Datenschutzkonzept

der

pco GmbH & Co. KG

Hafenstraße 11, 49090 Osnabrück
Telefon: +49 541 605 1500
E-Mail: info@pco-online.de

IT IST ALLES.

Inhaltsverzeichnis

Gültigkeit

Gültig von:	09.01.2023
Gültig bis:	01.02.2025
Nächste Prüfung:	01.02.2024
Verantwortliche Person(en):	M. Herzig, S. Weinrich
Vertraulichkeit:	Öffentlich/**Intern**/Vertraulich/Streng vertraulich

Änderungshistorie

Datum	Version	Autor	Kommentare
01.06.2016	1.00	M. Steinkamp	Finale Fassung
01.10.2017	1.05	M. Steinkamp	Überarbeitung DSGVO
01.03.2018	1.10	M. Steinkamp	Finalisierung Neufassung
07.05.2019	2.01	M. Herzig, A. Weyert	Überarbeitung
26.03.2020	2.02	M. Herzig, A. Weyert	Überarbeitung, Hinzufügung Sicherheitsrichtlinie für Lieferanten und Sicherheitsrichtlinie Cloud Computing
23.02.2022	2.03	M. Herzig, A. Weyert	Anpassung pco GmbH & Co. KG, Ergänzung um weitere Sicherheitsrichtlinien, Aufnahme weiterer Rechenzentren
04.01.2023	2.04	M. Herzig, S. Weinrich	Grafische Überarbeitung, Anpassung Informationssicherheitsbeauftragter

1. Datenschutz bei der pco

Die pco GmbH & Co.KG (im Folgenden „pco“ oder „Unternehmen“ genannt) achtet 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 ihrer eigenen 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).

Zur Achtung des Datenschutzes für solche Daten bedarf es gar nicht in erster Linie der vielfältigen rechtlichen Verpflichtungen. Die Achtung des Datenschutzes leitet sich direkt aus dem Unternehmensleitbild ab. Es heißt dort: „Wir pflegen einen offenen und respektvollen Umgang mit Kollegen, Kunden und Partnern.“ und „Wir streben langfristige und nachhaltige Partnerschaften an.“ Der respektvolle Umgang mit Kollegen setzt einen konsequenten Beschäftigtendatenschutz ebenso voraus wie der Fokus auf Kunden und eine nachhaltige und langfristige Partnerschaft den Schutz von Daten ihrer Mitarbeiter und Kunden unabdingbar macht.

Besondere personenbezogene Daten i.S.d. Art. 9 Abs. 1 DSGVO werden bei der pco außerhalb der Mitarbeiterverwaltung nicht verarbeitet. Diesbezügliche Rückschlüsse lassen sich lediglich in Einzelfällen aus den Angaben oder Tätigkeitsfeldern von Auftraggebern schlussfolgern.

Ein konsequenter Datenschutz ist dabei ohne eine angemessene Informationssicherheit nicht möglich. Der Bedarf für Informationssicherheit bestand und besteht bei der pco gleichwohl auch unabhängig vom Datenschutz. Da alle wesentlichen strategischen und operativen Geschäftsprozesse im Unternehmen durch Informationstechnologie (IT) maßgeblich unterstützt werden, besteht aus eigenem Anspruch heraus ebenso wie aufgrund von Kundenanforderungen oder Vorgaben von Wirtschaftsprüfern und Kreditgebern die Notwendigkeit, mit Risiken in der Informationsverarbeitung angemessen umzugehen. Datenschutz und Informationssicherheit werden insoweit als Wettbewerbsvorteile, Qualitätsmerkmale und wirkungsvolle Marketingmaßnahmen begriffen.

Die pco hat sich deshalb zur Etablierung eines Managementsystems für Informationssicherheit (ISMS) auf Basis des international anerkannten Standards ISO/IEC 27001 entschieden und sich nach diesem Standard erfolgreich zertifizieren lassen, u.a. manifestiert durch die *Informationssicherheitsleitlinie*.

Es ist Gegenstand dieses Dokuments, die vollständige Erfüllung der Anforderungen aus dem Datenschutz aufzuzeigen, indem auf die entsprechenden Inhalte des ISMS oder vergleichbarer Regelungen verwiesen wird. Dieses Konzept hat selbst keinen anweisenden oder regelnden

Charakter. Ebenso wie die herangezogenen Richtlinien und Konzepte wird es fortlaufend weiterentwickelt und ggf. den sich ändernden Gegebenheiten und Anforderungen im Unternehmen angepasst.

2. Erklärung der Geschäftsleitung

Der Datenschutz ist bereits durch die Erklärung zur Informationssicherheitsleitlinie Teil der verfolgten Informationssicherheitsstrategie. Der Datenschutz wird in den zu beachtenden rechtlichen Grundlagen angeführt, ferner leitet sich eine Beachtung des Datenschutzes direkt aus dem Ziel „Wahrung von Persönlichkeitsrechten und Geschäftsgeheimnissen" sowie indirekt aus dem Ziel „Vermeidung von Ansehensverlust bzw. Imageschaden" ab.

Es ist somit Anspruch und Aussage zugleich, dass der Datenschutz auf allen Ebenen innerhalb der pco beachtet werden soll. Die Geschäftsleitung der pco bekennt sich ausdrücklich zu einer Achtung des Datenschutzes und erwartet von allen Mitarbeitern ein durchgängiges Denken und Handeln in diesem Sinne.

3. Geltungsbereich

Dieses Konzept erläutert vorrangig die nach europäischem Datenschutzrecht beispielsweise in Art. 32 DSGVO geforderten technisch-organisatorischen Maßnahmen.

Eine Festlegung des formalen Geltungsbereiches ist darüber hinaus nicht erforderlich, da durch dieses Konzept keine Regeln und Festlegungen in Kraft gesetzt werden. Der jeweilige Gültigkeitsbereich ergibt sich mithin aus den zugrundliegenden Richtlinien.

Personenbezogene Daten werden zu diesem Zweck grundsätzlich als VERTRAULICH im Sinne der Informationssicherheitsleitlinie klassifiziert und entsprechend geschützt.

4. Datenschutzbeauftragter

Die pco hat gemäß Art. 37 DSGVO i.V.m. § 38 BDSG in der ab dem 25.05.2018 gültigen Fassung **Herrn Michael Herzig** zum betrieblichen Datenschutzbeauftragten bestellt. Er nimmt die ihm kraft Gesetzes und aus betrieblichen oder vertraglichen Regelungen zugewiesenen Aufgaben bei weisungsfreier Anwendung seiner Fachkunde wahr.

Insbesondere ist der Datenschutzbeauftragte mit folgenden Aufgaben betraut:

- Beratung und Information der Geschäftsleitung (z.B. durch regelmäßige Berichte) zur Verfasstheit der Datenschutzorganisation,
- Kommunikation (Anfragen, Auskunftsersuchen, Beschwerden, Meldungen etc.) gegenüber Kunden und den Datenschutzaufsichtsbehörden, soweit dafür keine Vertretungsbefugnis nach außen erforderlich ist,
- Entgegennahme und Nachverfolgung von Hinweisen, Anregungen oder Beschwerden von Mitarbeitern, wobei auf Wunsch absolute Vertraulichkeit gewahrt wird,
- Kontrolle des Verzeichnisses der Verarbeitungstätigkeiten,
- Kontrolle der Verträge, für die eine Auftragsdatenverarbeitung vertraglich zu vereinbaren ist,
- Beratung bei der Durchführung von Datenschutzfolgeabschätzungen sowie
- Schulung aller Mitarbeiter, die ständig mit der Verarbeitung von personenbezogenen Daten beschäftigt sind.

Der Datenschutzbeauftragte hat ein jederzeitiges Vortragsrecht bei der Geschäftsleitung. Ihm werden von der Geschäftsleitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vorgenannten Aufgaben zu erfüllen.

5. Informationssicherheitsbeauftragter

Die pco hat **Herrn Stefan Weinrich** zum Informationssicherheitsbeauftragten (CISO) benannt. Insbesondere ist der Informationssicherheitsbeauftragte mit folgenden Aufgaben betraut:

- Sicherstellung des erforderlichen Informationsflusses für das ISMS.
- Regelmäßige Überprüfung und Aktualisierung der *Informationssicherheitsleitlinie* dahingehend, ob die Vorgaben des Managements adäquat abgebildet sind.
- Regelmäßige Überprüfung bzw. Auditierung des technisch-organisatorischen Sicherheitskonzepts dahingehend, ob einerseits die dort dokumentierten Maßnahmen ausreichend sind, um die Vorgaben des Managements zu gewährleisten; andererseits muss geprüft werden, ob die im technisch-organisatorischen Sicherheitskonzept dokumentierten Sicherheitsmechanismen umgesetzt worden sind und in den Betriebsablauf integriert sind – u.a. eingefordert durch die *Richtlinie zur Durchführung von internen Audits*.
- Regelmäßige Durchführung einer Risikoanalyse mit dem Ziel, die Angemessenheit der technisch-organisatorischen Maßnahmen auf der Grundlage des in der Risikoanalyse

definierten Schutzbedarfs und der identifizierten Bedrohungen zu bewerten – u.a. geregelt in den *Vorgaben zur Risikoanalyse*.

- Stichprobenartige Überprüfung von Systemparametern dahingehend, ob der Zustand eines IT-Systems mit den Einträgen im Change-Management übereinstimmt.
- Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem *Notfallvorsorgekonzept* zusammengestellt. Ziel ist es, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen. Dieses *Notfallvorsorgekonzept* muss regelmäßig aktualisiert werden.

6. Technisch-organisatorische Maßnahmen

6.1 Maßnahmen zur Wahrung der Vertraulichkeit

6.1.1 Zutrittskontrolle

Mit Zutritt im Sinne des Datenschutzes ist die physische Erreichbarkeit von Servern und Clients gemeint, d.h. insbesondere die Möglichkeit, Liegenschaften und Gebäude der pco körperlich zu betreten.

Die pco nutzt unter Rückgriff auf eine Liegenschaft der Hellmann Worldwide Logistics SE & Co. KG (im Folgenden „Hellmann" genannt) ein Multi-Zonen-Konzept, umgesetzt durch den Werkschutz von Hellmann in Bezug auf den äußeren Perimeter und geregelt durch den IT-Bereich von Hellmann für den inneren Perimeter (vgl. *Standardbetriebsverfahren Rechenzentrums-Zutritt von Hellmann*).

Zone 1: Arbeitsplätze der pco befinden sich auf dem **Betriebsgelände „Campus Elbestr./Hafenstr." von Hellmann**, welches das Unternehmen auch für operative Tätigkeiten nutzt. Dadurch ist die Grundstücksgrenze als äußerster Perimeter grundsätzlich abgesichert und eingezäunt (inkl. Kameraüberwachung). Zugänge und Zufahrten sind durch Schrankenanlagen und Personenvereinzelungsschleusen gesichert oder werden von Mitarbeitern des Werksschutzes von Hellmann kontrolliert. Es werden Besucherausweise ausgegeben und es wird eine Besucherdatenbank geführt.

Die Sicherung der Grundstücksgrenze folgt neben einem Eigeninteresse von Hellmann an der Diebstahlssicherung eigener Anlagegüter und als Logistikunternehmen während der Obhut von hochwertigen Kundengütern auch aus der besonderen Stellung von Hellmann als zugelassener Wirtschaftsbeteiligter für Zollrechtliche Vereinfachungen/ Sicherheit. Aus der Zulassung folgt

die regelmäßige Begehung und Kontrolle der Liegenschaften durch Mitarbeiter des zuständigen Hauptzollamtes.

Zone 2: Auf dem Betriebsgelände findet die Datenverarbeitung bei der pco ausschließlich im **geschlossenen Gebäude** „Digital Community Center" (DCC) statt, zu dem der Zutritt beschränkt ist. Außerhalb der üblichen Bürozeiten wird das Gebäude durch den Werkschutz von Hellmann verschlossen, zu den üblichen Bürozeiten ist das Gebäude sowohl in Sichtlinie des Werkschutzes als auch mit einem besetzten Empfang ausgestattet.

Zone 3: Die **Arbeitsplätze** von Mitarbeitern der pco befinden sich in einer geschlossenen Sicherheitszone im Erdgeschoss sowie im zweiten Obergeschoss des DCC mit gesonderter Zutrittssicherung (Kartenleser). Die Türöffnung ist pco-Mitarbeitern bzw. gesondert Berechtigten vorbehalten. Es sind keine Türklingeln etc. vorhanden, Besucher sind am Empfang abzuholen.

Zone 4: Das von Hellmann betriebene **Rechenzentrum** im DCC ist nur aus dem zur Zone 3 gehörenden gesicherten Bereich im Erdgeschoss erreichbar. Der Zutritt ist wenigen Mitarbeitern vorbehalten. Besucher werden begleitet und in einem gesonderten Besucherbuch erfasst. Dienstleister, die im Rechenzentrum Arbeiten durchführen, unterzeichnen gesonderte Verpflichtungserklärungen (vgl. *Standardbetriebsverfahren Rechenzentrums-Zutritt von Hellmann* nebst Anlagen und Vereinbarungen).

Das Rechenzentrum auf dem Campus dient dabei als Ausweichlokation. Die zentrale Informationstechnik wird im Rechenzentrum Georgsmarienhütte des Unternehmens EWE TEL GmbH betrieben. Es handelt sich um ein dediziertes Rechenzentrum ohne Publikumsverkehr, dessen Betrieb erfolgreich unter der ISO/IEC 27001 zertifiziert wurde. Entsprechend sind auch dort alle technisch-organisatorischen Maßnahmen (Werkschutz, Zutrittskontrollsysteme mit einer 2-Faktor-Authentifizierung, Überwachung durch Alarm- und Videokontrollsysteme) innerhalb des ISMS der EWE TEL GmbH geregelt.

Mit Hellmann bzw. der EWE TEL GmbH wurden unter Beachtung der einschlägigen gesetzlichen Vorgaben entsprechende Verträge über das Server-Housing geschlossen.

Darüber hinaus erfolgt die Nutzung weiterer Rechenzentren (u.a. NTT Global Data Centers/ e-shelter in Deutschland, Azure-Rechenzentren von Microsoft in Europa, ...), ebenfalls unter Beachtung der einschlägigen gesetzlichen Vorgaben nebst entsprechender Verträge.

6.1.2 Zugangskontrolle

Mit Zugang im Sinne des Datenschutzes ist die Möglichkeit gemeint, Informationstechnische System benutzen zu können, d.h. i.d.R. sich an IT-Systemen anmelden zu können.

Mitarbeiter der pco verwenden eine eindeutige und individuelle User-ID. Es werden komplexe Passwörter eingesetzt und in sensiblen Bereichen – insbesondere, wenn es sich um einen extern Zugriff handelt - eine starke Authentisierung über zwei Faktoren eingesetzt (2FA). Soweit die Passwortkomplexität nicht durch technische Systeme erzwungen werden kann, sind Mitarbeiter durch die *Endbenutzerrichtlinie* verpflichtet, Passwörter hinreichend komplex zu wählen.

Die User-ID eines internen oder externen Mitarbeiters wird beim Beschäftigungsende deaktiviert, dies wird analog zum Einstellungsprozess durch einen Workflow der Personalabteilung angestoßen.

6.1.3 Zugriffskontrolle

Mit Zugriff im Sinne des Datenschutzes ist die Möglichkeit gemeint, auf konkrete Inhalte (Dateien, Ordner etc.) zugreifen zu können, d.h. über eine entsprechende Berechtigung zu verfügen.

Die pco folgt einem strengen Need-to-know/ Need-to-do-Prinzip auf Basis des fachlichen Berechtigungskonzeptes und schränkt den Zugriff auf Informationen im Sinne eines Whitelistings ein. Für besonders sensible Zugriffe erfolgt eine Zugriffskontrolle über ein 4-Augen-Prinzip.

Es wird ferner die regelmäßige Prüfung der vergebenen Berechtigungen (mindestens jährlich, bei entsprechend klassifizierten Zugriffsrechten auch häufiger) verlangt.

Die unwiderrufliche Löschung vertraulicher und personenbezogener Informationen erfolgt auf Basis der *Sicherheitsrichtlinie zum Löschen und Vernichten von Daten*.

6.1.4 Trennungskontrolle

Mit Trennung im Sinne des Datenschutzes ist die Beachtung der Zweckbindung gemeint, d.h. die Einschränkung der Datennutzung auf den Zweck, zu dem sie erhoben wurden.

Produktion- und Testsysteme sind bei der pco getrennt, ein Multi-Staging-Konzept zur Trennung von Test und Produktion wird umgesetzt inkl. des Verbots, personenbezogene Daten ohne weiteres zu Testzwecken einzusetzen.

Die pco setzt in der Regel mandantenfähige Systeme ein bzw. trennt diese den Einsatz virtualisierter, autarker Systeme. Ordnerstrukturen und Tabellen innerhalb von Datenbanken bzw. gesamte Datenbanken werden strikt getrennt, um eine versehentliche Vermischung von Datenbeständen zu verhindern.

6.2 Maßnahmen zur Wahrung der Integrität

6.2.1 Weitergabekontrolle

Mit Weitergabe im Sinne des Datenschutzes ist die Übertragung von Daten an Empfänger gemeint. Zu kontrollieren ist hier insbesondere, dass eine Übertragung (aber auch Speicherung) gesichert stattfindet und z.B. nicht abgehört werden kann und dass nachvollziehbar ist, wohin Daten übertragen werden.

Vertrauliche Inhalte werden generell nur verschlüsselt versandt unter Verwendung zulässiger Verfahren und Parameter, die in der *Sicherheitsrichtlinie Kryptographie* beschrieben sind. Durch die festgelegten Übertragungswege ist die Übertragung regelmäßig eingeschränkt. Für die Datenübertragung über Netzwerke gelten die internen Vereinbarungen und Regelungen der pco. Nach außen, insbesondere für die regelmäßige Kundenkommunikation, gelten die Vereinbarungen mit dem Kommunikationspartner und das Firewall-Setup der pco. Vorgaben hierzu finden sich in der *Sicherheitsrichtlinie Netzwerk*, *Sicherheitsrichtlinie Wireless-LAN* und der *Sicherheitsrichtlinie Firewall*.

Die Nachvollziehbarkeit der Datenübertragung wird regelmäßig durch Protokollierung und Überwachung gewährleistet. Hierbei ist jedoch immer zu berücksichtigen, dass eine ausufernde Überwachung durch die damit verbundene Leistungs- oder Verhaltenskontrolle nicht in jedem Fall zulässig ist und oft auch nicht in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, weshalb ein Verzicht entsprechend der Regelung in Art. 32 DSGVO regelmäßig geprüft wird.

6.2.2 Eingabekontrolle

Mit Eingabe im Sinne des Datenschutzes ist gemeint, ob und von wem Daten erfasst, verändert oder entfernt wurden.

Eine Kontrolle der Eingabemöglichkeiten selbst wird analog zu Zugangs- und Zugriffskontrollen sichergestellt (s.o.). Die Nachvollziehbarkeit der Dateneingaben wird regelmäßig durch Protokollierung und Überwachung gewährleistet, dessen Umsetzung in der *Sicherheitsrichtlinie Protokollierung und Monitoring* definiert ist. Hierbei ist jedoch, wie bei der Weitergabekontrolle zu berücksichtigen, dass eine ausufernde Überwachung durch die damit verbundene Leistungs- oder Verhaltenskontrolle nicht in jedem Fall zulässig ist und oft auch nicht in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht, weshalb ein Verzicht entsprechend der Regelung in Art. 32 DSGVO regelmäßig geprüft wird.

6.3 Maßnahmen zur Wahrung der Verfügbarkeit und der Belastbarkeit

6.3.1 Verfügbarkeitskontrolle

Mit Verfügbarkeit im Sinne des Datenschutzes ist die Vermeidung von Zerstörung und Verlust von Daten gemeint.

Die Systeme der pco-Systeme sind hochverfügbar und anteilig mehrfach redundant ausgelegt. Die Verfügbarkeit wird durch zahlreiche Schutzmaßnahmen (Klimaüberwachung, Überspannungsschutz) und eine unterbrechungsfreie Stromversorgung nebst NEA (Notstromersatzanlage) unterstützt. Die Datensicherung erfolgt durch die von Hellmann und der EWE TEL GmbH genutzten Infrastrukturen über zwei redundante Rechenzentren auf Basis des *Datensicherungskonzepts*. Es erfolgt ein regelmäßiger Test von Rücksicherungen. Der Umgang mit nicht gänzlich auszuschließenden Notfällen wird im *Notfallvorsorgekonzept* behandelt.

6.3.2 Belastbarkeitskontrolle

Mit Belastbarkeit im Sinne des Datenschutzes ist die Widerstandsfähigkeit („Resilience") gemeint, Aufgaben auch unter widrigen Bedingungen planmäßig zu erfüllen.

Der Grundstein für die sichere Beschaffung und Konfiguration von IT-Systemen wird abhängig von der Geräteart durch die Beachtung der einschlägigen Richtlinien gelegt und das *Computervirenschutzkonzept* etc. aufrechterhalten.

Die Wirksamkeit der Maßnahmen wird zudem regelmäßig durch interne Audits geprüft (inkl. interner Penetrationstests in Form automatisierter Vulnerability Scans), zudem sind die Maßnahmen Gegenstand externer Audits durch Kunden der pco, die sich im Rahmen der Anforderungen aus der Auftragsdatenverarbeitung von der ordnungsgemäßen Datenverarbeitung bei der pco überzeugen. Grundlage zur angemessenen Härtung von PC- und Server-Systemen sind die *Sicherheitsrichtlinie PC-Clients* und die *Sicherheitsrichtlinie zur Härtung von Servern*. Vorgaben zum Patch- und Schwachstellenmanagement finden sich in der *Sicherheitsrichtlinie Patch & Schwachstellenmanagement*.

6.4 Maßnahmen zur Überprüfung und Aufrechterhaltung des Datenschutzes

6.4.1 Incident Response Management

Mit Incident Response im Sinne des Datenschutzes ist insbesondere die Erfüllung von Meldepflichten nach den Art. 33 und 34 DSGVO bei Datenpannen gemeint.

Durch die zuvor beschriebenen technisch-organisatorischen Maßnahmen sowie durch Meldungen von Mitarbeitern und Kunden werden Sicherheitsvorfälle und Datenpannen angemessen erkannt und gemeldet. Vorfälle werden in einem Ticketsystem erfasst, bearbeitet, dokumentiert und einer Nachbetrachtung unterzogen.

In die Bearbeitung von Sicherheitsvorfällen und Datenpannen werden der Informationssicherheitsbeauftragte und der Datenschutzbeauftragte eingebunden. Dem Datenschutzbeauftragten obliegt die Prüfung etwaiger Meldepflichten gegenüber Behörden und Betroffenen, im Falle der Auftragsverarbeitung erfolgt die Abstimmung mit dem Vertragspartner. Der angemessenen Umgang mit Sicherheitsvorfällen und Datenpannen ist in der *Sicherheitsrichtlinie zur Handhabung von Informationssicherheitsvorfällen* beschrieben.

6.4.2 Auftragskontrolle

Mit Auftrag im Sinne des Datenschutzes ist gemeint, einen Dritten mit der Verarbeitung von Daten zu beauftragen. Die Kontrolle soll gewährleisten, dass die Verarbeitung gemäß Weisungen im Rahmen des erteilten Auftrags erfolgt.

Die pco verlangt von allen Auftragnehmern und Support leistenden Unternehmen, die mit personenbezogenen Daten in Kontakt kommen können, die Vereinbarung einer Auftragsverarbeitung entsprechend Art. 28 DSGVO. Außerdem werden mit den beauftragten Unternehmen bzw. deren Mitarbeitern regelmäßig Geheimhaltungsvereinbarungen geschlossen.

Die pco prüft die vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation, die Auswahl jedes Auftragnehmers erfolgt unter Sorgfaltsgesichtspunkten gerade in Bezug auf Datenschutz und Datensicherheit (*vgl. Sicherheitsrichtlinie für Lieferanten und sonstige Auftragnehmer*). Bei längerer Zusammenarbeit ist eine laufende Überprüfung des Auftragnehmers und seines Schutzniveaus obligatorisch. Der Datenschutzbeauftragte ist zur vollständigen Abdeckung aller Verträge frühzeitig in die Prüfung zu involvieren.

6.4.3 Privacy by Design/by Default

Es werden grundsätzlich nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind. Um die Anwendung aller dieses Grundsatzes sowie die Vollständigkeit, Aktualität und Wirksamkeit aller Maßnahmen zu gewährleisten, wird durch den Datenschutzbeauftragten jedes neue Projekt auf die Auswirkung auf die Verarbeitung personenbezogener Daten geprüft.

Insbesondere bei der Nutzung von Cloud-Diensten wird weitgehend vermieden, personenbezogene Daten in Drittstaaten außerhalb der Europäischen Union zu speichern (*vgl. Sicherheitsrichtlinie Cloud Computing*). Andernfalls wird intensiv geprüft und unter Berücksichtigung der geografischen Lage des Cloud-Dienstes, der Art der personenbezogenen

Daten und der verfügbaren technisch-organisatorischen Maßnahmen über den Einsatz entschieden.

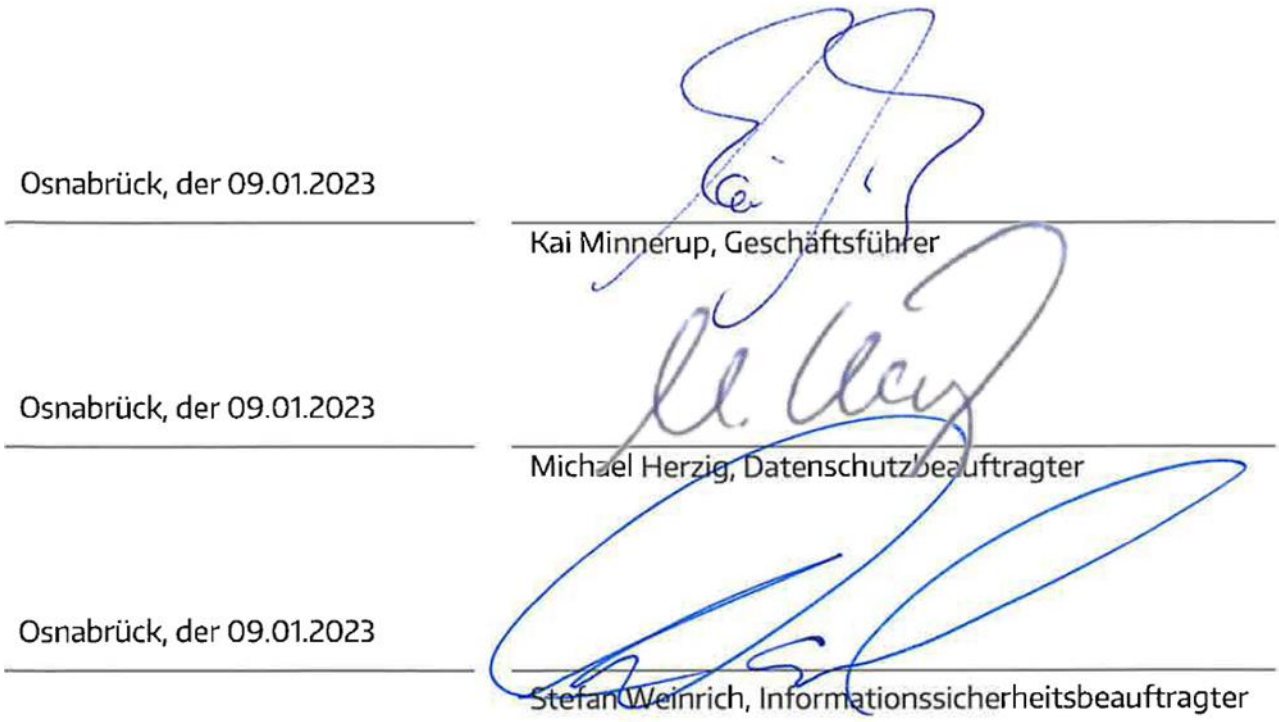
6.4.4 Verantwortung der Mitarbeiter

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 Datenschutz-relevante Vorgaben verstoßen, werden mit angemessenen Sanktionen belegt.

6.4.5 Unterschriften

Die folgenden Unterzeichner bekennen sich ausdrücklich zur Achtung des Datenschutzes und sind sich darüber hinaus einig, dass die in diesem Dokument genannten technisch-organisatorischen Maßnahmen des ISMS die Datensicherheit im Sinne des gesetzlich verpflichtenden und vertraglich vereinbarten Datenschutzes gewährleisten. Die Anforderungen des Datenschutzes werden auch zukünftig im Rahmen des ISMS stets berücksichtigt.



Osnabrück, der 09.01.2023

Kai Minnerup, Geschäftsführer

Osnabrück, der 09.01.2023

Michael Herzig, Datenschutzbeauftragter

Osnabrück, der 09.01.2023

Stefan Weinrich, Informationssicherheitsbeauftragter