Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

TEAM23 GmbH

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Sicherheitskonzept

Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

Grundsätzliche Maßnahmen

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung überwacht wird.

- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet.

- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet.

- Der Schutz von personenbezogenen Daten wird 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 der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).

Zutrittskontrolle

- Alarmanlage, die automatisch außerhalb der Geschäftszeiten aktiv ist
- Elektronisches Türschloss mit zeitlicher Einschränkung für einzelne Nutzer
- Eigener Serverraum im Büro, der mit einem separaten Schlüssel abgesperrt ist
- Zentrale Schlüsselverwaltung (Zugriff Assistenz/GF)
- Schlüsselregelung / Liste
- Dokumentation der Zugriffe in einem zentralen Dokument
- -Zusätzlich Schlüsselzugriff für berechtigte Mitarbeiter (Büro im 4. Stock)
- Verwaltung durch IT und Personalabteilung
- Fluchttüren nur von innen zu öffnen (Gebäudeverwaltung hat Schlüssel)
- Gebäudesicherheit durch Vermieter, Zugang wird zentral abgesperrt
- Empfang / Rezeption
- Besucher in Begleitung durch Mitarbeiter
- Schließsystem mit Codesperre
- Videoüberwachung der Eingänge
- Klingelanlage mit Kamera
- Sicherheitsschlösser
- Büro im 4. Stock

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Zugangskontrolle

- Anti-Virus-Software Clients
- Firewall
- Login mit Benutzername + Passwort
- Verschlüsselung von Datenträgern
  Die Festplatten aller Arbeitsplatzgeräte sind verschlüsselt

- Verschlüsselung Smartphones
- Richtlinie „Sicheres Passwort“ (12 Zeichen +, Groß-/Kleinschreibung, Mindestens eine Ziffer und Sonderzeichen)
- Temporäres Blocken des Zugriffs nach mehreren ungültigen Login-Versuchen.
  Je nach System: JIRA & Confluence, GitLab, Microsoft 365, LastPass, HubSpot, Miro, Slack

- Einsatz VPN bei Remote-Zugriffen
- Passwortregelung am Arbeitsplatz: Passworteingabe zeitlich begrenzt (Pause zwischen Eingabemöglichkeiten), Regelung zum automatischen Sperren des Arbeitsplatzes.
- Zugriff auf NAS nur über verschlüsselte Verbindung möglich (Login mit Benutzer/Passwort)
- Netzwerk ist in verschiedene VLANs aufgeteilt: Büro, BYOD, Extern, Gäste, ...
- Protokollierung der Zugriffe
- Mobile Device Management
- Intrusion Detection Systeme
- Automatische Desktopsperre
- Erstellen von Benutzerprofilen
- Richtlinie „Clean Desk“
- Verwalten von Benutzerberechtigungen
- Allg. Richtlinie Datenschutz und / oder Sicherheit / EDV
- Mobile Device Policy

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Zugriffskontrolle

- Minimale Anzahl an Administratoren
- Verwaltung Benutzerrechte durch Administratoren
- Alle Mitarbeiter, die mit personenbezogenen Daten Umgang haben, sind gesondert (z.B. durch Vertrag, Verpflichtungserklärung) oder gesetzlich zur Verschwiegenheit verpflichtet
- Rollen- und Berechtigungsmodells
- Applikations-Log-In
  Je nach Anwendung gibt es ein eigenständiges Rechte- und Rollenkonzept. Freigaben werden – so weit sinnvoll - nur einzeln erteilt.

- Identifikation und Authentifizierung der Benutzer
- Protokollierung
  - Zugriffe werden je nach Anwendung protokolliert, bei Auffälligkeiten erfolgt eine automatische Benachrichtigung an alle Administratoren.
  - Datenexport als Verarbeitung und Nutzung.
  - Datenexport kann nur durch einzelne, berechtigte Mitarbeiter durchgeführt werden

- Protokollierung des Zugriffs auf bestimmte Dateien
- E-Mails mit gefährlichen Dateianhängen wie ausführbaren Dateien, mit Passwort verschlüsselten ZIP-Archiven oder Office-Dokumente mit Makros werden vom Mailserver in einen Quarantäne-Ordner zur Analyse verschoben

Trennungskontrolle

- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept
- Getrennte Datenverarbeitung je nach Zweck der Verarbeitung -Zugriffsrechte je nach Rollen/Rechten
  -Persönliche Daten werden bei der Entwicklung in separaten Datenbank-Instanzen vorgehalten (docker Container)

- Vollständige Trennung von anderen Daten innerhalb von IT-Systemen
  - Separate Zugriffsrechte je nach Rollen/Rechten
  - Verschiedene Verzeichnisse zur Vergabe unterschiedlicher Zugriffsrechte

- Mandantenfähigkeit relevanter Anwendungen
  Freigabe auf Projektebene, bei Kommunikation mit Kunden/Dritten:
  - JIRA&Confluence
  - GitLab
  - Microsoft 365
  - Microsoft Sharepoint
  - Miro

- Trennung von Produktiv- und Test-umgebung
- Klare innerbetriebliche Vorgaben für Datenerhebung und Verarbeitung

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Pseudonymisierung & Verschlüsselung

- Zugriff auf öffentliche Webseiten über https-Protokoll
- Reduzierung des Risikos für die Rechte und Freiheiten natürlicher Personen (Pseudonymisierung)
  Abzug der Datenbanken soweit möglich in reduzierter Form (stripped Download), dadurch Reduzierung der verwendeten Datenmenge vor allem in Bezug auf Protokolle und persönliche Daten.

- Pseudonymisierung
  Nutzung von Pseudonymisierung, wenn durch eingesetzte Tools möglich (z.B. Google Analytics)

- Bei der Verwaltung unserer Passwörter, mit Hilfe eines Passwortspeicher, setzen wir auf ein Zero-Knowledge- Verschlüsselung Verfahren. Durch Verschlüsselung mit Hashing und Salting erzeugt die Methode einen Schlüssel, der zur Verschlüsselung (oder Entschlüsselung) Ihres Vaults verwendet wird, in dem Ihre Passwörter gespeichert sind.

Eingabekontrolle

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
  - Protokollierung je nach System unterschiedlich
  - Normal wird protokolliert: Nutzer/Bearbeiter, Zeitpunkt, Aktion

- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts

- Keine nachträgliche Veränderung von Protokolldaten
  Protokolldaten nur mit entsprechenden Rechten einseh- und änderbar

- Klare Zuständigkeiten für Löschungen

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Weitergabekontrolle

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https
- E-Mail-Verschlüsselung
- Einsatz von VPN
- Verschlüsselung von Übermittlungsgegenstand und Verbindung
  Übertragung der Daten über verschlüsselte Protokolle:
  - PGP-E-Mail
  - AirDrop
  - SSH-Zugang zum Server (alternativ FTPS)
  - Austausch verschlüsselter Festplatten/Speichersticks (in Ausnahmen)
  - HTTPS bei Verwendung von Web-basierten Tools
    Übermittlung an Dritte beschränkt sich in der Regel auf:
  - Steuerberater/Rechtsanwalt/...
  - Einsatz von Freelancern

  Freelancer: Es werden die Regelungen zum sicheren Umgang mit den Daten beibehalten, unter anderem: Verschlüsselte Festplatte, Verschlüsselte Übermittlung, Automatische Sperrung des Arbeitsplatzes, ...

- Weitergabepunkte- und Schnittstellendokumentation
  - Einsatz Firewall am Internetzugangspunkt
  - Trennung Netzwerk in verschiedene VLANs
  - Rechner-Firewall ist aktiviert (Arbeitsplatzgeräte)

- Schnittstellenkontrolle
  - Private Nutzung von USB, E-Mail, ... vertraglich ausgeschlossen
  - Stichprobenartige Kontrollen

- Applikationsmanagement
  Jeder Mitarbeiter verfügt über Administratorenrechte, aufgrund eingesetzter Systeme geringes Risiko für Schadsoftware
  Richtlinie zur Installation von Software und Umgang mit Arbeitsplatzgerät:
  - Vertrauenswürdige Quelle
  - Nur Software zur Bewältigung des Arbeitsauftrags

- Speichermedien Einsatz
  Speicherung nur auf verschlüsselten Datenträgern

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Verfügbarkeit und Belastbarkeit

- Patch-Management vorhanden
  Notwendigkeit von Updates sind den Mitarbeitern bewusst, Updates werden durch den Mitarbeiter regelmäßig eingespielt: Kritische Updates: Innerhalb einer Woche, Normale Aktualisierungen: Alle 3 Monate, Stichprobenartig erfolgen Kontrollen durch die IT, Verwaltung und Kontrolle über zentrales MDM

- Backup
  - Backup Zugriff nur durch IT und GF.
  - Backups werden täglich, wöchentlich, monatlich und ggf. jährlich erstellt.

- Serverraum/Rechenzentrum
  Betriebskritische Daten liegen meist extern, bei entsprechenden Dienstleistern:
  - Microsoft
  - Hetzner Cloud
  - domain factory
  ⇒ Absicherung durch Dienstleister gegeben
  - Internes NAS über ein Backup gesichert
  - Backup erstellt tägliche, wöchentliche, monatliche und jährliche Zwischenstände der Daten
  - Eigener Brandmelder im Serverraum

- Serverraumüberwachung Temperatur und Feuchtigkeit
- Serverraum klimatisiert
- Videoüberwachung Serverraum
- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- USV (unterbrechungsfreie Stromversorgung)
- Feuer- und Rauchmeldeanlagen
- Administratoren besitzen zwei Benutzer-Accounts: Einen für reine Administrationsaufgabe und einen für andere Tätigkeiten wie E-Mails lesen oder im Internet surfen Auf jedem PC/Server wird für das lokale Administrator-/Root-Konto ein unterschiedliches und starkes (mind. 16 Stellen) Passwort verwendet

- Interne Netzbereiche unterschiedlicher Sicherheitsstufen werden mittels Firewalls getrennt

Datenschutz-Management

- Software-Lösungen für Datenschutz-Management im Einsatz
- Benennung eines internen Informationssicherheitsbeauftragten
- Benennung eines externen Datenschutzbeauftragten
- Beschäftigte auf Vertraulichkeit verpflichtet
- Regelmäßige Datenschutz- und Informationssicherheitsschulungen der Beschäftigte
- Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Beschäftigte
- Die Datenschutz-Folgenabschätzung (DSFA) werden durchgeführt
- Einheitliche IT-Richtlinien für jeden Mitarbeiter

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster

Incident-Response-Management

- Einbindung von DSB und ISB in Sicherheitsvorfälle und Datenpannen
- Dokumentation von Sicherheitsvorfällen im ISMS
- Dokumentation von Sicherheitsvorfällen und Datenpannen
- Einsatz von Firewall und regelmäßige Aktualisierung
- Einsatz von Virenscanner und regelmäßige Aktualisierung
- Intrusion Prevention System (IPS)

Datenschutzfreundliche Voreinstellungen

- Ausübung des Widerrufsrechts von Betroffenen durch direkte Kontaktmöglichkeiten des Datenschutzbeauftragten
- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind Persönliche Daten aus Kunden-Datenbanken werden nur auf den einzelnen Arbeitsplätzen verarbeitet und nicht zentral gespeichert. Weitergabe intern nur an einzelne Mitarbeiter. Übertragung beispielsweise per AirDrop (Rechner zu Rechner).

Auftragskontrolle (Outsourcing an Dritte)

- Vorherige Prüfung der vom Auftragsverarbeiter getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragsverarbeiters unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Schriftliche Weisungen an den Auftragsverarbeiter
- Verpflichtung der Mitarbeiter des Auftragsverarbeiters auf Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragsverarbeiter bei Vorliegen der
- Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragsverarbeiter
- Regelung zum Einsatz weiterer Unterauftragsverarbeiter
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

TEAM23 GmbH
Beim Glaspalast 1, 86153 Augsburg
Tel.: 0821 / 207 085 0
www.TEAM23.de

Bankverbindung
Stadtsparkasse Augsburg
IBAN: DE12 7205 0000 0250 6727 06
BIC: AUGSDE77XXX

Rechtliches
Registergericht: Augsburg
USt-IdNr.: DE308873371
Registernummer: HRB 26700

Geschäftsführer
Fabian Ziegler
Michaela Schuster