TOM
Technische und organisatorische Maßnahmen

pco GmbH & Co. KG

Verantwortliche Person(en):
Mario Mosel, Michael Herzig

Sensitivitätsstufe:
Öffentlich

Letzte Änderung:
Aron Groothus am 30.01.2025

Nächste Prüfung:
31.01.2026

Gültig bis:
31.01.2028

Verteiler
Externe Dritte

Historie

Version	Datum	Autor	Änderungen
1.0	05.11.2024	Aron Groothus	Erstellung eines Entwurfes
1.01	10.01.2025	Aron Groothus	Überarbeitung des Entwurfes
1.02	23.01.2025	Aron Groothus	Überarbeitung nach Bemerkungen von D. Grüschow u. M. Schneider
1.03	30.01.2025	Aron Groothus	Letzte Überprüfung

Inhaltsverzeichnis

1 Einleitung ... 3
1.1 Pco GmbH & Co. KG ... 3
1.2 Geltungsbereich ... 3
1.3 Kontaktpersonen ... 3
2 Managementsystem zur Informationssicherheit ... 4
2.1 Zertifikat ... 4
3 Strategie für Rechenzentren ... 4
4 Vertraulichkeit ... 5
4.1 Zutrittskontrolle ... 5
4.2 Zugangskontrolle ... 5
4.3 Zugriffskontrolle ... 5
4.4 Trennungskontrolle ... 6
5 Integrität ... 6
5.1 Weitergabekontrolle ... 6
5.2 Eingabekontrolle ... 6
6 Verfügbarkeit und Belastbarkeit ... 7
6.1 Verfügbarkeitskontrolle ... 7
7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung ... 7
7.1 Datenschutz-Management ... 7
7.2 Incident-Response-Management ... 7
7.3 Datenschutzfreundliche Voreinstellungen ... 8
7.4 Auftragskontrolle ... 8
7.5 Sensibilisierung der pco-Mitarbeiter ... 8

1 Einleitung

1.1 Pco GmbH & Co. KG

Für Unternehmen des Mittelstands bedeutet IT heute viel mehr als zu den Zeiten unserer Gründung. Deshalb ist die pco GmbH & Co.KG (im Folgenden „pco" oder „Unternehmen" genannt) heute weit mehr als ein Systemhaus für Hard- und Software: Als Erfolgspartner der Kunden entwickelt die pco bedarfsgerechte und punktgenaue IT-Lösungen, die zum langfristigen wirtschaftlichen Vorsprung von Unternehmen beitragen.

Seit dem Gründungsjahr 1984 entwickelt sich die pco konstant weiter und hält höchste Zertifizierungen der bekanntesten Hersteller. Das langjährige Know-how macht die pco zu einem der führenden IT-Dienstleister Norddeutschlands.

Das starke Team aus mittlerweile über 200 Mitarbeitern entwickelt einzigartige Ansätze, in denen Beratung, Betreuung von Systemen und die Bereitstellung von IT-Services zusammengebracht werden.

Ganz getreu dem Markencredo: IT IST ALLES.

Die Sicherheit von Informationen ist für die pco von höchster Bedeutung. Im Rahmen der Verpflichtung zur Einhaltung höchster Sicherheitsstandards und zur Transparenz stellt die pco dieses Dokument bereit. Es enthält detaillierte Informationen zu unseren allgemeinen, technischen und organisatorischen Maßnahmen im Bereich der Informationssicherheit.

Alle Vorgaben und Maßnahmen werden fortlaufend weiterentwickelt und den ändernden Anforderungen angepasst.

Die folgenden aufgeführten technischen und organisatorischen Maßnahmen betreffen beide Standorte der pco:

- Albert-Einstein-Straße 8, 49076 Osnabrück
- Am alten Bahnhof 8, 97332 Volkach

1.2 Geltungsbereich

Dieses Dokument soll Dritten, wie Lieferanten und Dienstleistern, als umfassende Selbstauskunft dienen, um ihre Anfragen zur Informationssicherheit zu beantworten. Die hier aufgeführten Kriterien geben einen Einblick in Sicherheitspraktiken und demonstrieren das Engagement für den Schutz sensibler Daten.

1.3 Kontaktpersonen

Ansprechpartner für Rückfragen für das vorliegende Dokument sind:

CISO	Mario Mosel	Informationssicherheit@pco-online.de
DSB	Michael Herzig	Datenschutz@pco-online.de

2 Managementsystem zur Informationssicherheit

Informationssicherheit verfolgt das Ziel, Informationen jeglicher Art und Herkunft zu schützen. Solche Informationen können in vielfältiger Art und Weise vorliegen, beispielsweise in physischer Form wie z.B. auf Papier, in digitaler Form innerhalb von IT-Systemen oder als (Spezial-) Wissen einzelner Menschen.

Ein angemessenes Sicherheitsniveau kann dadurch sichergestellt werden, dass die Informationssicherheit ein elementarer Bestandteil der Planung, Konzeption, Durchführung und Kontrolle von Geschäftsprozessen und der Informationsverarbeitung ist. Dies kann erreicht werden, indem organisatorische, physische und technische Maßnahmen getroffen werden und in einem Managementsystem zur Informationssicherheit (nachfolgend kurz ISMS) verwaltet, gesteuert und gelebt werden. Ebenso wird durch die Erfassung verschiedenster Anforderungen an die Sicherheit gewährleistet, dass vertragliche, gesetzliche und selbst gesetzte Vorgaben umgesetzt und beachtet werden.

Neben der Informationssicherheit achtet die pco den Datenschutz in besonderer Weise. Für die pco selbst stellt die Verarbeitung personenbezogener Daten zwar kein Hauptbetätigungsfeld dar, die Verarbeitung von personenbezogenen Daten geschieht jedoch häufig im Auftrag, d.h. die pco kommt vorrangig mit personenbezogenen Daten von Kunden in Berührung. Daneben trifft der Datenschutz die pco wie jedes andere Unternehmen im Bereich der Mitarbeiterverwaltung (inkl. Bewerbungsverfahren) sowie der Kundenpflege und Akquise (vorrangig Daten von dort beschäftigten Personen).

2.1 Zertifikat

Die pco implementiert ein ISMS, um die Informationssicherheit gewährleisten und ständig verbessern zu können. Dabei orientiert sich die pco an den Empfehlungen und Vorgaben der ISO/IEC 2700x-Reihe. Dies wurde durch die datenschutz cert GmbH bestätigt: Das Informationssicherheitsmanagementsystem (ISMS) erfüllt die Anforderungen der internationalen ISO/IEC 27001:2017.

3 Strategie für Rechenzentren

Pco setzt auf eine Infrastrukturstrategie, die sich auf den Betrieb und die Betreuung von IT-Umgebungen unserer Kunden konzentriert. Dabei nutzt pco internationale sowie regionale Anbieter von Rechenzentren:

- Microsoft Azure, Amsterdam, NL
- IONOS-Cloud, Berlin
- IONOS-Cloud, Frankfurt
- DATAGROUP, Bremen

Ergänzend betreut pco IT-Infrastrukturen, die direkt in den Rechenzentren der Kunden betrieben werden.

Die von pco genutzten Rechenzentren erfüllen die Anforderungen der ISO/IEC 27001 sowie des C5-Standards (Cloud Computing Compliance Controls Catalogue). Darüber hinaus implementieren diese Rechenzentren zusätzliche Sicherheitsmaßnahmen, die über die Standardzertifizierungen hinausgehen, um ein höchstmögliches Maß an Informationssicherheit zu gewährleisten.

Mit dieser Strategie stellt die pco sicher, dass Kunden von hochverfügbaren, leistungsstarken und umfassend geschützten IT-Infrastrukturen profitieren, unabhängig davon, ob die Systeme in der Cloud, in regionalen Rechenzentren oder direkt vor Ort betrieben werden.

Die Maßnahmen zur Zutrittskontrolle der Anbieter der Rechenzentren erfüllen die Anforderungen der pco. Die technischen und organisatorischen Maßnahmen der oben aufgeführten Anbieter der Rechenzentren können auf Nachfrage bereitgestellt werden.

4 Vertraulichkeit

4.1 Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. Die aufgeführten Maßnahmen zur Zutrittskontrolle betreffen ausschließlich die Räumlichkeiten der pco.

- Besuchermanagement in Verfahrensanweisung geregelt: Anmelden von Besuchern und Begleitpflicht für Besucher, zusätzliche Regelungen für den Bereich des Security Operations Center
- Sicherheitszonenkonzept: definierte Schutzzonen mit jeweiligen (zutrittsbeschränkenden) Sicherheitsmaßnahmen je nach Kritikalität
- Meldewege bei Alarm im Bereitschaftsplan und IT-Notfallhandbuch definiert
- elektronische Zutrittskontrollsysteme mit Zutrittskarten nach Zonenkonzept

4.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Login mit Benutzername und Passwort
- Verwendung von biometrischen Daten
- 2-Faktor-Authentifizierung bei externem Zugriff
- Einsatz VPN bei Remote-Zugriffen
- Automatische Desktopsperre
- Verschlüsselung von Notebooks / Tablets mit Bitlocker
- Sperre externer Schnittstellen (USB)
- Anti-Viren-Software für Server, Clients und mobile Endgeräte
- Diverse Richtlinien: Endbenutzerrichtlinie, Informationssicherheitsleitlinie, Sicherheitsrichtlinie „Mobile Endgeräte“, Sicherheitsrichtlinie „Cloud Computing“, Sicherheitsrichtlinie „Zugriffskontrolle“
- Trennung von normalen und priviligierten Accounts
- Zugangskontrolllisten und Protokolle
- Kontrolle über Geräteausgabe/-rückgabe
- Verwaltung von Benutzerberechtigungen
- Next-Generation Firewall
- Intrusion Detection Systeme

4.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die Nutzungsberechtigten eines Datenverarbeitungssystems 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, verändert oder entfernt werden können.

- Richtlinie zur Kennzeichnung und Klassifizierung von Informationen
- Sicherheitsrichtlinie Löschen und Vernichten von Daten
- Datenschutz- und informationssicherheitskonforme Vernichtung und Löschung von (personenbezogenen) Daten: Aktenschredder, physische Löschung von Datenträgern
- Protokollierung von Zugriffen auf Anwendungen bei der Eingabe, Änderung und Löschung von Daten
- Aufbewahrung von Datenträgern in verschließbaren Schränken (Data Safes)
- Verschlüsselung der Daten während der Übertragung und Speicherung
- Benutzeridentifikation und Authentifizierung

- Verwaltung von Benutzerrechten durch die Administratoren / Berechtigungskonzept: Jährliche oder anlassbezogene Überprüfung der Berechtigungen

4.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung von Produktiv- und Backupsysteme (Systeme / Datenbanken / Datenträger)
- Mandantenfähigkeit relevanter Anwendungen
- Festlegung von Datenbankrechten
- Datenklassifizierung (öffentlich / intern / vertraulich / streng vertraulich)

5 Integrität

5.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, 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.

- Einsatz von VPN
- Verschlüsselung von Daten auf mobilen Datenträgern entsprechend dem Stand der Technik
- Protokollierung der Zugriffe und Abrufe
- Bereitstellung verschlüsselter Verbindungen wie SFTP, HTTPS
- Kontrolle der Bezugsberechtigungen
- Nutzung von Signaturverfahren
- E-Mail Transportverschlüsselung
- E-Mail End-to-End Verschlüsselung
- Sicherheitsrichtlinie "Kryptographie"

5.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Technische Protokollierung der Eingabe, Änderung und Löschung von Daten
- Manuelle oder automatisierte Kontrolle der Protokolle
- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden
- Klare Zuständigkeiten für Löschungen

6 Verfügbarkeit und Belastbarkeit

6.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Virenschutz
- Patchmanagement
- Backup & Recovery-Konzept
- Kontrolle von Sicherungsvorgängen
- Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- Feuer- und Rauchmeldeanlagen
- Serverraumüberwachung: Temperatur und Feuchtigkeit
- Serverraum klimatisiert (redundant)
- Schutzsteckdosenleisten Serverraum
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- RAID System / Festplattenspiegelung
- Betriebsbereitschaft
- Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)

7 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

7.1 Datenschutzmanagement

- Softwarelösungen für das Datenschutzmanagement im Einsatz
- Regelmäßige Überprüfung, Bewertung und Evaluierung der Datenschutzorganisation
- Beschäftigte werden durch Schulungen zum Datenschutz und Datensicherheit geschult und auf die Vertraulichkeit verpflichtet
- Interne Datenschutzkoordination
- Interner Datenschutzbeauftragter und Informationssicherheitsbeauftragter sind benannt
- Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

7.2 Incident-Response-Management

- Einsatz von Firewall, Spamfilter, Virenscanner und deren regelmäßige Aktualisierung
- Intrusion Detection System (IDS) und Intrusion Prevention System (IPS)
- Dokumentierter Prozess zur Erkennung und Meldung von Sicherheits- und Datenschutzvorfällen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- Einbindung von DSB und ISB in Sicherheits- und Datenschutzvorfälle
- Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
- Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheits- und Datenschutzvorfälle
- Sicherheitsrichtlinie „Incident-Management“

7.3 Datenschutzfreundliche Voreinstellungen

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind
- Sicherstellung der Einbindung von ISB / DSB in den Einführungsprozessen neuer Projekte (z.B. Einführung eines neuen Softwaresystems)

7.4 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. ggf. EU Standard-Vertragsklauseln
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Vertraulichkeit bei dem Umgang mit personenbezogenen Daten
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer
- Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
- Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

7.5 Sensibilisierung der Mitarbeiter der pco

Die Mitarbeiter von pco müssen sich ihrer Verantwortung beim Umgang mit personenbezogenen Daten bewusst sein. Datenschutz ist deshalb Teil der Trainingsmaßnahmen und Awareness-Kampagnen im Rahmen des ISMS und wird als Verpflichtung im Rahmen der Endbenutzerrichtlinie kommuniziert.

Sämtliche Mitarbeiter der pco werden schriftlich auf die Wahrung der Vertraulichkeit verpflichtet. Mitarbeiter, die gegen relevante Vorgaben aus dem Datenschutz verstoßen, werden mit angemessenen Sanktionen belegt.