen diese Verpflichtung können mit Geldstrafe und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder speziellen Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadensersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Die sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen ergebende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Neben dieser Datenschutzrichtlinie sind weitergehende gesetzliche wie interne Regelungen (insbesondere die IT-Richtlinie) in diesem Zusammenhang zu beachten.

Kenntnisnahme des Dokuments

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung nebst Anlage habe ich erhalten. Diese Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

_____

Köln, den _____

Einverständniserklärung zum Austausch von Personalinformationen

Im Rahmen Ihres Arbeitsverhältnisses werden Ihre personenbezogenen Daten (Name, Vorname, Standort, Abteilung/Funktion, persönliche Durchwahl -Telefon und -Fax-Nummern, persönliche United Waterways-E-Mail-Adresse, Geburtsdatum, Betriebszugehörigkeit) in Mail- und Kommunikationssystemen gespeichert und im Intranet im Rahmen des United Waterways-Adressbuches allen Mitarbeitenden aller United Waterways - Unternehmen zugänglich gemacht.

Über die Speicherung, Nutzung und Übermittlung meiner oben genannten Daten wurde ich unterrichtet und bin damit einverstanden.

_____

Köln, den _____

Ergänzung: Begrifflichkeiten und Verhaltenskodex

Die vorliegende Auswahl gesetzlicher Vorschriften soll einen Überblick über das datenschutzrechtliche Regelwerk verschaffen. Die Darstellung erfolgt exemplarisch und ist keineswegs vollständig. Für weitere Informationen zu datenschutzrechtlichen Fragestellungen stehen die betrieblichen Datenschutzbeauftragten zur Verfügung.

Begrifflichkeiten

Art. 4 Nr. 1 DS-GVO: „Personenbezogene Daten" [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") 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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „Verarbeitung" [meint] jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten 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, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Haftung/Strafbarkeit

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung […] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten […] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

§ 42 BDSG (neu): (1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder

2. auf andere Art und Weise zugänglich macht und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder

2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche, die oder der Bundesbeauftragte und die Aufsichtsbehörde.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

§ 43 BDSG (neu):

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 30 Absatz 1 ein Auskunftsverlangen nicht richtig behandelt oder

2. entgegen § 30 Absatz 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.

(2) Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Gegen Behörden und sonstige öffentliche Stellen im Sinne des § 2 Absatz 1 werden keine Geldbußen verhängt.

(4) Eine Meldung nach Artikel 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Artikel 34 Absatz 1 der Verordnung (EU) 2016/679 darf in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.