Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

TMC Amplio GmbH — Stand: Februar 2026

Sicherheitskonzept — Technische und organisatorische Maßnahmen gem. Art. 32 DSGVO

1. Grundsätzliche Maßnahmen

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

- Es ist ein/e Ansprechpartner/in für Datenschutz festgelegt, da keine Benennungspflicht vorliegt.
- Neue Beschäftigte werden zeitnah zum Thema Sicherheit sensibilisiert / geschult.
- Aktuelle Beschäftigte wurden auf Wahrung der Vertraulichkeit verpflichtet.
- Neue Beschäftigte werden zeitnah auf Wahrung der Vertraulichkeit verpflichtet.
- Es erfolgt eine regelmäßige Überprüfung der IST-Situation im Hinblick auf die getroffenen technischen und organisatorischen Maßnahmen (TOM) zur Sicherheit.
- Neue Beschäftigte werden zeitnah zum Thema Datenschutz sensibilisiert / geschult.
- Es erfolgt eine regelmäßige Überprüfung der IST-Situation im Hinblick auf den Datenschutz.
- Es gibt allgemeine Sicherheitsvorgaben für Beschäftigte.
- Es ist ein/e interne Datenschutzkoordinator/in benannt.
- Es gibt festgelegte Abläufe für die Beauftragung von Lieferanten und Dienstleistern, welche
- personenbezogene und/oder sensible Daten verarbeiten. (Auftragskontrolle)
- Der Datenschutzbeauftragte wird bei der Beschaffung oder Erstellung neuartiger Anwendungen, Dienste und Geräte frühzeitig eingebunden, wenn damit personenbezogene Daten verarbeitet werden.
- Es wurde festgelegt, dass bei der Beauftragung von Dienstleistern, deren Tätigkeit keine
- Auftragsverarbeitung darstellt, aber ein Zugriff auf personenbezogene Daten erfolgt oder möglich ist, sowohl eine Prüfung der Zulässigkeit im Hinblick auf die Vorgaben des Datenschutzrechtes, als auch Sicherheitsmaßnahmen erfolgt.
- Es gibt festgelegte Abläufe für den Eintritt und Austritt von Beschäftigten aus dem Unternehmen, sowie bei relevanten Tätigkeitsänderungen.

- Es gibt festgelegte Zuständigkeiten für die Kontrolle und Installation von Sicherheitsupdates und Updates. — Systemhaus
- Es erfolgen regelmäßige, wenn möglich, automatische, Kontrollen und Installationen von Sicherheitsupdates und Updates.
- Es gibt festgelegte Abläufe für die Beschaffung, Inbetriebnahme, Außerbetriebnahme und Rückgabe/Entsorgung von Geräten, Anwendungen und Diensten, mit denen personenbezogene und/oder sensible Daten verarbeitet werden.
- Es besteht ein Konzept zur Wahrung der Betroffenen-Rechte gemäß DSGVO, einschließlich Festlegung der Zuständigkeiten.

2. Zutrittskontrolle

Mithilfe der Maßnahmen der Kategorie »Zutrittskontrolle« soll erreicht werden, dass nur befugte Personen oder Personenkreise physischen Zutritt zu einem Gebäude, Raum oder Bereich haben, in denen personenbezogene Daten verarbeitet werden.

- Elektronisches Schließsystem mit individuell zugeordneten RFID-Tags
- Die Vergabe von RFID-Tags und VPN-Token erfolgt ausschließlich an Mitarbeiter. Die Vergabe erfolgt erst nach Unterzeichnung eines Übergabeprotokolls, in welchem die Vergabe mit Datum festgehalten wird.
- Die Rückgabe von RFID-Tags und VPN-Token erfolgt mit Unterzeichnung eines Übergabeprotokolls, in welchem die Abgabe mit Datum festgehalten wird.
- Der Zutritt zum Serverraum ist ausschließlich ausgewählten Mitarbeitern mittels RFID-Tag mit „Sonderberechtigung“ gestattet
- Ein Zutritt zum Serverraum ist Externen nur in Begleitung von ausgewählten Mitarbeitern gestattet
- Es gibt eine organisierte Herausgabe, Anpassung und Einzug von Zutrittssystemen ("Schlüsselliste").
- Es gibt ein Übergabeprotokoll mit Datum und Untershrift für die Übergabe des RFID-Tags
- Es ist ein Transponder-Schließsystem mit unterschiedlichen Berechtigungen für den Zutritt in unterschiedliche Zutrittsbereiche/-räume vorhanden.
    - Büro (alle Beschäftigten mit entspr. Token)
    - Serverraum (mit spezieller Berechtigung)
- Besucher, welche in Räume ohne Publikumsverkehr Zutritt erhalten sollen, werden abgeholt oder begleitet.

3. Zugangskontrolle

Mithilfe der Maßnahmen der Kategorie »Zugangskontrolle« soll erreicht werden, dass nur befugte Personen oder Personenkreise Zugang zu Datenverarbeitungssystemen haben, in denen personenbezogene Daten verarbeitet werden.

- Mitarbeiter und Beschäftigte sind angewiesen beim Verlassen des PCs den Bildschirm zu sperren: Anweisung in Wiki aufgenommen
- Einsatz von Firewalls: Im gesamten Unternehmensnetzwerk kommt eine Firewall zum Einsatz, die darin betriebene Arbeitsplatzrechner und Server vor unerwünschten Netzwerkzugriffen schützt.
- Passwortfreigabeverfahren und Passwortrücksetzungsverfahren
- Der Log-in erfolgt bei definierten Geräten mit arbeitsplatzspezifischen Zugangsdaten aus nicht personalisierten Benutzername und Passwort (Computer/Netzwerk).
- Der Log-in erfolgt mit Benutzername, Passwort & 2-Faktor (Computer/Netzwerk).
  Für die personenbezogenen Benutzerkonten (Microsoft 365) wurde der 2-Faktor aktiviert.
- Der Log-in erfolgt mit personalisierten Zugangsdaten aus Benutzername und Passwort (Computer/Netzwerk).
- Es sind Vorgaben zur Vergabe von Passwörtern hinsichtlich Länge und Komplexität technisch vorhanden und/oder organisatorisch vorhanden.
  - Groß- und Kleinbuchstaben, Sonderzeichen und Ziffern mit mind. 10 Stellen, sofern vom jew. System/Anwendung zulässig
- Es erfolgt eine geregelte Vergabe, Änderung und Entzug von Zugangsdaten.
  - On-/Offboarding-Checkliste
  - Passwortfreigabeverfahren
  - Passwortrücksetzungsverfahren
- Der Log-in in Anwendungsprogramme erfolgt mit Benutzername, Passwort und 2-Faktor.
- Der Log-in in Anwendungsprogramme erfolgt mit Benutzername und Passwort.
- Es ist eine automatische Sperre von Servern/Computern/Notebooks (manuell je Gerät) vorhanden.
- Es ist ein Virenschutz auf den Clients (Computer, Notebooks u. Ä.) vorhanden: Trend Micro
- Es ist ein Virenschutz auf den Servern vorhanden: Trend Micro
- Es ist sichergestellt, dass die zentrale Firewall regelmäßig mit Sicherheitsupdates versorgt wird: Zuständigkeit: Systemhaus
- Der Zugriff auf Smartphones ist mit einer PIN bzw. einem Code o. Ä. geschützt.
- Der Zugriff auf Tablets ist mit einer Pin bzw. einem Code o. Ä. geschützt.
- Bei Fernzugriffen mithilfe von Apps/Dienste (TeamViewer, pcVisit etc.) zum Support durch externe Dienstleister / Systemhäuser ist die Transportverschlüsselung aktiviert, sofern dies nicht standardmäßig bereits voreingestellt ist.

4. Zugriffskontrolle

Mithilfe der Maßnahmen der Kategorie »Zugriffskontrolle« soll erreicht werden, dass nur befugte Personen oder Personenkreise Zugriff auf die notwendigen personenbezogenen Daten haben und keine unbefugten Personen diese Daten lesen, kopieren, ändern oder löschen können.

- Datenschutztresor: Relevante und sensible Dokumente werden in einem Tresor aufbewahrt
- Sperrung von Zugängen beim Austritt von Mitarbeitern; Verlässt ein Mitarbeiter das Unternehmen, so erfolgt noch vor dessen Austritt die Sperrung bzw. Löschung aller ihm zugewiesenen Zugänge für interne und externe Systeme.
- Verwendung sicherer und individueller Passwörter
- Zentrale Verwaltung von Benutzerzugängen und -rechten
- Zur Sicherstellung der Zugriffskontrolle erfolgt die zentrale Verwaltung von Benutzeridentitäten und Zugriffsrechten über einen Active-Directory-Domain-Controller. Dadurch wird gewährleistet, dass nur berechtigte Personen entsprechend ihrer Aufgaben Zugriff auf personenbezogene Daten erhalten.
- Es erfolgt ein automatisches Monitoring von relevanten Netzwerkzugriffen.
- Es erfolgt eine ordnungsgemäße Vernichtung von Geräten mit Datenträgern und digitalen Datenträgern. Bis zur Vernichtung werden diese Geräte und/oder Datenträger sicher aufbewahrt.
- Es erfolgt eine ordnungsgemäße Vernichtung und Entsorgung von Papierunterlagen durch die Sammlung in abgesicherten Behältnissen ("Datenschutz-Tonne") und Entsorgung durch einen Dienstleister.
- Administrative Nutzer, die im Regelfall auch als nicht administrativer Nutzer die Anwendung verwenden, erhalten - wenn möglich - einen administrativen und nicht administrativen Benutzerzugang.
- Bei Anwendungen kommt - soweit die jeweilige Anwendung es ermöglicht - das Benutzer- und Rechtemanagement zum Einsatz.
- Es kommt ein zentrales Benutzer- und Rechtemanagement (Betriebssystem/Server) zum Einsatz — Microsoft 365
- Es sind Regelungen zum Umgang mit Zugangsdaten für die Beschäftigten vorhanden: On-/Offboarding-Checkliste

5. Trennungskontrolle

Mithilfe der Maßnahmen der Kategorie »Trennungskontrolle« soll erreicht werden, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden.

- Es erfolgt eine Trennung von Entwicklungs-, Test und Produktivumgebung durch logische oder physikalische Trennung.
- Trennung WLAN in WLAN für Mitarbeiter/Beschäftigte und Gäste-WLAN
- Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk
- Speicherung von Daten in kunden- und/oder projektspezifischen Verzeichnissen
- Bei der Nutzung von Anwendungen für die Datenverarbeitung für unterschiedliche Zwecke erfolgt eine logische Trennung, z. B. durch Nutzung von Mandantenfähigkeit der Anwendung oder die Nutzung von Filialen oder Standorten in der Anwendung.
    - Webhosting
    - Nutzung von Kundenaccounts, z. B. Webanalyse
    - Kunden und/oder projektspezifische Verzeichnisse

6. Weitergabekontrolle

Mithilfe der Maßnahmen der Kategorie »Weitergabekontrolle« soll erreicht werden, dass personenbezogene Daten bei der Übertragung bzw. Transport nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

- Bei der Übermittlung sensibler personenbezogener Daten per E-Mail werden Anhänge verschlüsselt übermittelt. Das jeweils notwendige Passwort wird über einen anderen, sicheren Kanal übermittelt oder im Vorfeld festgelegt. — Sofern mit dem Auftraggeber vereinbart und gewünscht; Alternativ Bereitstellung über Online-Speicher oder Projekt-Abwicklungs-Tools
- Beauftragung zuverlässiger Transportunternehmen beim Versand von Datenträgern oder Geräten mit Datenträgern, z.B. DHL / UPS etc.
- Beim Versand von Daten auf dem Postweg oder beim Transport von Servern wird darauf geachtet, dass nur zuverlässige und vertrauenswürdige Transportunternehmen Auftragsverarbeitungsvertrag – Anlage A: KUNDE mit TMC Amplio GmbH eingesetzt werden.
- Protokollierung von Operationen und Zugriffen im Firmennetzwerk; Sämtliche im Firmennetzwerk durchgeführten Operationen und Zugriffe werden protokolliert und der jeweilige Zugriff für sieben Tage gespeichert.
- Entsorgung von Datenträger über Fachunternehmen
- Bereitstellung von Daten online möglich statt E-Mail-Versand, z. B. OneDrive mit Kennwortschutz und Ablaufdatum des Zugrifflinks
- Bei elektronischen Nachrichten (E-Mails) kommt die Transportverschlüsselung (TLS/SSL) zum Einsatz.
- Bei Datenaustausch über gesicherte Online-Speicher wird - wenn möglich - der Zugriff durch ein Passwort abgesichert und zeitlich beschränkt.

7. Eingabekontrolle

- Es erfolgt eine Protokollierung des Systems (Server).
- Nutzung von Benutzer- und Rollenkonzepten für interne und externe Systeme
- Es erfolgt eine Protokollierung des Systems (Computer/Notebook). — Standardprotokollierung
- Es erfolgt eine Protokollierung von Dateneingaben-, Änderungen und Löschungen je nach Anwendung.
    - Moco (Agentursoftware)
    - Hubspot (CRM)
    - Personio (HR-System)

8. Verfügbarkeitskontrolle

Mithilfe der Maßnahmen der Kategorie »Verfügbarkeitskontrolle« soll erreicht werden, dass personenbezogene Daten gegen zufällige Zerstörung und Verlust geschützt sind und die Daten und verarbeitenden Systeme und Ressourcen im Falle eines Ausfalles in angemessener Zeit wiederhergestellt werden können.

- Datensicherungen werden sicher transportiert und aufbewahrt.
- Relevante Systeme sind mindestens redundant an unterschiedlichen Standorten verfügbar.
- Es erfolgt ein Monitoring der Datensicherung und Benachrichtigung über Fehler und erfolgreiche Datensicherungen.
- Verwendung und regelmäßige Aktualisierung eines Virenscanners und Spamfilters
- Verwendung einer Firewall
- Geregelter Prozess zur IT-Beschaffung
- Die Datensicherung wird automatisch geprüft.
- Relevante Server und Dienste / Anwendungen (Container) sind in einem professionellen externen Rechenzentrum ausgelagert.
    - Netzwerkserver (Kundenprojekte)
    - Mail-Server (MS 365)
    - Online-Speicher (MS 365, OneDrive / SharePoint online)
    - DATEV
    - Personio
- Server und relevante Systeme werden durch eine unterbrechungsfreie Stromversorgung (USV) und Überspannungsschutz geschützt.
- Der Serverraum ist nur für befugte Personen zugänglich.
- Datensicherungen werden stichprobenartig auf Vollständigkeit und Funktionalität (Wiederherstellungs-Test) geprüft. — Jährlicher Backup-Recovery-Test durch Systemhaus
- Für relevante Systeme, Dienste und Anwendungen wurden Wartungsverträge vereinbart.
- Es gibt festgelegte interne und externe Ansprechpartner für Probleme und Ausfälle. — Betreuung durch Systemhaus

9. Auftragskontrolle

- Vor der Beauftragung von Dienstleistern erfolgt eine Prüfung, ob eine Auftragsverarbeitung vorliegt oder die Verarbeitung auf Basis einer anderen Rechtsgrundlage erfolgt.
- Der Verantwortliche stellt als Auftragnehmer weist seine Kunden auf die Auftragsverarbeitung hin und stellt Vereinbarungen zur Auftragsverarbeitung online zur Verfügung.
- Unterzeichnung einer Verschwiegenheitserklärung durch alle Mitarbeiter; Alle Mitarbeiter unterzeichnen beim Eintritt in das Unternehmen eine gesonderte Verschwiegenheitserklärung. Darin verpflichten sich die Mitarbeiter, personenbezogene Daten vertraulich zu behandeln und diese ausschließlich auf Weisung ihrer Vorgesetzten zu verarbeiten.
- Der Verantwortliche stellt als Auftragsnehmer sicher, dass alle Mitarbeitende durch regelmäßige Unterweisungen und Schulungen in Webinarform zum Thema Datenschutz geschult werden.
- Der externe Datenschutzbeauftragte kann bei Bedarf zur Bewertung, ob eine Auftragsverarbeitung vorliegt oder nicht, hinzugezogen werden.
- Der externe Datenschutzbeauftragte kann bei Bedarf zur Prüfung der Vereinbarung zur Auftragsverarbeitung hinzugezogen werden.
- Vereinbarungen zur Auftragsverarbeitung werden in Textform festgelegt.
- Der Verantwortliche führt als Auftragnehmer ein Verzeichnis aller Verarbeitungen im Auftrag.
- Der Verantwortliche stellt als Auftragnehmer sicher, dass der Auftraggeber gemäß der Vereinbarung bei Datenschutzvorfällen zeitnah mit den festgelegten Angaben informiert wird.
- Der Verantwortliche stellt als Auftragnehmer sicher, dass der Auftraggeber gemäß der Vereinbarung bei Sicherheitsvorfällen zeitnah mit den festgelegten Angaben informiert wird.
- Der Verantwortliche stellt als Auftragnehmer sicher, dass der Auftraggeber gemäß der Vereinbarung bei Anfragen durch die Aufsichtsbehörde zeitnah mit den festgelegten Angaben informiert wird.