

Technische und organisatorische Maßnahmen

Mit diesem Dokument informieren wir Sie über die getroffenen Maßnahmen, welche im Zusammenhang mit Verarbeitungen von personenbezogenen Daten getätigt werden.

„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“ (Art. 32 (1) DSGVO).

Verantwortlicher:	Market Port GmbH
Anschrift:	Splietterstrasse 27, 48231 Warendorf
Datenschutzbeauftragter:	Nils Möllers, Keyed GmbH, Siemensstraße 12, 48341 Altenberge
IT-Verantwortlicher:	Tim Schlautmann
Datum:	10.08.2024

Grundlegende Angaben

- ☒ Es liegt eine wirksame Bestellung eines Datenschutzbeauftragten vor.
 - ☒ Die Beschäftigten sind auf die Vertraulichkeit (Art. 32 Abs. 1 lit. b) DSGVO) verpflichtet.
 - ☒ Beschäftigte werden regelmäßig zum Schutz personenbezogener Daten unterwiesen.
 - ☒ Es besteht ein aktuelles Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO).
-

Technische und organisatorische Maßnahmen

1. Maßnahmen zur Gewährleistung der Vertraulichkeit

<i>1.1 Zutrittskontrolle (Räumlicher Zutrittsschutz)</i>
☒ Manuelles Schießsystem (Sicherheitsschlüssel an den Außentüren und wichtigen Innentüren).
☒ Absicherung von Gebäudeschächten.
☒ Bestehen eines Zutrittsberechtigungskonzeptes.

☒ Es besteht eine Schlüsselregelung / ein Schlüsselkonzept.
☒ Personenkontrolle beim Empfang.
☒ Begleitung von Besucherzutritten durch eigene Mitarbeiter oder Sicherheitspersonal.
☒ Sorgfältige Auswahl von Reinigungspersonal.
☒ Gesondert gesicherter Zutritt zu Server-Umgebungen oder dem Rechenzentrum (siehe dazu die TOMs von der dogardo GmbH - https://marketport.de/dsgvo/ und der IONOS SE - https://www.ionos.de/terms-gtc/avv/).
<i>1.2 Zugangskontrolle (Ein unbefugter Zugang und die Nutzung Unbefugter von IT-Systemen ist zu verhindern.)</i>
☒ Einsatz geeigneter Verschlüsselung der Netzwerke.
☒ Passwortsicherung von Bildschirmarbeitsplätzen.
☒ Verwendung von individuellen Passwörtern bzw. Verhinderung von Gruppen-Passwörtern.
☒ Automatische passwortgesicherte Sperrung des Bildschirms nach Inaktivität (Bildschirmschoner).
☒ Automatische Sperrung von Nutzeraccounts nach mehrfacher Fehleingabe von Passwörtern.
☒ Einsatz eines Passwortservers samt Benutzerrollen und Protokollierung.
☒ Prozess zur Rechtevergabe bei Neueintritt von Mitarbeitern.
☒ Prozess zum Rechteentzug bei Abteilungswechseln von Mitarbeitern.
☒ Einsatz von VPN-Technologie wenn es das Projekt erfordert.
☒ Prozess zum Rechteentzug bei Austritt von Mitarbeitern.
☒ Einsatz von Anti-Viren-Software.
☒ Einsatz einer Hardware-Firewall.
☒ Einsatz einer Software-Firewall.
<i>1.3 Zugriffskontrolle (Unerlaubte Tätigkeiten in IT-Systemen außerhalb eingeräumter Berechtigungen sind zu verhindern.) Hier liegen Protokolle über die ISO9001 vor.</i>
☒ Festlegung der Zugriffsberechtigung / Einsatz eines Berechtigungskonzeptes mit

einem Passwortserver.
☒ Festlegung der Befugnis zur Dateneingabe, -änderung, -löschung.
☒ Regelmäßige Überprüfung von Berechtigungen.
☒ Protokollierung von Dateizugriffen.
☒ Protokollierung von Dateilöschungen.
☒ Protokollierung von Dateiveränderungen.
☒ Einsatz einer Anti-Viren-Schutz Lösung auf jedem Endgeät.
☒ Einsatz einer Firewall inkl. Spam-Schutz.
☒ Einsatzmöglichkeit zur Verschlüsselung auftragsbezogener / einzelner Dateien.
☒ Verschlüsselung von Datenträgern.
☒ Einsatz von Aktenvernichtern nach DSGVO.
☒ Ordnungsgemäße Vernichtung von Datenträgern.
☒ Vier-Augenprinzip bei Spezialanwendungen.
<i>1.4 Auftragskontrolle (Es ist sicherzustellen, dass Dienstleister, welche im Auftrag Daten verarbeiten, nur gemäß der Weisung des Auftraggebers Daten verarbeiten.)</i>
☒ Vertragsgestaltung der Auftragsverarbeitung gem. gesetzlichen Vorgaben (Art. 28 DSGVO).
☒ Zentrale Erfassung vorhandener Dienstleister und Auftragsverarbeiter.
☒ Es werden Kontrollen der technischen und organisatorischen Maßnahmen vor Verarbeitungsbeginn durchgeführt.
☒ Bei größeren Vorhaben sind wir bemüht, dass zwischen uns und dem Auftraggeber ein Termin mit unserem und dem Datenschutzler des Auftraggebers erfolgt um mögliche Risiken im Vorfeld zu lösen.
<i>1.5 Trennungskontrolle (Es ist sicherzustellen, dass Daten, die zu unterschiedlichen Zwecken, Personen und Unternehmen erhoben wurden, getrennt voneinander verarbeitet werden können.)</i>
☒ Trennung von Kunden (Mandantenfähigkeit der verwendeten Systeme).
☒ Logische Datentrennung (z.B. auf Basis von Kunden- oder Mandantennummern) in Datenbanken.

☒ Berechtigungskonzept, das der getrennten Verarbeitung der Auftraggeberdaten von Daten anderer Kunden Rechnung trägt.
☒ Trennung von Entwicklungs-, Test- und Produktivsystemen.
☒ Sandboxing.
☒ Protokollierung und Beweissicherung bei relevanten Systemen/Webseiten.
☒ Festlegung von Datenbankrechten.
☒ Versehen der Datensätze mit Datenfeldern/Zweckattributen.

2. Maßnahmen zur Gewährleistung der Integrität

<i>2.1 Weitergabekontrolle (Aspekte der Weitergabe (Übermittlung) personenbezogener Daten sind zu regeln: elektronische Übertragung, Datentransport, sowie deren Kontrolle.)</i>
☒ Es besteht eine sichere Versendungsart der Daten zwischen Auftraggeber, Auftragnehmer und Dritten (teilweise auch vom Auftraggeber bereit gestellt).
☒ Für den E-Mail Versand sind verschlüsselte ZIP-Dateien möglich.
☒ Einsatz von VPN-Verbindungen vorhanden und möglich.
☒ Upload und Download nur über einen SFTP-Server.
☒ Es findet ein Datenaustausch über eine SSL (https)-Verschlüsselung statt.
☒ Sicherstellung der Datenträgerentsorgung / Sichere Löschung von Datenträgern.
☒ Einsatz von Aktenvernichtern (Shredder gem. DIN 66399).
☒ Dokumentation der Stellen, an die eine Übermittlung vorgesehen ist, sowie der Übermittlungswege.
<i>2.2 Eingabekontrolle (Die Nachvollziehbarkeit bzw. Dokumentation der Datenverwaltung und -pflege ist zu gewährleisten.)</i>
☒ Kennzeichnung erfasster Daten.
☒ Protokollierung von Eingaben/Löschungen.
☒ Dokumentenmanagement nach ISO9001.
☒ Regelung zu Aufbewahrungsfristen für Revision/Nachweiszwecke nach ISO9001.

3. Maßnahmen zur Gewährleistung der Verfügbarkeit

3.1 Verfügbarkeitskontrolle (Die Daten sind gegen zufällige Zerstörung oder Verlust zu schützen.)

*Die Server sind ausgelagert bei der dogardo GmbH, alles weitere finden Sie hier:
<https://marketport.de/dsgvo/>*

*Die Server sind ausgelagert bei der IONOS SE, alles weitere finden Sie:
<https://marketport.de/dsgvo/>*

4. Maßnahmen zur Gewährleistung der Belastbarkeit

4.1 Widerstandsfähigkeit- und Ausfallsicherheitskontrolle

*Die Server sind ausgelagert bei der dogardo GmbH, alles weitere finden Sie hier:
<https://marketport.de/dsgvo/>*

*Die Server sind ausgelagert bei der IONOS SE, alles weitere finden Sie:
<https://marketport.de/dsgvo/>*

5. Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1 Kontrollverfahren

☒ Meldung neuer/veränderter Datenverarbeitungsverfahren an den Datenschutzbeauftragten.

☒ Prozesse zur Meldung neuer/veränderter Verfahren sind dokumentiert.

☒ Betroffene Sicherheitsmaßnahmen werden einer regelmäßigen internen Kontrolle unterzogen.

☒ Es wird nach der Qualitätsmanagement-Norm ISO 9001:2015 im Unternehmen gearbeitet

☒ Es wird ein Datenschutz-Management-System eingesetzt.

Diese Dokumentation von technischen und organisatorischen Maßnahmen wurde zuletzt im August 2024 von der Market Port GmbH aktualisiert.