Liste der technischen und organisatorischen Maßnahmen

Datenschutz-Management (organisatorisch)

1. Datenschutzbeauftragter - Interner Datenschutzbeauftragter ist Markus Wolf.
2. Datenschutz-Folgenabschätzung - Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt. Es besteht gemäß Artikel 35 DSGVO keine grundlegende Notwendigkeit.
3. Informationspflichten Betroffene - Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach.
4. Schulung/Verpflichtung - Mitarbeiter werden regelmäßig geschult und sind auf Vertraulichkeit verpflichtet.
5. Sensibilisierung - Eine regelmäßige Sensibilisierung der Mitarbeiter findet mindestens jährlich statt.

Datenschutz-Management (technisch)

1. Datenschutz-Management-Tools - Einsatz von Prive zur Dokumentation und kontinuierlichen Kontrolle datenschutz-relevanter Themen.
2. Dokumentiertes Sicherheitskonzept - Das Sicherheitskonzept zum Datenschutz von envivo als Softwareanwendung ist im Dokument "envivo_Infrastructure Architecture.pdf" dokumentiert.
3. Prüfung technische Schutzmaßnahmen - Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt.

Datenschutzfreundliche Voreinstellungen (technisch)

1. Datenminimierung - Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.

Eingabekontrolle (technisch)

1. Veränderungsprotokollierung - Es erfolgt eine technische Protokollierung der Eingabe, Änderung und Löschung von Daten.

Incident-Response-Management (organisatorisch)

1. Dokumentation Vorgehen mit Datenpannen - Meldung unverzüglich an Vorgesetzten oder DSB (wenn meldepflichtig, Frist von 72 Stunden zur Meldung an Aufsichtsbehörde). Auswirkungen werden unverzüglich auf Minimum begrenzt. Maßnahmen ergreifen, um erneutem Vorfall entgegenzuwirken.

Incident-Response-Management (technisch)

1. Virenscanner - Einsatz von Virenscanner und regelmäßigeAktualisierung
2. Spamfilter - Einsatz von Spamfilter und regelmäßige Aktualisierung
3. Firewall - AWS VPC und Security Groups im Einsatz.
4. Intrusion-Detection-System - Intrusion Detection System (IDS) AWS GuardDuty.

Transport- und Weitergabekontrolle (technisch)

1. Protokollierung der Zugriffe und Abrufe - Protokollierung der Zugriffe und Abrufe
2. Verschlüsselte Verbindungen - Daten werden ausschließlich verschlüsselt über https und ssh übertragen.
3. Webseitenverschlüsselung - Webseiten werden ausschließlich über https bereitgestellt.
4. Signaturverfahren - Nutzung von Signaturverfahren CloudFront / S3 Signed URLs

Trennungskontrolle (technisch)

1. Gesonderte Aufbewahrung - Physische und elektronisch Daten aus dieser Verarbeitungstätigkeit werden von anderen Datensätzen getrennt aufbewahrt.
2. Berechtigungskonzept - Mandantenfähigkeit (auftragsbezogene Daten liegen in einer eigenen Datenbank). Zweckbindung, Datensparsamkeit (keine Weiterverwendung der Daten und keine Speicherung von nicht relevanten Daten). Funktionstrennung (Produktion / Test).

Verfügbarkeitskontrolle (organisatorisch)

1. Dezentrale Aufbewahrung - Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Server-Raums. Details sind im Dokument "envivo_Infrastructure Architecture.pdf" dokumentiert.

2. Backupkonzept - Backup & Recovery-Konzept ist im Dokument "envivo_Infrastructure Architecture.pdf" dokumentiert. Siehe Abschnitt 3 "Disaster Recovery Plan".

3. Backupprotokollierung - Kontrolle des Sicherungsvorgangs ist im Dokument "envivo_Infrastructure Architecture.pdf" dokumentiert. Siehe Abschnitt 3 "Disaster Recovery Plan".

Verfügbarkeitskontrolle (technisch)

1. Verfügbarkeitskontrolle - Alle Daten werden redundant über mehrere Availability Zones bei AWS gespeichert.

Zugangskontrolle (organisatorisch)

1. Passwort-Richtlinien - Sicheres Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts). Automatische Sperrung bei Inaktivität und Fehlversuchen.

2. Telefonate - Für vertrauliche Telefonate können gesonderte Räumlichkeiten genutzt werden.

3. Videokonferenzen - Videokonferenzen werden grundsätzlich hinter verschlossener Tür geführt.

4. Benutzerberechtigungen - Zentrale Verwaltung von Benutzerberechtigungen. Nur berechtige Benutzer dürfen auf Kundendaten zugreifen.

Zugangskontrolle (technisch)

1. Anti-Viren-Software Clients - Systemabhängig relevante Anti-Viren-Software im Einsatz.

2. Passwortschutz - Zugang ist mittels eines Passworts geschützt

3. Datenträgerverschlüsselung - Verschlüsselung von Datenträgern in Laptops / Notebooks

4. Firewall - Einsatz einer Firewall

5. Benutzerprofil Login - Login mit Benutzername + Passwort

6. Zugangskontrolle - Zugangsberechtigungen zu envivo Systemen sind im Dokument "envivo_Infrastructure Architecture.pdf" dokumentiert.

Zugriffskontrolle/Pseudonymisierung (organisatorisch)

1. Autorisierter Zugriff - Zugriff nur für dafür autorisiertes Personal

Zugriffskontrolle/Pseudonymisierung (technisch)

1. Aktenschredder - Nutzung eines Aktenschredders (mind. Stufe 3, cross cut)

Zutrittskontrolle (organisatorisch)

1. Besucherbegleitung - Besucher bewegen sich nur in Begleitung durch Mitarbeiter in den Räumlichkeiten. Sicherheitsbereiche sind festgelegt (Besucherzone, Arbeitsräume, Serverräume)

2. Schlüsselregelung - Schlüsselausgabe ist auf Personen bezogen und wird dokumentiert.

3. Vertrauenswürdiges Reinigungspersonal - Sorgfältige Auswahl von fest-angestelltem Reinigungspersonal

4. Empfang - Personenkontrolle beim Empfang

Zutrittskontrolle (technisch)

1. Elektronisches Schließsystem - Schließsystem über App (nur auf Einladung) und mit zusätzlichem Türcode für den Arbeitsbereich.

2. Alarmanlage - Sicherung des Gebäudes oder Eingängen mittels einer Alarmanlage

3. Codesperre - Schließsystem mit Codesperre

4. Mechanisches Schließsystem - Manuelles Schließsystem

07.01.2020
Arne Geisel

Datum, Verantwortlicher