Unirez

Effizienz *steigern.*
Wachstum *fördern.*
IT-Lösungen,
die wirken.

Technische und organisatorische Maßnahmen

Anlage 2 zur Vereinbarung zur Verarbeitung von Daten im Auftrag

IT-Qualität
seit 1967

Unirez GmbH
Ernest-Solvay-Weg 6,
32760 Detmold, Germany
www.unirez.de

Geschäftsführer: Stephan Westerdick
Handelsregister: Lemgo HRB 3451
USt-IdNr: DE124619699
Steuernummer: 313/5821/0985

Sparkasse Paderborn-Detmold-Höxter
IBAN: DE06476501300046040986
BIC: WELADE3LXXX

Als nicht-öffentliche Stelle, die im Auftrag personenbezogene Daten erhebt, verarbeitet oder nutzt, müssen wir technische und organisatorische Maßnahmen treffen, die erforderlich sind, um die Ausführung der Datenschutzvorschriften zu gewährleisten, sofern wir von unseren Kunden mit der entsprechenden Datenverarbeitung beauftragt wurden. Nach DSGVO Art. 32 (1) sind insbesondere Vertraulichkeit, Integrität, Verfügbarkeit und Systembelastbarkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen. Die technischen und organisatorischen Maßnahmen werden regelmäßig einmal jährlich von einem Team aus IT- und Software-Beratern mit Unterstützung unseres externen Datenschutzbeauftragten überprüft, bewertet, die Wirksamkeit evaluiert und gegebenenfalls erweitert und angepasst. Nach einem physischen oder technischen Zwischenfall sind wir durch ein ausgefeiltes Sicherungskonzept, das Hardware, Software, Internetverbindung und Personal berücksichtigt, rasch in der Lage, die Verfügbarkeit und den Zugang zu personenbezogenen Daten wieder herzustellen. Die folgenden technischen und organisatorischen Maßnahmen sind dazu in unserem Unternehmen umgesetzt:

1 Gebäudeabsicherung

- Alarmanlage
- Manuelles Schließsystem
- Videoüberwachung der Zugänge
- Sicherheitsschlösser
- Schlüsselregelung (Schlüsselausgabe etc.)
- Personenkontrolle beim Pförtner / Empfang
- Sorgfältige Auswahl von Reinigungspersonal

2 Absicherung Systemzugang

- Zuordnung von Benutzerrechten
- Einsatz von individuellen Benutzernamen
- Vorgaben für sichere Passwörter
- Authentifikation mit Benutzername/ Passwort
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie (Fernzugriff)
- Sperren von externen Schnittstellen (USB etc.)
- Verschlüsselung von mobilen Datenträgern
- Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum Fern-Löschen)
- Sichere Passwörter für Smartphones
- Verschlüsselung von Smartphone-Inhalten

- Verschlüsselung von Datenträgern in Laptops

3 Sicherstellung von Zugriffsberechtigungen

- Einhaltung des Berechtigungskonzepts
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das „Notwendigste“ reduziert
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
- Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten
- Sichere Aufbewahrung von Datenträgern
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)
- Verschlüsselung von Datenträgern
- Einsatz von Anti-Viren-Software
- Einsatz einer Software-Firewall

4 Sicherheit beim Datentransfer

- Einrichtungen von Standleitungen bzw. VPN-Tunneln
- E-Mail-Verschlüsselung
- Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und –fahrzeugen

5 Nachvollziehbarkeit von Änderungen in Datenvereinbarungen

- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer-namen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

6 Einbindung von Unterauftragsverarbeitern

- Auswahl der (Unter-)Auftragsverarbeiter unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)
- Vorherige Prüfung und Dokumentation der beim Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen
- Schriftlich dokumentierte Weisungen an den Auftragsverarbeiter (z. B. durch Auftragsdatenverarbeitungsvertrag)
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf das Datengeheimnis/ Vertraulichkeit
- Auftragsverarbeiter hat Datenschutzbeauftragten bestellt (wenn erforderlich)
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Wirksame Kontrollrechte gegenüber dem Auftragsverarbeiter vereinbart
- Laufende Überprüfung des Auftragsverarbeiters und seiner Tätigkeiten

7 Schutz von Daten vor zufälliger Zerstörung und Verlust

- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Erstellen eines Backup- und Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort
- Serverräume nicht unter sanitären Anlagen
- Serverräume über der Wassergrenze

8 Maßnahmen zur Zwecktrennung von Daten

- Logische Mandantentrennung (softwareseitig)
- Einhaltung des Berechtigungskonzepts
- Festlegung von Datenbank-Rechten
- Trennung von Produktiv- und Testsystem
- Keine Produktivdaten in Testsystemen