EBG-Data

EBG-DATA GMBH • BUSSARDWEG 18 • 41468 NEUSS • TEL: +49 2131 347-200 • FAX: +49 2131 347-199
WWW.EBG-DATA.DE • E-MAIL: INFO@EBG-DATA.DE

Technische und organisatorische Maßnahmen nach Art. 32 der DSGVO

Art. 32 der DSGVO verpflichtet Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Hier werden die technischen und organisatorischen Maßnahmen der EBG-Data GmbH beschrieben, die sie in ihrer Eigenschaft als Auftragsverarbeiter trifft. EBG-Data GmbH nutzt für die Auftragsverarbeitung Subunternehmen. Deren technische und organisatorische Maßnahmen werden zur Transparenz ebenfalls veröffentlicht und sind unter der gleichen URL abrufbar. Teile der technischen und organisatorischen Maßnahmen der Subunternehmer sind in diese Dokumentation eingeflossen.

Diese Dokumentation wird fortlaufend ergänzt und angepasst. Sie ist unter gleicher URL in der jeweils aktuellen Fassung abrufbar.

1. Zutrittskontrolle
   Die Zugangskontrolle soll verhindern, dass Unbefugte Zugang zu Verarbeitungsanlagen erhalten, mit denen die Verarbeitung durchgeführt wird.

technische Maßnahme	organisatorische Maßnahme
Transponder-Schließsystem für Bürokomplex	Besucher bewegen sich in den Räumlichkeiten ausschließlich mit zugewiesenen Mitarbeitern.
Sicherheitsschlösser	Schlüsselbuch
	Rückgabe Transponder/Schlüssel bei Ausscheiden eines Mitarbeiters.

2. Zugangskontrolle
   Mit der Zugangskontrolle soll ein Eindringen unberechtigter Personen in die Informationsverarbeitenden Systeme verhindert werden. Hierzu sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung implementiert.

technische Maßnahme	organisatorische Maßnahme
Authentifizierungsverfahren	Passwortrichtlinie/Passwortregeln inkl. Passwortlänge, erzwungener Passwortwechsel nach festgelegtem Zeitintervall.
Einsatz von Firewalls	Ticketsystem protokolliert das Erteilen und Löschen von Benutzerberechtigungen.
Einsatz von Mobile Device Management	Sperren von Berechtigungen sobald der Benutzer das Unternehmen verlässt.
Einsatz von VPN-Technologie	Bildschirmsperre aufheben nur mit Benutzer und Passwort
	Zugangsberechtigungen nur dafür, wo dies auf Grund der Funktion und Aufgabenerfüllung benötigt wird.

3. Zugriffskontrolle
   Die Zugriffskontrolle soll gewährleisten, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberichtigung umfassten personenbezogenen Daten Zugang haben.

DZ BANK AG FRANKFURT • IBAN: DE06 5006 0400 0000 1394 15 • BIC: GENODEFFXXX
GESCHÄFTSFÜHRER: CHRISTIAN BRAUN, KAI SCHMIDT
UST-IDNR.: DE812791298 • ST.-NR.: 122/5719/5021 • AMTSGERICHT NEUSS: HRB 15 857

technische Maßnahme	organisatorische Maßnahme
	Benutzerberechtigungen verwaltet durch Systemadministrator
	Differenzierte Berechtigung für Daten, Anwendungen und Betriebssystem
	Veränderungen der Berechtigungen nur durch Systemadministratoren möglich.
	Zeitnahes Löschen von Berechtigungen wenn z.B. ein Mitarbeiter das Unternehmen verlässt.
	Anzahl der Administratoren auf das „Notwendigste“ reduziert
	Ticketsystem protokolliert das Erteilen und Löschen von Benutzerberechtigungen.

4. Weitergabekontrolle
   Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung, sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

technische Maßnahme	Organisatorische Maßnahmen
Verschlüsselung der Übertragungsdateien	Systeme (z.B. Kasse und Warenwirtschaft) übertragen auf fest definierte Ziele
	Alle Mitarbeiter sind auf das Datengeheimnis gem. § 5 BDSG verpflichtet.
	Datenträger mit personenbezogenen Daten werden ausschließlich an Auftraggeber gesendet. Die Dateien werden mit gängigen Verfahren durch Passwort geschützt.

5. Eingabekontrolle
   Die Veränderung personenbezogener Daten erfolgt ausschließlich im Rahmen einer Auftrags-/Vertragserfüllung. Nur hierfür angewiesene Mitarbeiter sind berechtigt die Daten zu Verarbeiten. Die Durchführung der Verarbeitung wird in einem Ticketsystem protokolliert.

6. Auftragskontrolle
   Die Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten liegen in der Regel in Schriftform vor. Die Verarbeitung von personenbezogenen Daten in Zweck, Art und Umfang richten sich nach den Weisungen des Auftraggebers. Die durchgeführten Tätigkeiten werden in einem Ticketsystem protokolliert.

7. Verfügbarkeitskontrolle
   Die Verfügbarkeitskontrolle soll gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind.

technische Maßnahme	organisatorische Maßnahme
Feuerlöschgeräte in Serverräumen	Erstellen eines Backup- &Recoverykonzepts
Feuer und Rauchmeldeanlagen	Erstellen eines Notfallplans-
Klimaanlagen in Serverräumen	Testen von Datenwiederherstellung
Schutzsteckdosen in Serverräumen	Aufbewahrung von Datensicherungen an einem anderen Ort.
Unterbrechungsfreie Stromversorgung (USV)	

8. Trennungskontrolle
   Die Speicherkontrolle soll verhindern, dass Unbefugte von gespeicherten personenbezogenen Daten Kenntnis nehmen sowie diese eingeben, verändern und löschen können.

technische Maßnahme	organisatorische Maßnahme
	Trennung von Produktiv-, Test- und Entwicklungssystemen
	Differenzierte Berechtigung für Produktiv-, Test- und Entwicklungssystemen
	Festlegung von Datenbankrechten
	Logische Mandantentrennung (softwareseitig)

9. Maßnahmen zur Verschlüsselung personenbezogener Daten
   .

technische Maßnahme	organisatorische Maßnahme
Verschlüsselte Speicherung der Kundendaten innerhalb der Datenbank.	
Datenaustausch zwischen Warenwirtschaft und erfolgt verschlüsselt.	

Stand: 17.12.2024
Version: 1.3