ANHANG III

Technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit

Nachfolgend findet sich eine Aufstellung der wesentlichen seitens ANYLINE ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen für den Schutz der Sicherheit sämtlicher Verarbeitungen personenbezogener Daten, die der zugrundeliegenden Vereinbarung zur Datenverarbeitung unterliegen. Die konkrete Ausgestaltung einzelner abstrakter Sicherheitsmaßnahmen wird fortlaufend anhand des Stands der Technik adaptiert und verbessert, wobei eine Angemessenheitsprüfung mittels geeigneter Auditverfahren umgesetzt wird.

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

- ANYLINE verwendet dem Stand der Technik entsprechende Speicherverschlüsselung für die Infrastruktur- und Datenbankkomponenten, auf welchen personenbezogene Daten verarbeitet werden (ISO/IEC 27001:2022 A.5.10, A.8.24 – A.8.27)
- ANYLINE nutzt dem Stand der Technik entsprechende Verschlüsselungsverfahren zum Schutz von personenbezogenen Daten bei der Übertragung (ISO/IEC 27001:2022 A.8.21, A.5.14)
- ANYLINE hat interne Richtlinien bezüglich der Mindeststandards und des angemessenen Einsatzes von Kryptographie als Teil interner Betriebsprozesse etabliert (ISO/IEC 27001:2022 A.8.24)

Maßnahmen zur fortdauernden Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung

- ANYLINE betreibt ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE hat angemessene Informationssicherheitsrichtlinien & -prozesse etabliert (ISO/IEC 27001:2022 8.1, A.5.1)
- ANYLINE hat Richtlinien und Verfahren für den Umgang mit Sicherheits- und Datenschutzvorfällen etabliert (ISO/IEC 27001:2022 A.5.24 – A.5.28, A.5.34)
- ANYLINE hat Wiederherstellungsverfahren für kritische Dienste, welche personenbezogene Daten verarbeiten, definiert (ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.14)
- ANYLINE hat Geschäftskontinuitätspläne etabliert, welche die Anforderungen an die Kontinuität der Informationssicherheit sowie ICT-Funktionalität berücksichtigen (ISO/IEC 27001:2022 A.5.29, A.5.30)
- Kritische Systeme, welche für die Verarbeitung personenbezogener Daten verwendet werden, verfügen über ausreichend Redundanzen & Kapazitäten (ISO 27001 A.8.6, A.8.14)

ANNEX III

Technical and organizational data security measures

The list outlined below composes the essential technical and organizational security measures taken by ANYLINE to protect all processes personal data that is subject to the underlying data processing agreement. The specific implementation of individual abstractly described security measures is continuously adapted and improved in accordance with the state of the art, whereby the adequacy of such measures is assessed on a regular basis through appropriate audit procedures.

Measures for pseudonymization and encryption of personal data

- ANYLINE uses state-of-the-art storage encryption for infrastructure and database components which process personal data (ISO/IEC 27001:2022 A.5.10, A.8.24 – A.8.27)
- ANYLINE uses state-of-the-art encryption methods to protect personal data during transmission (ISO/IEC 27001:2022 A.8.21, A.5.14)
- ANYLINE has established internal policies regarding minimum standards for as well as appropriate usage of cryptography as part of internal operating procedures (ISO/IEC 27001:2022 A.8.24)

Measures to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services

- ANYLINE operates a certified information security management system according to ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE has established appropriate information security policies and processes (ISO/IEC 27001:2022 8.1, A.5.1)
- ANYLINE has established policies and procedures for handling security incidents and data breaches (ISO/IEC 27001:2022 A.5.24 – A.5.28, A.5.34)
- ANYLINE has defined recovery procedures for critical services that process personal data (ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.14)
- ANYLINE has established business continuity plans that consider the requirements for information security continuity and ICT functionality (ISO/IEC 27001:2022 A.5.29, A.5.30)
- Critical systems used for processing personal data have sufficient redundancies and capacities (ISO 27001 A.8.6, A.8.14)

Maßnahmen zur Sicherstellung der Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

- ANYLINE hat Richtlinien und Verfahren für den Umgang mit Sicherheits- und Datenschutzvorfällen etabliert (ISO/IEC 27001:2022 A.5.24 – A.5.28, A.5.34)
- ANYLINE hat Wiederherstellungsverfahren für kritische Dienste, welche personenbezogene Daten verarbeiten, definiert (ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.14)
- ANYLINE hat Geschäftskontinuitätspläne etabliert, welche die Anforderungen an die Kontinuität der Informationssicherheit sowie ICT-Funktionalität berücksichtigen (ISO/IEC 27001:2022 A.5.29, A.5.30)

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

- ANYLINE betreibt ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE führt regelmäßige technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten zum Einsatz kommen, durch (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)
- ANYLINE führt regelmäßige Audits sowie Performancemessungen zur Bewertung der Wirksamkeit des internen Informationssicherheitsmanagementsystems durch (ISO/IEC 27001:2022 9.1, 9.2)

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

- ANYLINE hat interne Richtlinien für die Zugriffs- und Zutrittskontrolle etabliert, welche Regeln und Sicherheitsstandards für die Benutzeridentifikation und -autorisierung hinsichtlich des Zugriffs auf personenbezogene Daten festlegen, etabliert (ISO/IEC 27001:2022 A.5.15 – A.5.18, A.8.3)
- ANYLINE hat Prozesse für die Registrierung/De-Registrierung von Benutzern sowie für die Vergabe von Zugriffsrechten etabliert (ISO/IEC 27001:2022 A.5.16, A.5.18, A.8.3)

Measures to ensure the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident

- ANYLINE has established policies and procedures for handling security incidents and data breaches (ISO/IEC 27001:2022 A.5.24 – A.5.28, A.5.34)
- ANYLINE has defined recovery procedures for critical services which process personal data (ISO/IEC 27001:2022 A.5.29, A.5.30, A.8.14)
- ANYLINE has established business continuity plans that consider the requirements for information security continuity and ICT operability (ISO/IEC 27001:2022 A.5.29, A.5.30)

Procedures for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing

- ANYLINE operates a certified information security management system according to ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE conducts regular technical and organizational security audits covering systems used for the processing personal data (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)
- ANYLINE conducts regular audits and performance measurements to evaluate the effectiveness of the internal information security management system (ISO/IEC 27001:2022 9.1, 9.2)

Measures for user identification and authorization

- ANYLINE has established internal policies for access and entry control, which set rules and security standards for user identification and authorization regarding access to personal data (ISO/IEC 27001:2022 A.5.15 – A.5.18, A.8.3)
- ANYLINE has established processes for user registration/de-registration and granting access rights (ISO/IEC 27001:2022 A.5.16, A.5.18, A.8.3)

Maßnahmen zum Schutz der Daten während der Übermittlung

- ANYLINE nutzt ausschließlich technische angemessen gesicherte und datenschutzkonforme Dienste für den Austausch personenbezogener Daten. (ISO/IEC 27001:2022 A.5.14, A.5.34, A.8.21)
- ANYLINE gibt personenbezogene Daten ausschließlich an die vorab genehmigten Empfänger und gem. den Weisungen der für die Verarbeitung verantwortlichen Stelle weiter (soweit dies im Einklang mit gesetzlichen Vorschriften steht) (ISO/IEC 27001:2022, A.5.14, A.5.31, A.5.34)
- ANYLINE nutzt dem Stand der Technik entsprechende Verschlüsselungsverfahren zum Schutz von personenbezogenen Daten bei der Übertragung (ISO/IEC 27001:2022 A.8.21, A.5.14)

Maßnahmen zum Schutz der Daten während der Speicherung

- ANYLINE verwendet dem Stand der Technik entsprechende Speicherverschlüsselung für die Infrastruktur- und Datenbankkomponenten, auf welchen personenbezogene Daten verarbeitet werden (ISO/IEC 27001:2022 A.5.10, A.8.24 – A.8.27)
- ANYLINE beschränkt die Speicherung von personenbezogenen Daten auf vorab genehmigte, angemessen geschützte sowie datenschutzkonforme Speicherorte (ISO/IEC 27001:2022 A.5.10, A.5.12)
- ANYLINE speichert und verarbeitet personenbezogene Daten, die für unterschiedliche Verarbeitungszwecke erhoben und/oder verarbeitet werden, werden in angemessen technisch voneinander getrennten Umgebungen verarbeitet (ISO/IEC 27001:2022 A.8.3, A.8.22, A.8.31)

Maßnahmen zur Gewährleistung der physischen Sicherheit von Orten, an denen personenbezogene Daten

- ANYLINE hat ein sicherheitsbezogenes physisches Zonenkonzept für Räumlichkeiten, innerhalb derer personenbezogene Daten verarbeitet werden, etabliert (ISO/IEC 27001:2022 A.7.1 – A.7.3)
- ANYLINE beschränkt den Zutritt zu den Räumlichkeiten die zur Verarbeitung personenbezogener Daten genutzt werden auf hierfür explizit autorisiertes Personal und stellt dies mittels geeigneter Authentifizierung und/oder Schlüsselregelungen sicher (ISO/IEC 27001:2022 A.7.1, A.7.2, A.8.3)
- ANYLINE hat Richtlinien für das Arbeiten innerhalb gesicherter Bereiche etablier (ISO/IEC 27001:2022 A.7.6, A7.7, A.8.1)
- ANYLINE hat eine durchgängige „Clean-Desk“ und „Clean Screen“-Richtlinie etabliert (ISO/IEC 27001:2022 A.7.7)

Measures to protect data during transmission

- ANYLINE uses only technically secured and privacy compliant services for the exchange of personal data (ISO/IEC 27001:2022 A.5.14, A.5.34, A.8.21)
- ANYLINE provides personal data exclusively to pre-approved recipients and in accordance with the instructions of the responsible processing entity (as long as this complies with applicable laws and regulations) (ISO/IEC 27001:2022, A.5.14, A.5.31, A.5.34)
- ANYLINE uses state-of-the-art encryption methods to protect personal data during transmission (ISO/IEC 27001:2022 A.8.21, A.5.14)

Measures to protect data during storage

- ANYLINE uses state-of-the-art storage encryption for infrastructure and database components which process personal data (ISO/IEC 27001:2022 A.5.10, A.8.24 – A.8.27)
- ANYLINE restricts the storage of personal data to pre-approved, adequately protected, and data protection-compliant storage locations (ISO/IEC 27001:2022 A.5.10, A.5.12)
- ANYLINE stores and processes personal data collected and/or processed for different processing purposes in environments which are properly separated on a technical level (ISO/IEC 27001:2022 A.8.3, A.8.22, A.8.31)

Measures to ensure the physical security of premises where personal data is processed

- ANYLINE has established a physical zoning concept which security specific requirements for premises where personal data is processed (ISO/IEC 27001:2022 A.7.1 – A.7.3)
- ANYLINE restricts access to premises used for processing personal data to explicitly authorized personnel and enforces this restriction through appropriate authentication and/or key management mechanisms (ISO/IEC 27001:2022 A.7.1, A.7.2, A.8.3)
- ANYLINE has established policies for working within secured areas (ISO/IEC 27001:2022 A.7.6, A7.7, A.8.1)
- ANYLINE has established a "Clean Desk" and "Clean Screen" policy across the organization (ISO/IEC 27001:2022 A.7.7)

Maßnahmen zur Gewährleistung der angemessenen Protokollierung von Ereignissen

- ANYLINE hat klare Anforderungen für die Protokollierung sicherheitsrelevanter Ereignisse definiert, einschließlich der zu protokollierenden Ereignistypen, und hat entsprechende technische Maßnahmen umgesetzt (ISO/IEC 27001:2022 A.8.15)
- ANYLINE führt regelmäßige Prüfungen relevanter Protokolldaten durch, um potenzielle Sicherheitsprobleme oder Schwachstellen frühzeitig zu erkennen (ISO/IEC 27001:2022 A.6.8, A.8.15)

Maßnahmen zur für die sichere Konfiguration sowie den sicheren Betrieb von Systemen

- ANYLINE hat Verfahren für den sicheren Betrieb, die Konfiguration sowie die Wartung von IT-Systemen etabliert (ISO/IEC 27001:2022 A.5.37, A.7.13, A.8.9, A.8.26)
- ANYLINE hat ein internes Änderungsmanagement etabliert, welches Sicherheitsaspekte im Zuge von Änderungen an IT-Systemen mitberücksichtigt (ISO/IEC 27001 A.8.32)
- ANYLINE führt regelmäßige technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten zum Einsatz kommen, durch (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)

Maßnahmen für die interne Governance sowie die Verwaltung der IT und IT-Sicherheit

- ANYLINE betreibt ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE hat Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit und des Datenschutzes definiert (ISO/IEC 27001:2022 A.5.2, A.5.3)
- ANYLINE hat einen dezidierten Datenschutzbeauftragten für die Überwachung der Datenschutzkonformität benannt (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE hat eine Reihe interner Kennzahlen zur Informationssicherheit festgelegt und überwacht diese kontinuierlich (ISO 27001 9.1)
- ANYLINE hat angemessene Informationssicherheitsrichtlinien & -prozesse etabliert (ISO/IEC 27001:2022 8.1, A.5.1)

Measures to ensure an adequate level of event logging

- ANYLINE has defined clear requirements for logging relevant security-related events, including the types of events to be logged, and has implemented appropriate technical measures (ISO/IEC 27001:2022 A.8.15)
- ANYLINE conducts regular reviews of relevant log data to detect potential security issues or vulnerabilities in a timely manner (ISO/IEC 27001:2022 A.6.8, A.8.15)

Measures to ensure secure configuration and operation of systems

- ANYLINE has established procedures for the secure operation, configuration, and maintenance of IT systems (ISO/IEC 27001:2022 A.5.37, A.7.13, A.8.9, A.8.26)
- ANYLINE has established an internal change management process that considers security aspects as part of changes to IT systems (ISO/IEC 27001 A.8.32)
- ANYLINE conducts regular technical and organizational security audits covering systems used for the processing personal data (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)

Measures for internal governance as well as the management of IT and IT security topics

- ANYLINE operates a certified information security management system according to ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE has defined roles and responsibilities in the field of information security and data protection (ISO/IEC 27001:2022 A.5.2, A.5.3)
- ANYLINE has appointed a dedicated data protection officer to monitor data protection compliance (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE has established a set of internal key performance indicators for information security and continuously monitors them (ISO 27001 9.1)
- ANYLINE has established appropriate information security policies and processes (ISO/IEC 27001:2022 8.1, A.5.1)

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

- ANYLINE betreibt ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE führt regelmäßige technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten zum Einsatz kommen, durch (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)
- ANYLINE führt regelmäßige Audits sowie Performancemessungen zur Bewertung der Wirksamkeit des internen Informationssicherheitsmanagementsystems durch (ISO/IEC 27001:2022 9.1, 9.2)

Maßnahmen zur Gewährleistung der Datenminimierung

- ANYLINE beschränkt sämtliche Erhebungen personenbezogener Daten auf die für die zugrundeliegende Verarbeitung minimal erforderlichen Datenfelder (ISO/IEC 27001:2022 A.5.34)
- ANYLINE hat strukturierte Verfahren für die Erhebung personenbezogener Daten sowie der Sicherstellung geeigneter Rechtsgrundlagen etabliert (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE hat Richtlinien und Verfahren für die Pseudonymisierung/Anonymisierung bzw. Maskierung von Daten etabliert, um sämtliche nicht erforderlichen personenbezogenen Referenzen aus Datensätzen zu entfernen (ISO/IEC 27001:2022 A.5.34, A.8.11)
- ANYLINE hat klare Verfahren sowie Aufbewahrungsfristen für die sichere sowie datenschutzkonforme Speicherung und Löschung personenbezogener Daten etabliert (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)

Maßnahmen zur Gewährleistung der Datenqualität

- ANYLINE hat klare Anforderungen für die Protokollierung sicherheitsrelevanter Ereignisse definiert, einschließlich der zu protokollierenden Ereignistypen, und hat entsprechende technische Maßnahmen umgesetzt (ISO/IEC 27001:2022 A.8.15)
- ANYLINE führt regelmäßige Prüfungen relevanter Protokolldaten durch, um potenzielle Sicherheitsprobleme oder Schwachstellen frühzeitig zu erkennen (ISO/IEC 27001:2022 A.6.8, A.8.15)
- ANYLINE hat strukturierte Betriebsprozesse sowie zugehörige Dokumentationen für den sicheren und effektiven Geschäftsablauf etabliert (ISO/IEC 27001:2022 (8.1, A.5.37)

Measures for certification/quality assurance of processes and products

- ANYLINE operates a certified information security management system according to ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE conducts regular technical and organizational security audits covering systems used for the processing personal data (ISO/IEC 27001:2022 9.2, A.5.35, A.5.36, A.8.29, A.8.34)
- ANYLINE conducts regular audits and performance measurements to evaluate the effectiveness of the internal information security management system (ISO/IEC 27001:2022 9.1, 9.2)

Measures to ensure data minimization

- ANYLINE limits all collections of personal data to the minimally required data fields for the underlying processing activity (ISO/IEC 27001:2022 A.5.34)
- ANYLINE has established structured procedures for the collection of personal data and to ensure an appropriate legal basis for them (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE has established policies and procedures for pseudonymization/ anonymization or data masking to remove all unnecessary personal references from datasets (ISO/IEC 27001:2022 A.5.34, A.8.11)
- ANYLINE has established clear procedures and retention periods for the secure and privacy compliant storage and deletion of personal data (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)

Measures to ensure data quality

- ANYLINE has defined clear requirements for logging relevant security-related events, including the types of events to be logged, and has implemented appropriate technical measures (ISO/IEC 27001:2022 A.8.15)
- ANYLINE conducts regular reviews of relevant log data to detect potential security issues or vulnerabilities in a timely manner (ISO/IEC 27001:2022 A.6.8, A.8.15)
- ANYLINE has established structured operational processes and associated documentation for secure and effective business operations (ISO/IEC 27001:2022 (8.1, A.5.37)

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- ANYLINE betreibt ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE hat Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit und des Datenschutzes definiert (ISO/IEC 27001:2022 A.5.2, A.5.3)
- ANYLINE hat einen dezidierten Datenschutzbeauftragten für die Überwachung der Datenschutzkonformität benannt (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE hat eine Reihe interner Kennzahlen zur Informationssicherheit festgelegt und überwacht diese kontinuierlich (ISO 27001 9.1)
- ANYLINE hat angemessene Informationssicherheitsrichtlinien & -prozesse etabliert (ISO/IEC 27001:2022 8.1, A.5.1)
- ANYLINE hat die anwendbaren gesetzlichen und vertraglichen Anforderungen in Bezug auf Informationssicherheit und Datenschutz ermittelt und angemessen adressiert (ISO/IEC 27001:2022 4.1, 4.2, A.5.31 - A.5.34)
- ANYLINE identifiziert, dokumentiert und aktualisiert relevante Aufzeichnungen zur Erfüllung geltender Rechenschaftspflichten im Bereich des Datenschutzes und der Informationssicherheit auf regelmäßiger Basis (ISO/IEC 27001:2022 4.1, 4.2, A.5.31 - A.5.34)
-

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und Datenlöschung

- ANYLINE hat klare Verfahren sowie Aufbewahrungsfristen für die sichere sowie datenschutzkonforme Speicherung und Löschung personenbezogener Daten etabliert (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)
- ANYLINE hat Verfahren für die Beauskunftung sowie Bereitstellung personenbezogener Daten an berechtigte Parteien definiert (ISO/IEC 27001:2022 A.5.34)
- ANYLINE hat ein angemessenes Löschkonzept für die Löschung von personenbezogenen Daten innerhalb der Organisation etabliert (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)

Measures to ensure accountability

- ANYLINE operates a certified information security management system according to ISO/IEC 27001:2022 (ISO/IEC 27001:2022 4.4)
- ANYLINE has defined roles and responsibilities in the field of information security and data protection (ISO/IEC 27001:2022 A.5.2, A.5.3)
- ANYLINE has appointed a dedicated data protection officer to monitor data protection compliance (ISO/IEC 27001:2022 A.5.31, A.5.34)
- ANYLINE has established a set of internal key performance indicators for information security and continuously monitors them (ISO 27001 9.1)
- ANYLINE has established appropriate information security policies and processes (ISO/IEC 27001:2022 8.1, A.5.1)
- ANYLINE has identified and properly addressed applicable legal and contractual requirements regarding information security and data protection (ISO/IEC 27001:2022 4.1, 4.2, A.5.31 - A.5.34)
- ANYLINE identifies, documents, and regularly updates relevant records to fulfill applicable accountability obligations in the field of data protection and information security (ISO/IEC 27001:2022 4.1, 4.2, A.5.31 - A.5.34)

Measures to enable data portability and data deletion

- ANYLINE has established clear procedures and retention periods for the secure and privacy compliant storage and deletion of personal data (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)
- ANYLINE has defined procedures for providing access to personal data through exports or direct access for authorized parties (ISO/IEC 27001:2022 A.5.34)
- ANYLINE has established a suitable data deletion concept for deleting personal data across the organization (ISO/IEC 27001:2022 A.5.34, A.8.10, A.8.11)

Maßnahmen zur Gewährleistung der Datensicherheit entlang der Lieferkette	**Measures to ensure data security along the supply chain**
Sofern ANYLINE im Zuge der Datenverarbeitung eine Übermittlung personenbezogener Daten an (Unter-) Auftragsverarbeiter vornimmt, finden zudem folgenden Maßnahmen Anwendung: • (Unter)-Auftragsverarbeiter, die personenbezogene Daten durch ANYLINE erhalten, werden durch ANYLINE zur Einhaltung technischer und organisatorischer Datensicherheitsmaßnahmen verpflichtet, welche zumindest dem Sicherheits- und Datenschutzniveau der in diesem Dokument angeführten Maßnahmen entsprechen. • Sämtliche (Unter-)Auftragsverarbeiter werden durch ANYLINE dazu verpflichtet, Verfahren zur effektiven Einhaltung datenschutzrechtlicher Pflichten gegenüber ANYLINE bzw. der für die Verarbeitung verantwortlichen Partei zu etablieren (hierunter fallen insbesondere sämtliche Auftragsverarbeiter-Pflichten gem. Art 28 EU-DSGVO) • Sämtliche (Unter-)Auftragsverarbeiter werden von ANYLINE dazu verpflichtet, ANYLINE bei der Einhaltung datenschutzrechtlicher Pflichten angemessen zu unterstützen sowie eine angemessene Kontrolle vorhandener Datenschutzmaßnahmen zu ermöglichen.	If ANYLINE transfers personal data to (sub-)processors as part of the data processing activity, the following measures apply in addition: • (Sub-)processors receiving personal data from ANYLINE are required by ANYLINE to comply with technical and organizational data security measures that at least match the security and data protection level of the measures listed in this document. • All (sub-)processors are required by ANYLINE to establish procedures for effectively complying with data protection obligations towards ANYLINE or the responsible processing party (this especially includes all processor obligations according to Art 28 EU-GDPR) • All (sub-)processors are required by ANYLINE to adequately support ANYLINE in complying with data protection obligations and to enable appropriate control of existing data protection measures.