Allgemeine Datenschutzrichtlinie

Walter Binde GmbH & Co. KG, Königstrasse 134b, 32427 Minden in NRW/Deutschland (im Weiteren „die Firma“ genannt)

Verantwortlich vertreten durch Jörn Binde und Walter Koenemann (im Weiteren als „Verantwortliche/r“ bezeichnet).

Die Firma Walter Binde GmbH & Co. KG verpflichtet sich im Rahmen ihrer gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten insbesondere nach der EU Datenschutzgrundverordnung. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und die Reputation der Firma als Arbeitgeber. Diese Datenschutzrichtlinie gewährleistet, dass das von europäischen und nationalen Gesetzen verlangte angemessene Datenschutzniveau besteht.

Die jeweils aktuellste Version der Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite der Walter Binde GmbH & Co. KG heruntergeladen werden.

Unsere Führungskräfte und Mitarbeiter sind verpflichtet, diese Datenschutzrichtlinie einzuhalten und die jeweiligen Datenschutzgesetze zu wahren.

Als externer Datenschutzbeauftragter wurde bestellt:

Frank Sewing, Bornestrasse 3, 32361 Preußisch Oldendorf, Kontaktadresse: dsb@icopa.de

Unsere Prinzipien für die Verarbeitung personenbezogener Daten:

1

Rechtmäßigkeit

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

2

Zweckbindung

Die Verarbeitung personenbezogener Daten darf lediglich die Zwecke verfolgen, die vor der Erhebung der Daten festgelegt wurden.

3

Transparenz

Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei Erhebung der Daten muss der Betroffene mindestens folgendes erkennen können oder entsprechend darüber informiert werden:

- Die Identität der verantwortlichen Stelle
- Den Zweck der Datenverarbeitung
- Dritte oder Kategorien von Dritten, an die die Daten gegebenenfalls übermittelt werden

4

Datensparsamkeit

Vor einer Verarbeitung personenbezogener Daten muss geprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Wenn es zur Erreichung des Zwecks möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Zweck steht, sind anonymisierte Daten zu verwenden. Personenbezogene Daten dürfen nicht auf Vorrat für potentiell zukünftige andersartige Zwecke gespeichert werden, es sei denn dies ist durch staatliches Recht vorgeschrieben oder erlaubt.

5

Löschung

Personenbezogene Daten, die nach Ablauf von gesetzlichen der geschäftsprozessbezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen, müssen die Daten weiter gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt wurde.

6

Richtigkeit der Daten

Personenbezogene Daten sind richtig, vollständig und – soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nichtzutreffende, unvollständige oder veraltete Daten gelöscht, berichtigt ergänzt oder aktualisiert werden.

7

Vertraulichkeit

Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

8

Zulässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

- Datenverarbeitung für eine vertragliche Beziehung

Personenbezogene Daten des betroffenen Interessenten, Kunden oder Partners dürfen zur Begründung, zur Durchführung und zur Beendigung eines Vertrages verarbeitet werden. Dies umfasst auch die Betreuung des Vertragspartners, sofern dies im Zusammenhang mit dem Vertragszweck steht.

- Datenverarbeitung zu Werbezwecken

Die Verarbeitung personenbezogener Daten zu Zwecken der Werbung oder Marktforschung ist zulässig soweit der Betroffene in die Verarbeitung seiner Daten aktiv und nachweislich einwilligt. Der Betroffene ist über die Verwendung seiner Daten für Zwecke der Werbung oder Marktforschung 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.

Widerspricht der Betroffene der Verwendung seiner Daten zu Zwecken der Werbung oder Marktforschung, so ist eine weitere Verwendung seiner Daten für die Zwecke unzulässig und sie 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 gemäß Punkt 3 dieser Datenschutzrichtlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen.

- Datenverarbeitung aufgrund gesetzlicher Erlaubnis

Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach dessen Rechtsvorschriften.

- Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über die rassische und ethnische Herkunft, über politische Meinungen, über religiöse oder philosophische Überzeugungen, über

Gewerkschaftszugehörigkeiten oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Der Betroffene kann ferner freiwillig in eine Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren um eine Datenschutzfolgeabschätzung vorzunehmen.

- Telekommunikation und Internet

Telefonanlagen, Telekommunikationsgeräte, E-Mal-Adressen, Intranet und Internet werden in erster Linie im Rahmen betrieblicher Aufgabenstellungen durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der betrieblichen Aufgabenerfüllung aufgrund jeweils geltender Rechtsvorschriften und unternehmensinterner Richtlinien genutzt werden. Im Fall der erlaubten Nutzung zu privaten Zwecken sind das Fernmeldegeheimnis und das geltende Telekommunikationsrecht zu beachten.

Eine generelle Überwachung der Telefon- und E-Mail-Kommunikation bzw. der Intranet- und Internetnutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur oder auf einzelne Nutzer oder aus anderen Gründen der Sicherheit kann die Nutzung der Telefonanlagen, der E-Mail-Adressen, des Intranets und Internets zeitlich befristet protokolliert werden. Personenbezogene Auswertungen dieser Daten dürfen nur bei einem konkreten begründeten Verdacht eines Verstoßes gegen Gesetze erfolgen.

9

Datenübermittlung

Eine Übermittlung von personenbezogenen Daten an Empfänger außerhalb der Firma unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Punkt 8. Im Falle einer Übermittlung von Daten an einen Dritten muss dieser ein zu dieser Datenschutzrichtlinie gleichwertiges Datenschutzniveau gewährleisten. Dies gilt nicht, wenn die Übermittlung aufgrund einer gesetzlichen Verpflichtung erfolgt. Im Falle einer Datenübermittlung von Dritten an die Firma muss sichergestellt sein, dass die Daten nur für die vorgesehenen Zwecke verwendet werden dürfen.

10

Auftragsdatenverarbeitung

Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird. In diesen Fällen ist mit den externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die volle Verantwortung für die korrekte Durchführung der Datenverarbeitung. Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrages sind die nachfolgenden Vorgaben einzuhalten.

- Der Auftraggeber ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen.

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

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

11

Betroffenenrechte

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den Verantwortlichen zu bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen

- Der Betroffene kann Auskunft darüber verlangen, welche personenbezogenen Daten welcher Herkunft über ihn zu welchem Zweck gespeichert sind.
- Werden personenbezogene Daten an Dritte übermittelt, muss auch über die Identität des Empfängers oder über die Kategorie von Empfängern Auskunft gegeben werden.
- Sollten personenbezogene Daten unrichtig oder unvollständig sein, kann der Betroffene ihre Berichtigung oder Ergänzung verlangen.
- Der Betroffene kann der Verarbeitung seiner personenbezogenen Daten zu Zwecken der Werbung oder der Marktforschung widersprechen. Für diese Zwecke müssen die Daten dann gesperrt werden.
- Der Betroffene ist berechtigt, die Löschung seiner Daten zu verlangen, wenn die Rechtsgrundlage für die Verarbeitung der Daten fehlt oder entfallen ist. Gleiches gilt für den Fall, dass der ursprüngliche Zweck der Datenverarbeitung durch Zeitablauf oder aus anderen Gründen entfallen ist. Bestehende Aufbewahrungspflichten und einer Löschung entgegenstehende schutzwürdige Interessen müssen beachtet werden.
- Der Betroffene hat ein grundsätzliches Widerspruchsrecht gegen die Verarbeitung seiner Daten, das zu berücksichtigen ist, wenn sein schutzwürdiges Interesse aufgrund einer besonderen persönlichen Situation das Interesse der Verarbeitung überwiegt. Dies gilt nicht, wenn eine Rechtsvorschrift zur Durchführung der Verarbeitung verpflichtet.

12

Vertraulichkeit

Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung, Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut und entsprechend berechtigt zu sein. Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweiligen Aufgaben erforderlich ist. Dies wird durch eine Aufteilung von Rollen und Zuständigkeiten sowie deren Umsetzung und Pflege im Rahmen eines Berechtigungskonzeptes

umgesetzt. Mitarbeiter dürfen personenbezogene Daten nicht für eigene private oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diesen auf andere Weise zugänglich machen. Die Mitarbeiter werden bei Beginn des Beschäftigungsverhältnisses zur Wahrung des Datengeheimnisses verpflichtet. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

13

Sicherheit der Verarbeitung

Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe sowie gegen Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT-Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf der Daten zu orientieren. Diese Maßnahmen werden kontinuierlich an die technischen Entwicklungen und an organisatorische Änderungen angepasst.

14

Kontrolle

Die Einhaltung der Richtlinie zum Datenschutz und der geltenden Datenschutzgesetze wird regelmäßig durch Kontrollen und Datenschutzaudits überprüft. Die Durchführung obliegt dem bestellten Datenschutzbeauftragten. Empfehlungen zur Verbesserung des Datenschutzniveaus werden im Rahmen der Angemessenheit zeitnah von der Geschäftsleitung umgesetzt.

15

Datenschutzvorfälle

Fälle von Verstößen gegen die EU-Datenschutzgrundverordnung, sogenannte Datenschutzvorfälle, wie unrechtmäßiger Übermittlung personenbezogener Daten an Dritte, unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten oder der Verlust personenbezogener Daten sind der zuständigen Aufsichtsbehörde unter Einbeziehung des bestellten Datenschutzbeauftragten binnen 72 Stunden durch den Verantwortlichen zu melden. Ebenso sind die Betroffenen hiervon in einem angemessenen Zeitrahmen zu informieren.

16

Datenschutzbeauftragter

Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den bestellten Datenschutzbeauftragten der Firma wenden. Diese Anfragen sowie Beschwerden werden auf Wunsch vertraulich behandelt.

Anlage

Technische und Organisatorische Maßnahmen der Firma zum Schutz personenbezogener Daten

gemäß (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO) Erstelldatum: 23/05/2018

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen) statt. Dies umfasst die folgenden Maßnahmen:

- Schlüssel / Schlüsselvergabe
- Gebäudesicherung (Zäune, Pforten)
- Alarmsicherung
- Schließsystem

Es findet eine Zugangskontrolle (keine unbefugte Systembenutzung) statt. Dies umfasst die folgenden Maßnahmen:

- Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
- Automatische Sperrung (z.B. Pausenschaltung)
- Verschlüsselung von Datenträgern und Datensätzen
- Software Firewall
- Hardware Firewall
- Anti-Viren Software

Es findet eine Trennungskontrolle / Verwendungszweckkontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden) statt. Dies umfasst die folgenden Maßnahmen:

- Jeweilige Zweckbindungskontrolle
- Daten werden nicht für andere Zwecke weiterverwendet

Es findet keine Pseudonymisierung von Datensätzen statt.

- Eine Pseudonymisierung findet nicht statt, da diese Maßnahme unzweckmäßig wäre und die Bearbeitungsabläufe erheblich erschweren würde. Außerdem ist eine Pseudonymisierung in der eingesetzten Software von SAGE nicht vorgesehen. Dies kann vom Verantwortlichen nicht beeinflusst werden

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport) statt. Dies umfasst die folgenden Maßnahmen:

- Verschlüsselung / Tunnelverbindung zu IT Dienstleistern
- Prüfung der Rechtmäßigkeit der Weitergabe von Daten

Es findet eine Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind) statt. Dies umfasst die folgenden Maßnahmen:

- Protokollierungs- und Protokollauswertungssysteme
- Sicherung von Protokolldaten gegen Verlust oder Veränderung

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Es findet eine Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust) statt. Dies umfasst die folgenden Maßnahmen:

- Backup-Strategie (offline)
- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsschutz
- Schutz vor Diebstahl
- Virenschutz / Firewall

Es ist eine rasche Wiederherstellbarkeit gegeben. Dies wird durch folgenden Maßnahmen gewährleistet:

- regelmäßiges testen der Wiederherstellungssysteme
- durchspielen von Wiederherstellungsszenarien

Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DS-GVO)

Folgende Maßnahmen wurden getroffen:

- Löschen von Datensätzen unter Beachtung der gesetzlichen Aufbewahrungsfristen
- Mehrfaches Überschreiben von aussortieren Datenträgern
- Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern
- Sorgfältige Auswahl von Entsorgungsdienstleistern

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Die technischen und organisatorischen Maßnahmen wurden zuletzt an folgendem Datum evaluiert:
23.05.2018

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind im Einsatz. Dies wird durch folgende Maßnahmen unterstützt:

- Datenschutz-Management
- Regelmäßige Datenschutzschulungen
- Auftragskontrolle für Auftragsverarbeiter (AV)
- Nachkontrollen

Es liegen folgende Anweisungen, Regeln oder Analysen schriftlich vor:

- Interne Verhaltensregeln(Passwortregeln, Verhaltensregeln am PC und am Telefon) (Anlage 1)
- Auftragskontrolle für Auftragsverarbeiter (AV)
- Wiederanlaufkonzept / Wiederherstellungskonzept

Jörn Binde
Digital unterschrieben von Jörn Binde
Datum: 2018.07.05 07:33:03 +02'00'