Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Dokumentation der technischen und organisatorischen Maßnahmen zur Sicherstellung der Einhaltung der datenschutzrechtlichen Bestimmung gemäß Datenschutzgrundverordnung seitens der coactum GmbH sowie von ihr beauftragter Unterauftragnehmer

https://www.coactum.de/datenschutz

Stand: 16. September 2019

coactum GmbH
Fürstenallee 11
33102 Paderborn
https://www.coactum.de

Vorbemerkung

Die coactum GmbH gestaltet in ihrem Verantwortungsbereich die innerbetriebliche Organisation so, dass sie den Anforderungen des Datenschutzes gerecht wird. Sie trifft dabei technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten vor Missbrauch und Verlust, um den Anforderungen der DSGVO zu entsprechen.

Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der Weiterentwicklung unterliegen, ist es der coactum GmbH gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei wird sichergestellt, dass das Sicherheitsniveau der festgelegten Maßnahme nicht unterschritten wird. Die coactum GmbH stellt die Sicherheit gem. Art. 28 Abs. 3 lit. c sowie Art. 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO her. Insgesamt handelt es sich bei den getroffenen Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

In diesem Dokument werden die aktuell umgesetzten technischen und organisatorischen Maßnahmen beschrieben. Sofern sich Änderungen ergeben, informiert die coactum GmbH ihre Vertragspartner über die Änderungen und erläutert diese auf Nachfrage. Die Liste der aktuell umgesetzten technischen und organisatorischen Maßnahmen ist jederzeit online unter der Adresse https://www.coactum.de/datenschutz verfügbar.

Die Erbringung des überwiegenden Teils der Dienstleistungen erfolgt über Systeme, die im Rechenzentrum eines Unterauftragnehmers erbracht werden. Die coactum GmbH hat mit diesem eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO getroffen. Im Folgenden werden sowohl die durch die Unterauftragnehmer umgesetzten technischen und organisatorischen Maßnahmen als auch die durch die coactum GmbH umgesetzten Maßnahmen dargelegt. Eine aktuelle Liste der eingesetzten Unterauftragnehmer ist ebenfalls unter der Adresse https://www.coactum.de/datenschutz verfügbar.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Unbefugten wird der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet und genutzt werden, verwehrt.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Festgelegte Sicherheitsbereiche. Individuelle Zutrittsberechtigungsvergabe. Elektronische Zutrittskontrollsysteme und Personal überwachen und gewährleisten den Zutritt zum Data Center nur für autorisierte Personen. Dokumentation von Zutrittsberechtigungen. Zutrittsdokumentation. Rollenabhängige Zutrittsregelungen für die Mitarbeiter (Administratoren, Hilfskräfte, Reinigungspersonal etc.). Besucher-Regulierungen. Automatisches Zuziehen und Verschließen von Türen. Schließung aller Gebäudeeingänge wie Fenster und Türen. Zusätzliche mechanische Schutzmaßnahmen für das Erdgeschoss oder die Kellerfenster. Büroräume außerhalb der Arbeitszeit sind verschlossen. Schutz und Beschränkung der Zutrittswege. Transponder- oder schlüsselkartenbasierte Schließanlage. Videokameras sowie Einbruch- und Kontaktmelder überwachen die Außenhaut des Gebäudes. Dem im Hauptgebäude 24/7 befindlichen Personal werden die Alarmmeldungen angezeigt. Eingezäuntes Gelände inklusive Videoüberwachung.

1.2. Zugangskontrolle

Es wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Zusätzliche Zugangsbeschränkungen der Serverräume. Änderung der Standardkennwörter aller System- und Infrastukturkomponenten. Protokollierung von Benutzer-relevanten Aktivitäten (Anmeldung, Abmeldung, Zugangsverweigerungen etc.). Demilitarisierte Zonen. Schutz der Infrastruktur durch Einbruchmeldeanlagen. Zugangsbeschränkungen für bestimmte IP-Adressbereiche. VPN-Beschränkungen. Sperrung von nicht erforderlichen Ports. Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar). W-LAN-Verschlüsselung. Regelmäßige Software-Updates. Benutzerauthentifizierung für Systemzugang erforderlich. Einschränkung der zeitlichen Gültigkeit der Benutzerkonten. Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins. Zwangs- oder Pflichtänderung der Kennwörter nach der ersten Anmeldung. Ablauf von Benutzerpasswörtern. Erforderliche Mindestkomplexität für Kennwörter. Passwort-Historie zur Verhinderung der Mehrfachnutzung desselben Passworts. Angemessene Gestaltung der Benutzeraccount-Wiederherstellung im Fall eines verlorenen oder vergessenen Authentifizierungsdatensatzes. Verschlüsselte Speicherung von User-Passwörtern. User-Login-Verlauf. Vernichtung von physikalischen Medien nach DIN 32757. Nutzung eines Aktenvernichters (mindestens Sicherheitsstufe 3 gemäß DIN 32757).

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Einhaltung aktueller Sicherheitsstandards. Authentifizierung mit

Benutzername und adäquat komplexem Passwort. Zeitbeschränkte Anmeldung. Verschlüsselung von Datenträgern.

1.3. Zugriffskontrolle

Es wird sichergestellt, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert oder verändert werden können.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Benutzerauthentifizierung für Anwendungszugriff erforderlich. Trennung von Anwendungs- und Administrationszugängen. Regelmäßige Sicherheits-Updates. Überwachung und Protokollierung allgemeiner Benutzeraktivität. Rollenabhängige Zugriffsbeschränkungen. Applikationsbasierte Überprüfung der Eingabeberechtigung.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Berechtigungskonzept mit Rollen und Zugriffsrechten. Differenzierte Rechtevergabe. Dokumentation der Zugriffsbrechtigungen in der Benutzerverwaltung. Beschränkung der Personen mit Administrationsrechten. Löschung von Daten nach Wegfall des Verwendungszwecks. Protokollierung von Zugriffen auf Anwendungen.

1.4. Weitergabekontrolle

Es wird dafür gesorgt, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Externer Zugang nur über sichere Verbindungen (VPN, RDP oder vergleichbar). Kontrollierter Zugang zu E-Mails und Internet. Regelmäßige Sicherheits-Updates. Dokumentation der Weitergabe von physischen Speichermedien. Verbot der Nutzung von privaten Datenträgern.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Nutzung von SSL-verschlüsselter Datenübertragung (https oder vergleichbar) für alle Dienste.

1.5. Trennungskontrolle

Es wird sichergestellt, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werde können.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Rollenbasiertes Berechtigungskonzept. Dokumentation der Vergabe von Zugriffsrechten. Strenge administrative Aufgaben-

trennung. Logische Datentrennung durch separate Datenbanken oder strukturierte Dateiablage. Separate Instanzen für Entwicklungs- und Produktivsysteme (Sandboxes).

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Berechtigungskonzept auf Funktions- und Datenebene. Logische Mandantentrennung. Trennung von Produktiv- und Testdaten. Trennung eigener Daten von Daten des Auftraggebers.

1.6. Pseudonymisierung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Pseudonymisierung von Daten, wo dies möglich ist.

1.7. Verschlüsselung

Die Verarbeitung personenbezogener Daten erfolgt in einer Weise, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

Von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Nutzung von SSL-verschlüsselter Datenübertragung (https oder vergleichbar) für alle Dienste. Zugriff auf Systemebene ausschließlich über sichere Verbindungen (VPN, RDP oder vergleichbar). Kontrollierter Zugang zu E-Mails und Internet. Verschlüsselte Speicherung von Dateien und Backups.

2. Integrität

2.1. Eingabekontrolle

Es kann nachträglich geprüft und festgestellt werden, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Protokollierung von externen Support-Prozessen. Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff. Berechtigungskonzept.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuell vergebene und genutzte Benutzernamen. Protokollierungs- und Protokollauswertungssysteme.

2.2. Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gemäß 1.4 dienen auch der Sicherstellung der Integrität.

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Es wird dafür Sorge getragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Schutz der Infrastruktur durch Hardware-Firewalls. Software-Firewall. Antivirus-Software auf allen Systemen. Überwachung und Protokollierung von administrativen Systemzugängen und von Konfigurationsänderungen. Protokollierung von administrativen Änderungen. Überspannungsschutz der Außenhaut des Gebäudes gegen Blitzeinschlag. Unterbrechungsfreie Stromversorgung (USV) mit Kraftstoffvorrat für mindestens 16 Stunden und Möglichkeit zur Betankung im laufenden Betrieb. Feuer- und/oder Rauchmelder verfügt über eine direkte Aufschaltung bei der örtlichen Feuerwehr. Kühlsystem im Rechenzentrum/Serverraum. Geräte zur Überwachung von Temperatur und Feuchtigkeit im Data Center. Flutung des Data Center mit Argon innerhalb von 60 Sekunden bei Rauchentwicklung bzw. Brand, falls erforderlich. Schutz gegen versehentliche Zerstörung und Verlust.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Serverüberwachung. Regelmäßige Erstellung von Backups.

3.2. Rasche Wiederherstellbarkeit

Es wurden Maßnahmen getroffen, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Disaster-Recovery-Mechanismen für die Datenwiederherstellung. Tägliche inkrementelle Datensicherung. Wöchentliche vollständige Datensicherung. Wöchentliche Backups auf separat gespeicherten physischen Medien oder auf physikalisch getrennten Systemen. Notfallplan. Externe Audits und Sicherheitstests.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Verschlüsseltes Backup an zweitem Standort.

4. Weitere Maßnahmenbereiche

4.1. Datenschutz-Managementsystem

Es wurde ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Regelmäßige Überprüfung der Systemzugangsberechtigungen. Interne und externe Audits. Disziplinarmaßnahmen im Fall einer Datenschutzverletzung. Regelmäßig Sicherheitsprüfungen. Regelmäßige Kontrolle externer Dienstleister. Regelmäßige Besprechungen mit allen Mitarbeitern in Bezug auf Betriebsprozesse, die die Verarbeitung von personenbezogenen Daten betreffen.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Grundsatz bei allen entwickelten Anwendungen ist die Verwendung möglichst datenschutzfreundlicher Voreinstellungen sowie die Minimierung der erhobenen Daten (Privacy by default sowie Privacy by design). Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß Art. 28 Abs. 3 S. 2 lit. b sowie Art. 29 und 32 Abs. 4 DSGVO. Schulungen aller zugriffsberechtigten Mitarbeiter mit regelmäßig stattfindenden Nachschulungen. Bestellung eines Datenschutzbeauftragten, sofern gesetzlich vorgeschrieben. Bestellung eines Informationssicherheitsbeauftragten, sofern gesetzlich vorgeschrieben. Durchführung regelmäßiger IT-Schwachstellenanalysen. Durchführung regelmäßiger interner Audits. Dokumentation zur Nachvollziehbarkeit von Sicherheitsverstößen und Problemen.

4.2. Auftragskontrolle

Es wird dafür gesorgt, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Von den Unterauftragnehmern umgesetzte Maßnahmen: Vertraulichkeitserinnerungen. Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit. Regelmäßige Datenschutz-Unterweisung der Mitarbeiter. Geregeltes Löschen bzw. Entsorgen von Datenträgern. Datentransfer und -weitergabe in Übereinstimmung mit den Anweisungen des Auftraggebers. Schriftliche Richtlinien für die Datenübertragung und -weitergabe. Verbindliche Regeln für die Offenlegung von sensiblen Daten. Datenschutzkonforme Löschung aller Datenkopien und Datensicherungen nach Abschluss des Auftrags. Verarbeitung personenbezogener Daten ausschließlich entsprechend den Weisungen des Auftraggebers. Festgelegte Ansprechpartner für Änderungsanfragen. Kontrollrechte der Auftraggeber bei der Auftragsverarbeitung.

Darüber hinaus von der coactum GmbH für die von ihr erbrachten Dienstleistungen umgesetzte Maßnahmen: Sicherstellung der datenschutzkonformen Löschung von Daten nach Beendigung des Auftrags. Zusicherung der Unterstützung in Fällen notwendiger Aus-

künfte. Vereinbarung zur Auftragsdatenverarbeitung gemäß Art. 28 DSGVO mit Unterauftragnehmern.