KIEPE ELECTRIC

Datenschutz Policy der Kiepe Electric Ges.m.b.H.

Revision 1.0 – Mai 2018

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 der Kiepe Electric Ges.m.b.H. bestehenden Verantwortlichkeiten. Alle Mitarbeiter sind zur Einhaltung der Richtlinie verpflichtet.

Sie richtet sich an

- die Personen oder Abteilungen, die über den Einsatz/die Bereitstellung eines Anwendungssystems entscheiden (IT/Organisation)
- die Personen oder Abteilungen, die über die Nutzung der Systeme für ihre Aufgaben entscheiden (das sind die Fachabteilungen)
- Benutzer, d.h. diejenigen, die ein zur Verfügung gestelltes System für die Erledigung ihrer betrieblichen Aufgaben nutzen (bei Speicherung personenbezogener Daten auf einem Arbeitsplatzrechner entscheidet der einzelne Benutzer ggf. auch über die im System erfolgende Verarbeitung und die dazu verwendeten Programme)
- den Datenschutzkoordinator (DSK), der ihre Umsetzung beratend und kontrollierend begleitet und die ihm speziell zugewiesenen Aufgaben wahrzunehmen hat.

Dabei gelten folgende Grundsätze:

- Die DV-Hard- und Software sind für betriebliche Aufgaben, und zwar für die jeweils vorgesehenen Zwecke, zu verwenden und gegen Verlust und Manipulation zu sichern. Eine Nutzung für private Zwecke bedarf der ausdrücklichen Genehmigung.
- Jeder Mitarbeiter ist in seinem Verantwortungsbereich für die Umsetzung der Richtlinie verantwortlich. Die Einhaltung muss von ihm regelmäßig kontrolliert werden.
- Die für die Verarbeitungen der eingesetzten Systeme Verantwortlichen stellen sicher, dass ihre Mitarbeiter (Benutzer) über diese Richtlinie informiert werden; das gilt auch für temporär Beschäftigte.
- Der Datenschutzkoordinator berät bei der Umsetzung der Richtlinie und prüft deren Einhaltung. Insoweit sind alle Adressaten der Richtlinie dem DSK auskunftspflichtig.

2. Der betriebliche Datenschutzkoordinator

2.1 Die Kiepe Electric Ges.m.b.H. hat einen Datenschutzkoordinator (DSK) und einen Abwesenheitsvertreter bestellt. Die Kontaktdaten des Datenschutzkoordinators sind zu finden unter:

Herr Ing. Mag. Stefan Ofner,

Der DSK nimmt die ihm aus dieser Richtlinie zugewiesenen Aufgaben bei weisungsfreier Anwendung seines Fachwissens sowie seiner beruflichen Qualifikation war.

2.2 Der Datenschutzkoordinator unterrichtet und berät die Unternehmensleitung sowie die Beschäftigten hinsichtlich ihrer Datenschutzpflichten. Ihm obliegt die Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter.

Im Falle risikoreicher Datenverarbeitungen steht der DSK dem Verantwortlichen beratend bei der Abschätzung des Risikos zur Seite.

2.3 Der DSK berichtet unmittelbar der Unternehmensleitung.

2.4 Der DSK wird frühzeitig in alle Datenschutzfragen eingebunden und wird sowohl von der Unternehmensleitung als auch den Beschäftigten bei der Erfüllung seiner Aufgaben unterstützt.

2.6 Die Kiepe Electric Ges.m.b.H. führt ein zentrales Verzeichnis über alle Verarbeitungsvorgänge. In jeder Fachabteilung wird mindestens einer Person die Verantwortung übertragen, die dafür notwendigen Informationen zu den Verfahren der jeweiligen Abteilung zusammenzutragen und diese entsprechend den Anforderungen des Art. 30 DS-GVO zu dokumentieren. Bei Unklarheiten hinsichtlich der gesetzlich geforderten Informationen kann der Datenschutzkoordinator beratend hinzugezogen werden. Der Datenschutzkoordinator führt die in den Abteilungen erstellten Dokumentationen zu einem zentralen Verfahrensverzeichnis zusammen.

Auf Anfrage stellt das Unternehmen der Aufsichtsbehörde das Verzeichnis zur Verfügung. Im Einvernehmen mit der Unternehmensleitung ist hierfür der Datenschutzkoordinator zuständig und arbeitet mit der Aufsichtsbehörde zusammen.

2.7 Jeder Mitarbeiter kann sich unmittelbar mit Hinweisen, Anregungen oder Beschwerden an den DSK wenden, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird.

2.8 Der DSK berichtet jährlich in einem Tätigkeitsbericht der Geschäftsführung über stattgefundene Prüfungen, Beanstandungen und ggf. noch zu beseitigende Organisationsmängel. Die eigentliche Prüftätigkeit erfolgt durch die interne Revision. Der DSK unterstütz die interne Revision bei der Prüftätigkeit. Soweit der Bericht die Verarbeitung von Mitarbeiterdaten oder Fragen der betrieblichen Organisation betrifft, wird er auch dem Betriebsrat zugänglich gemacht.

3. Beschaffung/Hard- und Software

3.1 Die Beschaffung von Hard- und Software erfolgt grundsätzlich auf Anforderung der über die Verarbeitungen entscheidenden Person/Abteilung durch die zentrale DV-Beschaffung. 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. Siehe dazu auch Kapitel 11.

3.2 Falls mit der Beschaffung ein neues Verfahren der Verarbeitung personenbezogener Daten eingeführt werden soll, ist der Datenschutzkoordinator rechtzeitig vorab von der anfordernden Stelle zu informieren (siehe hierzu Näheres in Ziff. 5.2). Die Beschaffung erfolgt erst nach Stellungnahme des DSK. Der DSK berät dahingehend, ob die Durchführung einer Datenschutz-Folgenabschätzung erforderlich ist. Die Durchführung einer Datenschutz-Folgenabschätzung richtet sich nach der Vorlage zur Datenschutz-Folgenabschätzung.

3.3 Private Hard- und Software dürfen nicht zur Verarbeitung personenbezogener Daten Verwendung finden.

3.4 Die IT-Abteilung führt ein Verzeichnis der eingesetzten Hardware und der verwendeten DSGVO-relevanten Anwendungsprogramme. Der DSK auf dieses Verzeichnis jederzeit zugreifen.

3.5 Bei Verdacht des Diebstahls von Hard- und Software, des unbefugten Zugriffs auf personenbezogene Daten, von Sabotage etc. sind der DSK und IT/Organisation unverzüglich zu informieren. Der DSK stellt sicher, dass entsprechende Prozesse zur zeitgerechten Information des Betroffenen und der Aufsichtsbehörde implementiert sind. IT/Organisation ist für die Analyse von Art, Umfang und Kombinierbarkeit der ungewollt abgeflossenen Daten verantwortlich. Nach der unmittelbaren Schließung der Lücke durch IT/Organisation werden unter der Leitung des DSK technische und organisatorische Maßnahmen zur zukünftigen Verbesserung entwickelt und umgesetzt.

Näheres regelt die unternehmensintern verfügbare Prozessanweisung zur Umsetzung der Datenschutzgrundverordnung DSGVO.

4. Verpflichtung/Schulung der Mitarbeiter

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

4.2 Die Verpflichtung erfolgt unter Verwendung des im Unternehmen eingesetzten Online-Schulungstools AS-Trainer (Plegro) und wird elektronisch geführt.

4.3 Der DSK ist über die Verpflichtung von Mitarbeitern und deren Arbeitsplatz zwecks von ihm vorzunehmenden weiteren Schulungen und die Feststellung evtl. Kontrollbedarfs zu informieren.

4.4 Für in Abstimmung mit den jeweiligen Abteilungsleitungen angesetzte Schulungstermine sind die betroffenen Mitarbeiter freizustellen.

5. Transparenz der Datenverarbeitung

5.1 Über Verfahren, die den Umgang mit personenbezogenen Daten betreffen, führt der Datenschutzkoordinator ein Verzeichnis von Verarbeitungen gem. Art. 30 DS-GVO. Der für ein Verfahren Verantwortliche bzw. der zuständige Datenschutzmanager meldet dieses zeitnah gemäß den vom DSK definierten Vorgaben. Gleiches gilt für Veränderungen (Change Request).

5.2 Unabhängig von dieser Meldung ist der DSK bei der Planung der Einführung neuer Verarbeitungen bzw. der Veränderung bestehender Verfahren über Zweck und Inhalt der Anwendung und die Erfüllung der Benachrichtigungspflicht zu informieren (vgl. Ziff. 6.3). Bei standardisierten Erhebungen (Fragebögen, Preisausschreiben, Eingabefelder auf der Internet-Homepage etc.) ist der Erhebungsbogen etc. dem DSK zur Abstimmung vorzulegen.

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

5.4 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 zentrale Bearbeitung durch den DSK. Auskunfts- und Einsichtsrechte von Mitarbeitern werden durch die Personalabteilung erfüllt. Der DSK wird auch hier einbezogen. Näheres regelt die unternehmensintern verfügbare Prozessanweisung zur Umsetzung der Datenschutzgrundverordnung DSGVO.

5.5 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 DSK und die IT-Abteilung festzulegen. Näheres regelt die unternehmensintern verfügbare Prozessanweisung zur Umsetzung der Datenschutzgrundverordnung DSGVO.

5.6 Die IT/Organisation hat in Abstimmung mit dem DSK für die technische Umsetzung der Löschung personenbezogener Daten im Sinne des Art. 17 DSGVO zu sorgen. Näheres regelt die unternehmensintern verfügbare Prozessanweisung zur Umsetzung der Datenschutzgrundverordnung DSGVO.

5.7 Um die Betroffenen-Rechte einfordern zu können, ist der Betroffene (Kunde, Mitarbeiter, etc.) entsprechend darüber zu informieren, dass die Kiepe Electric Ges.m.b.H. personenbezogene Daten über ihn verarbeitet. Die Information an die Betroffenen ist präzise, leicht zugänglich und verständlich, sowie in klarer und einfacher Sprache abzufassen. Der Betroffene wird insbesondere über Namen und Kontaktdaten des Verantwortlichen für die Verarbeitung bei Kiepe Electric Ges.m.b.H., Kontaktdaten des DSK, die Rechtsgrundlage der Verarbeitung und ggf. Empfänger der Daten informiert. Um eine faire und transparente Verarbeitung zu gewährleisten informiert die Kiepe Electric Ges.m.b.H. auch über die Dauer der Datenspeicherung, die Rechte des Betroffenen (Auskunft, Löschung, etc.) die Möglichkeit zum Widerruf einer Einwilligung und die Möglichkeit zur Beschwerde bei der Aufsichtsbehörde (im Sinne des Art. 13 DSGVO).

6. Erhebung/Verarbeitung von personenbezogenen Daten

6.1. Die Erhebung und Verarbeitung personenbezogener Daten darf nur im Rahmen des rechtlich Zulässigen erfolgen. Grundsätzlich dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen.

6.2 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).

6.3 Vor Einführung neuer Arten von Erhebungen ist die die Zulässigkeit bestimmende Zweckbestimmung der Daten durch den für die Anwendung Verantwortlichen schriftlich zu dokumentieren. 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.

6.4 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 der DSK zu kontaktieren.

6.5. Es ist auf die besonderen Voraussetzungen für die Erhebung und Verarbeitung sensibler Daten gemäß Art. 9 Abs. 1 DS- GVO zu achten. Zu den sensiblen Daten gehören die folgenden Informationen einer natürlichen Person:

- Rassische und ethnische Herkunft
- Politische Meinungen
- Religiöse und weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische Daten
- Biometrische Daten
- Gesundheitsdaten
- Daten zur sexuellen Orientierung

6.6 Sofern eine Einwilligung des Betroffenen als Rechtsgrundlage für die Verarbeitung von personenbezogenen Daten erforderlich ist, hat der DSK insbesondere sicherzustellen, dass:

- Die Zustimmung in Form einer eindeutig bestätigenden Handlung erfolgt.
- Das Ersuchen um Zustimmung in einfacher und klarer Sprache erfolgt.
- Eine klare Unterscheidung der Zustimmungserklärung von sonstigen Bestimmungen erfolgt (Hervorhebung).
- Der Betroffene über seine Rechte informiert wird (insbesondere auch Widerruf).

7. Datenhaltung/Versand/Löschung

7.1 Die Speicherung von Daten erfolgt grundsätzlich auf den hierzu zur Verfügung gestellten Netzlaufwerken. Eine Speicherung auf mobilen Datenträgern oder Cloudspeicher (z.B. Flashspeicher, Streamer-Bändern) bedarf der Genehmigung durch die IT-Abteilung und der Registrierung durch die den Träger einsetzende Abteilung/Benutzer. Bei Netzwerken ist die IT-Abteilung für die Sicherung der Daten verantwortlich, die auf dem Server gespeichert sind.

7.2 Soweit technisch bedingt ein anderer Speicherort erforderlich ist (z.B. Notebook, Desktop-PC) ist der jeweilige Benutzer für die Durchführung der Datensicherung selbst verantwortlich. Ist ein Netzzugang möglich (z.B. bei Notebook mit WLAN, Tablet), ist zumindest einmal wöchentlich der aktuelle Datenbestand auf das für den Benutzer reservierte Netzlaufwerk zu überspielen. Die gewählten Datensicherungsmaßnahmen sind in dem Verfahrensverzeichnis zu dokumentieren.

7.3 Gesetzliche Aufbewahrungsfristen und Löschungstermine sind von dem über die Verarbeitung der Daten Entscheidenden in seiner Verantwortung zu beachten. Der Datenschutzkoordinator ist über die Einhaltung der Termine insbesondere im Hinblick auf die Löschung personenbezogener Daten zu informieren und das unternehmensinterne „Aufbewahrungsverzeichnis" in entsprechender Form zu korrigieren.

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

8. Externe Dienstleister/Auftragsverarbeitung/Wartung

8.1 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 die Rechtsabteilung vor der Beauftragung unter Vorlage des den Anforderungen des Art. 28 DS-GVO genügenden Vertragsentwurfs und der Kriterien der erfolgten bzw. nachfolgend vorgesehenen Auftragskontrolle zu informieren.

8.2 Entsprechendes gilt, falls die Kiepe Electric Ges.m.b.H. entsprechende Tätigkeiten im Auftrag Dritter wahrnehmen will.

9. Sicherheit der Verarbeitung

9.1 Für jedes Verfahren ist eine Analyse bzgl. der für den Betroffenen möglichen Risiken zu erstellen. Diese richten sich an der Art, dem Umfang, der Umstände und Zwecke der Verarbeitung sowie der Wahrscheinlichkeit des Eintritts einer solchen Gefahr.

9.2 Neben dieser Richtlinie bestehen ergänzende Regelungen, die insbesondere zur Realisierung der Datensicherungsgebote des Art. 32 DS-GVO zu treffende Maßnahmen betreffen. Hierzu gehören u.a.:

- IT Sicherheitsrichtlinie

Ferner ist die Verarbeitung von Personaldaten in einer Anzahl von Betriebsvereinbarungen näher festgelegt. Hierzu gehören u. a. die Vereinbarung

- über die Nutzung von Telekommunikation (Telefon, E-Mail, Internet) in der Kiepe Electric Ges.m.b.H. GmbH

10. Rechenschafts- und Dokumentationspflicht

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

11. Privacy by Design und by Default

Die Kiepe Electric Ges.m.b.H. orientiert sich bei der Umsetzung des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO) an den Vorgaben der Europäischen Agentur für Netz- und Informationssicherheit (ENISA). Die Kiepe Electric Ges.m.b.H. verfolgt demgemäß folgende acht Privacy-Design-Strategien:

- *Minimise*: Die Menge der verarbeiteten Daten wird so gering wie möglich gehalten.
- *Separate*: Personenbezogene Daten werden möglichst verteilt verarbeitet und getrennt gespeichert.
- *Aggregate*: Personenbezogene Daten werden im höchsten Aggregationsniveau und mit dem niedrigsten Detailgrad verarbeitet, in dem sie noch ihren Zweck erfüllen.
- *Inform*: Betroffene werden angemessen informiert, wann immer ihre personenbezogenen Daten verarbeitet werden.
- *Control*: Betroffene erhalten Kontrolle über die Verarbeitung Ihrer personenbezogenen Daten.
- *Enforce*: Mit den rechtlichen Anforderungen in Einklang stehende Datenschutzregeln werden definiert und durchgesetzt.
- *Demonstrate*: Der Verantwortliche ist in der Lage, die Einhaltung der Datenschutzregeln und aller gesetzlichen Bestimmungen nachzuweisen.
- Bezüglich der technischen Umsetzung dieser Strategischen Ziele orientiert sich die Kiepe Electric Ges.m.b.H. an den Maßnahmen, die ENISA im Report „Privacy and Data Protection by Design – from policy to engineering" in Kapitel 4 beschrieben hat[1].

Geschäftsführer DI Peter Pichler