Datenschutzkonzept für KSH Schleswig GmbH Metall und Recycling

1. Grundsätze

Der Schutz personenbezogener Daten ist uns ein wichtiges Anliegen. Deshalb verarbeiten wir die personenbezogenen Daten unserer Mitarbeiter, Kunden sowie Geschäftspartner in Übereinstimmung mit den anwendbaren Rechtsvorschriften zum Schutz personenbezogener Daten und zur Datensicherheit.

In dieser Datenschutzrichtlinie wird beschrieben, welche Arten von personenbezogenen Daten wir erheben, wie diese Daten genutzt werden, an wen sie übermittelt werden und welche Wahlmöglichkeiten und Rechte betroffene Personen im Zusammenhang mit unserer Verarbeitung der Daten haben.

Außerdem beschreiben wir, mit welchen Maßnahmen wir die Sicherheit der Daten gewährleisten und wie betroffene Personen Kontakt mit uns aufnehmen können, wenn Sie Fragen zu unserer Datenschutzpraxis haben.

Diese Richtlinie regelt die datenschutzkonforme Informationsverarbeitung und die insoweit bei genannten Unternehmen Gruppe bestehenden Verantwortlichkeiten. Alle Mitarbeiter sind zur Einhaltung der Richtlinie verpflichtet.

Sie richtet sich an

- die Geschäftsleitung
- den IT-Systemadministrator
- die Annahme
- die Buchhaltung
- den Vertrieb
- die Auftragsabwicklung inkl. Rechnungsabteilung
- alle Benutzer, die die zur Verfügung gestellten Systeme für die Erledigung ihrer betrieblichen Aufgaben nutzen.

für die Gesellschaften und Standorte

- KSH Schleswig GmbH Metall und Recycling

  Margarethenwallstr. 2, 24837 Schleswig

Dabei gelten folgende Grundsätze:

- Die Hardware und Software zum Zwecke der Datenverarbeitung sind ausschließlich für betriebliche Aufgaben zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung durch die Geschäftsleitung.

- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die Geschäftsleitung stellt sicher, dass ihre Mitarbeiter über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.
- Die Geschäftsleitung berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie der Geschäftsleitung gegenüber auskunftspflichtig.

2. Beschaffung Hard- und Software

2.1
Die Beschaffung von Hard- und Software erfolgt grundsätzlich erst nach Genehmigung durch die Geschäftsleitung. Bereits bei der Auswahl von Hard- und Software wird das Prinzip der Gewährleistung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen als ein tragendes Kriterium beachtet.
Die Verfahrensanweisung „Checkliste zur Beachtung der Anforderungen an Privacy-by Design / Privacy-by-Default“ (Anlage 1) ist maßgebend.

2.2
Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist die Geschäftsleitung rechtzeitig vorab von der anfordernden Stelle zu informieren (siehe 5.2). Die Beschaffung erfolgt erst nach Freigabe durch die Geschäftsleitung. Die Geschäftsleitung entscheidet, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die Durchführung einer Datenschutz-Folgenabschätzung richtet sich nach der Verfahrensanweisung „Risikominimierung durch Datenschutz-Folgenabschätzung“ (Anlage 2)

2.3
Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden. Die dienstliche Nutzung privater Hard- und Software im heimischen und außerbetrieblichen Bereich (z.B. private Notebooks) bedarf der Genehmigung durch die IT-Abteilung im Einzelfall.

2.4
Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind die DV-Abteilung und die Geschäftsleitung unverzüglich zu informieren.

3. Verpflichtung/Schulung der Mitarbeiter

3.1
Jeder Mitarbeiter, der Umgang mit personenbezogenen Daten hat, ist auf einen vertraulichen Umgang mit personenbezogenen Daten und die Einhaltung dieser Richtlinie zu verpflichten.

3.2
Die Schulung der Mitarbeiter erfolgt regelmäßig, jedoch mindestens einmal im Jahr.

4. Transparenz der Datenverarbeitung

4.1
Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Daten- die Geschäftsleitung ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO.

4.2
Der für ein Verfahren Verantwortliche meldet Veränderungen die Geschäftsleitung zur Aktualisierung des Verzeichnisses. Unabhängig von dieser Meldung ist die Geschäftsleitung bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren von Beginn einzubeziehen.

4.3
Soweit der für ein Verfahren Verantwortliche feststellt, dass die beabsichtigte Verarbeitung einer Datenschutz-Folgenabschätzung unterliegt, teilt er dies umgehend mit. Das Verfahren darf erst nach Zustimmung der Geschäftsleitung durchgeführt werden. Im Zweifel entscheidet die Geschäftsleitung.

4.4
Macht ein Betroffener von seinem Auskunftsrecht nach Art. 15 DS-GVO oder seinem Korrektur- oder Widerspruchsrecht nach Art. 16 und Art. 21 DS-GVO Gebrauch, so erfolgt die Bearbeitung durch den für das Verfahren Verantwortliche. 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.

5. Erhebung / Verarbeitung von personenbezogenen Daten

5.1
Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Hierbei sind auch die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DS-GVO zu beachten.
Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

5.2
Personenbezogene Daten werden zum Zwecke der Vertragsabwicklung zwischen den Verantwortlichen der oben genannten Gesellschaften arbeitsteilig verarbeitet. Diese gemeinsame Verarbeitung erfolgt für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen. Die gemeinsame Verarbeitung gilt weiterhin für die Durchführung der aus den Beschäftigtenverhältnissen erwachsenen rechtlichen Verpflichtungen (z.B. Lohn- und Gehaltsabrechnungen). Über diese gemeinsame Verarbeitung bestehen Vereinbarungen, in denen in transparenter Form die jeweiligen Verpflichtungen, insbesondere die Informationspflichten gegenüber den Betroffenen, dargelegt werden.

5.3
Es wird sichergestellt, dass Betroffene keiner Entscheidung unterworfen werden, die ausschließlich auf einer automatisierten Verarbeitung beruhen und zugleich den Betroffenen gegenüber eine rechtliche Wirkung entfalten oder sie in ähnlicher Weise erheblich beeinträchtigen (bspw. Profiling).

5.4
Vor Einführung neuer Arten von Erhebungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen zu prüfen. Grundsätzlich ist eine Zweckänderung nur dann zulässig, wenn die Verarbeitung mit denjenigen Zwecken vereinbar ist, für die die Daten ursprünglich erhoben worden sind. Eine Zweckänderung ist auch zulässig, wenn eine Einwilligung der betroffenen Person durch den Verantwortlichen eingeholt wird. Gleichzeitig hat der für die Verarbeitung Verantwortliche vor der Erhebung bzw. der Speicherung von Daten schriftlich festzulegen, ob und in welcher Art und Weise der gesetzlichen Benachrichtigungspflicht des Betroffenen zu genügen ist.

5.5
Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung oder ein die Weitergabe rechtfertigendes legitimes Interesse des Unternehmens besteht und die Identität des Anfragenden zweifelsfrei feststeht. Im Zweifel ist die Geschäftsleitung zu kontaktieren.

6. Datenhaltung / Versand / Löschung

6.1
Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher bedarf der Genehmigung durch die IT-Abteilung. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

6.2
Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

6.3
Gesetzliche Aufbewahrungsfristen und Löschungstermine sind zu beachten. Die IT-Abteilung ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten in Sicherungskopien zu informieren.

6.4
Bei der Weiter- oder Rückgabe nicht mehr benötigter IT-Komponenten ist der Benutzer verpflichtet, dafür zu sorgen, dass zuvor sämtliche Daten wirksam gelöscht wurden.

7. Externe Dienstleister / Auftragsverarbeitung / Wartung

Sollen externe Dienstleister erstmals mit der Verarbeitung personenbezogener Daten bzw. einzelnen Verarbeitungsschritten (z.B. Erhebung, Löschung = Entsorgung) bzw. mit Tätigkeiten (z.B. Wartung, Reparatur) beauftragt werden, bei denen sie die Möglichkeit der Kenntnis personenbezogener Daten bekommen, so ist mit diesen ein Vertrag unter vollständiger Berücksichtigung der Anforderungen des Art. 28 DS-GVO zu schließen.

8. Sicherheit der Verarbeitung

8.1
Für jedes Verfahren sind eine dokumentierte Schutzbedarfsfeststellung sowie eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Dieses erfolgt im Rahmen der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten.

8.2
Neben dieser Richtlinie bestehen ergänzende Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen.

9. Rechenschafts- und Dokumentationspflicht

Die Einhaltung der Vorgaben, die sich aus dieser Richtlinie ergeben, muss jederzeit nachweisbar sein. Eine Nachweisbarkeit hat insbesondere durch eine schlüssige und nachvollziehbare schriftliche Dokumentation hinsichtlich getroffener Maßnahmen und dazugehöriger Abwägungen zu erfolgen.