PIMCORE
Own the Digital World

Pimcore Technische &
Organisatorische Maßnahmen (TOM)

TECHNISCHE UND ORGANISATORISCHE STANDARDMAßNAHMEN

Zum Schutz von personenbezogenen Daten vor Verlust oder Zugriff durch unbefugte Personen gemäß DSGVO der Pimcore GmbH, im Folgenden kurz PIMCORE genannt:

Alle technisch-organisatorischen Maßnahmen werden kontinuierlich auf Aktualität und Stand der Technik evaluiert und aktualisiert.

1. Interne Verarbeitungstätigkeiten

Physische Zutrittskontrolle

- Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen, in jedem Fall durch Schlüssel oder elektrische Türöffner (Transponder). Die Serverräume, Netzverteiler und TK-Anlagen befinden sich in einem Sperrbereich mit eingeschränktem Zugang und werden ausschließlich von PIMCORE genutzt.
- Zusätzliche Schutzeinrichtungen: Generalschlüsselanlage; Schlüsselregelung; Manuelles Schließsystem; Versperrbare Bürokästen für Rollen mit Aufgaben im Kontext personenbezogener Daten, Anwesenheitskontrolle; Zeiterfassungssystem angeschlossen; Protokollierung; Kontrolle von Remote-/Heimarbeitern; Sorgfalt und Kontrolle von Reinigungs- und Wartungsarbeiten, Einsatz und Sorgfalt bei Auswahl des Revierdienst durch Sicherheitsunternehmen; Besucher in Begleitung durch Mitarbeiter; Eingangstür mit Knauf Außenseite;

Zugangskontrolle für Informationssysteme

- Schutz vor unbefugter Systembenutzung durch Benutzerkennung und Passwortverfahren mit aktuellen Standards entsprechender und validierter Policy (Zeichenzusammensetzung, Länge, regelmäßiger Wechsel, Passworthistorie) oder durch aktuellen Sicherheitsstandards entsprechenden Public-Keys (SSH-Zugänge). Weitere Maßnahmen: Zwei-Faktor-Authentifizierung bei zentralen Benutzerkonten (Active Directory) von MitarbeiterInnen sowie administrativen Benutzerkonten; Bildschirmsperre bei Pausen mit Passwort-Aktivierung ; Erstanmeldeprozedur; geregelte und gesicherte Aufbewahrung von Administrator-& MitarbeiterInnen-Passwörtern; Single-Sign-On; zwingende Verschlüsselung von mobilen Datenträgern; Direktanbindung Internet-Serviceprovider (Glasfaser); Zugriffsberechtigungskonzepte; Hardware-Firewalls; Laufende manuelle/teilw. automatisierte und zentrale Installation von Updates und Sicherheitspatches; zentrale Verwaltung der Konfigurationen; Aufgabenbezogene systemtechnische Trennung bei mehreren Administratoren; getrennte Benutzerkonten für Systemadministratoren; Anwendung des 4-AugenPrinzips bei kritischen Systemänderungen;

Zugriffskontrolle für Informationssysteme

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb der Systeme. Es gibt Standard-Berechtigungsprofile auf „need-to-know-Basis", einen Standardprozess für Berechtigungsvergabe, periodische Überprüfung der vergebenen Berechtigungen. Administrative Benutzerkonten sind auf den kleinstmöglichen Kreis an Administratoren begrenzt und werden mit besonderer Sorgfalt regelmäßig geprüft. Weitere Maßnahmen: Berechtigungskonzepte für Daten, Anwendungen und Betriebssysteme; Protokollierung von Dateizugriffen, Programmausführungen und Richtlinienverstößen; Aufbewahrung der Protokolle für einen angemessenen Zeitraum; Synchronisierung der Uhren zur Auswertung von Protokollen; Keine Administrationsrechte für Nutzer auf Endgeräten ; Prozesse zur Erlangung / Veränderung von Berechtigungen (Neuanlage, Aufgabenänderung, Austritt); Regelmäßige Überprüfung, ob vergebene Berechtigungen noch notwendig sind; Berechtigungen gehören wenn immer möglich nicht zu Personen sondern zu Rollen; Zugriffsschutz durch automatische oder über

Funktionstasten ausgelöste Bildschirmsperre mit ausschließlicher passwortgestützter oder biometrischer Verfahren verifizierter Aufhebung; Regelungen und Kontrolle von externer Wartung und Fernwartung; nur unternehmenseigene Geräte dürfen mit dem internen Netzwerk verbunden werden; Offene oder nicht ausschließlich intern verwendete WLAN-Segmente sind mit einer Firewall vom internen Netz getrennt; die Kommunikation in drahtlosen Netzen erfolgt verschlüsselt; Mobile Endgeräte sind verschlüsselt; Bei Internet-Anwendungen werden Anmeldedaten ausschließlich verschlüsselt übertragen; zentral verwalteter Schutz gegen Malware mit automatisierter Verteilung von Sicherheitsupdates, Firewall mit aktivierter Intrusion Detection und Intrusion Prevention, Vernichtung von Papierunterlagen mit Aktenvernichter

Weitergabekontrolle

- Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung und Transport ausschließlich über verschlüsselte Verbindungen (z.B. HTTPS, SFTP, VPN). Weitere Maßnahmen: Festplattenverschlüsselung bei mobilen Endgeräten; Protokollierung der Übermittlung; Regelungen für Remotearbeiter und Fernwartung (Software, Zugriffsrechte, Zugriffsweg, Freischaltung / Freigabeverfahren, Verschlüsselung, Zugangskontrolle, Monitoring & Protokollierung);

Eingabekontrolle

- Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, durch entsprechende Benutzeridentifizierung, Protokollierung & Einsatz von elektronischen Signaturen bei Vertragsunterzeichnungen.

Auftragskontrolle

- Keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers durch formalisierte Auftragserteilung oder gesonderter Vereinbarung. Kontrolliert und dokumentiert werden in jedem Fall: Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, Art der personenbezogenen

Daten, Kategorien der betroffenen Personen. Alle Mitarbeiter und Sub-Auftragnehmer sind zur Vertraulichkeit verpflichtet.

- Vorherige Prüfung der vom Auftrag- nehmer getroffenen Sicherheitsmaß-nahmen und deren Dokumentation, Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit, Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard- Vertragsklauseln, Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer, Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags, Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Verfügbarkeitskontrolle

- Brandschutzeinrichtungen (Rauch- oder Brandmelder); Feuerlöscher; Rauchverbot in Server- und PC-Arbeitsräumen; zentral verwaltete und automatisch aktualisierte Virenschutz / Schutz vor Schadsoftware; Spamfilter; zentrale IDS und IPS Systeme; Monitoring-Dienste für Pimcore Cloud Edition-Server

2. Webserver

- Der Betrieb der Server erfolgt in Rechenzentren innerhalb der Europäischen Union, die durch unabhängige Stellen nach den Vorgaben der ISO 27001 und anderer Qualitätsrichtlinien zertifiziert wurden. So wird ein hoher Standard für die Bereiche der Zutrittskontrolle, Zugangskontrolle sowie der Verfügbarkeitskontrolle erreicht.
- Sofern die Einrichtung des Webservers ausschließlich durch PIMCORE erfolgt, werden initial die folgenden Maßnahmen ergriffen: Zugriff nur durch berechtigtes und geschultes Personal (Rollenkonzept); Software-Firewall (nur unbedingt notwendige Ports werden geöffnet); Shell-/Administrationszugang nur für eingeschränkten IP Bereich und Personenkreis(Systemadministratoren); Protokollierung der Zugriffe (7 Tage

Speicherdauer); Serverbetrieb ausschließlich für die beauftragte Software; Datenübertragung ausschließlich über verschlüsselte Verbindungen; Auf ausdrücklichen Wunsch des Auftragsgebers können auftragsbedingt oder anlassbezogen Änderungen an den Maßnahmen notwendig sein. Es erfolgt keine laufende Wartung der einmalig eingerichteten Maßnahmen, sofern dies nicht gesondert vertraglich geregelt ist (Wartungsvertrag).

3. Web-Applikationen (Cloud Edition, Lizenzprüfung)

- Der Betrieb der Server erfolgt in Rechenzentren innerhalb der Europäischen Union, die durch unabhängige Stellen nach den Vorgaben der ISO 27001 und anderer Qualitätsrichtlinien zertifiziert wurden. So wird ein hoher Standard für die Bereiche der Zutrittskontrolle, Zugangskontrolle sowie der Verfügbarkeitskontrolle erreicht.
- Die durch PIMCORE erstellten Web-Applikationen werden an den Auftraggeber mit folgenden Schutzmaßnahmen initial übergeben (bei Erstellung der Applikation): Standard-Berechtigungskonzept auf Rollenbasis, passwortauthentifizierte Benutzeraccounts, personalisierte Benutzeraccounts für PIMCORE-Administratoren sowie für den Support oder Beratung befugte Mitarbeiter, Werkzeug zur Kontrolle der Zugriffsrechte, Schutz gegen Brute-Force Attacken, Standardmechanismen zum Schutz vor ungewollten Zugriff
- Kundendaten werden im Rahmen der Leistungen der Pimcore Cloud Edition durch getrennte Instanzen (eigene virtuelle Server und Datenbanken) getrennt bereitgestellt.