B4 KATALOG DER TECHNISCHEN UND ORGANISATORISCHEN MAßNAHMEN

Version: 2.0

b4value.net GmbH | www.b4value.net

Public

Inhalt

Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherstellung des Schutzes personenbezogener Daten nach §32 EU Datenschutz Grundverordnung.

Verantwortlicher:

b4value.net GmbH
Trippstadter Straße 122
D-67663 Kaiserslautern
HRB 4024 AG Kaiserslautern
St.Nr.19 673 0799 1
UstID DE 813949895
im Folgenden als „b4“ bezeichnet.

Die Beschreibung der Maßnahmen bezieht sich auch auf Einrichtungen an der Betriebsstätte:
Dieselstraße 1
67269 Grünstadt
sowie das dem Firmennetzwerk integrierte Rechenzentrum in Frankfurt

Verantwortliche verfügungsberechtigte Vertreter (Haftende/r) von b4:
Hr. Harald Ross
Hr. Dieter Keller

zum Beauftragten für den Datenschutz ist benannt:
Bernd Alf Sittel (datenschutz@b4value.net)
Dieselstraße 1
67269 Grünstadt
Tel.: +49 6359 87292-55

1. Technische und organisatorische Maßnahmen

Gemäß Arti. 32 DS-GVO, werden durch b4 die technischen und organisatorischen Maßnahmen zur Sicherstellung und Einhaltung des Datenschutzes im Sinne des Gesetzes festgelegt.

2. Innerbetriebliche Organisation

b4 gestaltet seine innerbetriebliche Organisation derart, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei werden insbesondere Maßnahmen bereitgestellt, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind, ein adäquates Datenschutzniveau zu erreichen.

3. Notwendige, einzuhaltende Kontrollmechanismen:

Die von b4 getroffenen Maßnahmen wurden im Hinblick auf die Sicherstellung der in den anzuwendenden gesetzlichen Vorschriften verankerten Kontrollebenen konzipiert.

Diese sind:

Gemäß Art. 32 DS-GVO „Sicherheit der Verarbeitung“:

1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
    a. die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
    b. die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
    c. die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
    d. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von, beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.
3) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.
4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Technische und organisatorische Maßnahmen die der Pseudonymisierung oder Verschlüsselung gem. Art. 32, Satz 1 lit. a DSGVO dienen:

Im Umfeld der Geschäftstätigkeit der b4value.net GmbH existiert kein Vorgang, der eine Pseudonymisierung verlangt oder notwendig erscheinen lässt.

Alle Festplatten, aller Systeme verfügen über eine Hardwareverschlüsselung.
Jeder Zugriff auf b4-Systeme erfolgt ausschließlich über transportverschlüsselte Kanäle und Mechanismen. Alle Datentransfers gegenüber allen Systemen, die verschlüsselten Transfer unterstützen, erfolgen verschlüsselt.

Technische und organisatorische Maßnahmen die der Vertraulichkeit, Verfügbarkeit, Belastbarkeit und Integrität, gem. Art. 32, Satz 1 Lit. b DSGVO, dienen:

Datenträger unterliegen einem dokumentierten Kommissionierungs- und Dekommissionierungsprozess. Es werden ausschließlich zertifizierte Dienstleister zur Datenträgervernichtung eingesetzt.
Alle Dienstleister unterliegen einem strengen Auswahlverfahren. Bei Vertragsschluss ist eine der beauftragten Leistung entsprechende Datenschutzvereinbarung obligatorisch.

Alle b4-Mitarbeiter sind zur Verschwiegenheit verpflichtet. Die Rechtsgrundlagen der Verschwiegenheitsverpflichtung unterliegen einem dokumentierten, regelmäßigen Sensibilisierungsprozess.
Alle b4-Mitarbeiter werden permanent zu Datenschutz und Informationssicherheit geschult und sensibilisiert. Zum Umgang mit Daten und Datenverarbeitungsanlagen findet ein regelmäßiges, dokumentiertes Schulungs- und Sensibilisierungsprogramm Anwendung.

Alle Mitarbeiter unterliegen einem dokumentierten Prozess der regelmäßigen Sicherheitsüberprüfung

Zutritt zu den b4- Räumlichkeiten unterliegt einem dokumentierten Zugangskontrollprozess. Alle Besuche betriebsfremder Personen werden dokumentiert.

Alle Netzwerkinfrastrukturkomponenten unterliegen einem dokumentierten Aktualisierungsprozess sowie einem dokumentierten Inventarisierungsverfahren.

Es ist eine umfangreiche Firewall-Appliance in Betrieb, die alle Zugriffe von außen auf die Netzwerkinfrastruktur absichert.

Es existieren getrennte WLAN-Strukturen für Gäste und interne b4-Ressourcen (Mitarbeiter und Devices)

Die logische Trennung von Datenbeständen unterschiedlicher Zwecke oder Umgebungen ist durchgängig sichergestellt.

Nicht benötigte oder Verbindungen im Leerlauf werden stets automatisch getrennt.

Zur Verarbeitung personenbezogener Daten sind prozessbezogene Verfahren etabliert. Datenzugriffsberechtigungen in allen Systemen folgen den Grundsätzen der „Datensparsamkeit“ und Zweckmäßigkeit, entsprechend den Aufgaben der jeweiligen Personen und Personengruppen. Diese werden durch ein umfangreiches Rollen- und Rechtekonzept realisiert.

Unterbeauftragte Lieferanten werden mittels einer auf die Verarbeitung zugeschnittene Datenschutzvereinbarung (Auftragsverarbeitung oder gemeinsame Verantwortlichkeit) auf ein angemessenes Datenschutzniveau verpflichtet.

Alle Zugriffe auf öffentlich erreichbare Systeme erfolgen ausschließlich mittels verschlüsselten Transfers.

Alle Computersysteme sind mit einem mehrstufigen Virenschutzsystem versehen.

Alle im Unternehmensumfeld verwendeten Browser werden gemäß der jeweiligen Herstellervorgaben gehärtet.

Alle Datenbestände unterliegen einem mehrstufigen Backup und Restore Verfahren, das regelmäßig auf Zuverlässigkeit geprüft wird.

Änderung und Aktualisierung von Systemen oder Diensten werden gemäß definierten Prozessen durchgeführt und dokumentiert.

Technische und organisatorische Maßnahmen die der Wiederherstellbarkeit, gem. Art. 32, Satz 1 Lit. c DSGVO dienen:

Alle Datenbestände unterliegen einem mehrstufigen Backup und Restore Verfahren, das regelmäßig auf Zuverlässigkeit geprüft wird.

Verfahren, die der regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32, Satz 1 Lit. d DSGVO dienen:

Alle technischen und organisatorischen Maßnahmen unterliegen einer regelmäßigen Überprüfung auf Einhaltung und Wirksamkeit durch dafür qualifizierte Mitarbeiter des Verantwortlichen und im notwendigen Einzelfall durch externe Prüfende.

Die Prüfergebnisse werden dokumentiert.

Dieses Dokument wurde elektronisch erstellt und ist ohne Unterschrift gültig.