ANHANG III

Technische und organisatorische Massnahmen einschliesslich zur Gewährleistung der Sicherheit der Daten

Beschreibung der von dem/den Verantwortlichen ergriffenen technischen und organisatorischen Sicherheitsmaßnahmen (einschließlich aller relevanten Zertifizierungen) zur Gewährleistung eines angemessenen Schutzniveaus unter Berücksichtigung der Art, des Umfangs, der Umstände und des Zwecks der Verarbeitung sowie der Risiken für die Rechte und Freiheiten natürlicher Personen Beispiele für mögliche Maßnahmen:

Maßnahmen der Pseudonymisierung und Verschlüsselung personenbezogener Daten

- ANYLINE verwendet eine dem Stand der Technik entsprechende Speicherverschlüsselung für die Infrastruktur- und Datenbankkomponenten, die personenbezogene Daten enthalten (ISO 27001 A.8.1.3, A.8.2.3, A.12.4.2)
- Die Übertragungen personenbezogener Daten werden mittels Stands der Technik entsprechender Verschlüsselungsverfahren geschützt (ISO 27001 A.13.1.2, A.13.2.2, A.13.2.3)
- ANYLINE hat interne Richtlinien bezüglich der Mindeststandards und des angemessenen Einsatzes von Kryptographie als Teil ihrer technischen Betriebsprozesse erstellt (ISO 27001 A.10.1.1, A.10.1.2, A.12.1.1)

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

- ANYLINE hat ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2013 etabliert (ISO 27001 4 - 10)
- ANYLINE hat eine Politik und ein Verfahren für das Management von Sicherheits- und Datenschutzvorfällen eingeführt (ISO 27001 A.16.1.1 - .7)
- ANYLINE hat Wiederherstellungsverfahren für kritische Dienste, die personenbezogene Daten verarbeiten, sind definiert (ISO 27001 A.17.1.1, A.17.1.2)
- ANYLINE hat Geschäftskontinuitätspläne definiert, die unter Anderem Anforderungen an die Kontinuität der Informationssicherheit berücksichtigen (ISO 27001 A.17.1.1, A.17.1.2)
- Kritische Systeme, welche für die Verarbeitung personenbezogener Daten verwendet werden, sind redundant ausgeführt (ISO 27001 A.17.2.1)

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 eine Richtlinie sowie einen zugehörigen Prozess für den Umgang mit Sicherheits- und Datenschutzvorfällen etabliert (ISO 27001 A.16.1.1 - .7)
- Für kritische Services, die personenbezogene Daten verarbeiten, sind angemessene Wiederherstellungsverfahren definiert (ISO 27001 A.17.1.1, A.17.1.2)

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

- ANYLINE hat ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2013 etabliert (ISO 27001 4 - 10)
- ANYLINE führt regelmäßig technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten eingesetzt werden, durch (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)
- ANYLINE führt regelmäßig Audits sowie Performancemessungen zur Bewertung der Wirksamkeit des internen Informationssicherheitsmanagementsystems durch (ISO 27001 9.1, 9.2)

ANNEX III

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Description of the technical and organisational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

- ANYLINE uses state-of-the-art storage encryption for the infrastructure and databases components containing personal data of customers (ISO 27001 A.8.1.3, A.8.2.3, A.12.4.2)
- All transfers or personal data are protected through state-of-the-art encryption (ISO 27001 A.13.1.2, A.13.2.2, A.13.2.3)
- ANYLINE established internal guidelines regarding the minimal standards and appropriate usage of cryptography as part of its technical operating procedures (ISO 27001 A.10.1.1, A.10.1.2, A.12.1.1)

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

- ANYLINE established a certified information security management system in accordance with ISO/IEC 27001:2013 (ISO 27001 4 – 10)
- ANYLINE established a security and privacy incident management policy and process (ISO 27001 A.16.1.1 – .7)
- ANYLINE has defined recovery procedures for critical services, which process personal data (ISO 27001 A.17.1.1, A.17.1.2)
- ANYLINE defined business continuity plans which consider also consider information security continuity requirements (ISO 27001 A.17.1.1, A.17.1.2)
- Critical systems used for the processing of personal data are implemented in a redundant way (ISO 27001 A.17.2.1)

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

- ANYLINE established a security and privacy incident management policy and process (ISO 27001 A.16.1.1 – .7)
- For critical services, which process personal customer data, ANYLINE defined adequate recovery procedures (ISO 27001 A.17.1.1, A.17.1.2)

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

- ANYLINE established a certified information security management system in accordance with ISO/IEC 27001:2013 (ISO 27001 4 - 10)
- ANYLINE performs regular technical and organisational security audits on systems used in the processing of personal data (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)
- ANYLINE performs regular audits regarding the effectiveness of the internal information security management system and monitors its performance (ISO 27001 9.1, 9.2)

Maßnahmen zur Identifizierung und Autorisierung der Nutzer

- ANYLINE hat eine interne Richtlinie für die Zugriffskontrolle etabliert, welche Regeln und Sicherheitsstandards für die Benutzeridentifikation und -autorisierung auf Systemen, die persönliche Daten verarbeiten, definiert (ISO 27001 A.9.1.1)
- ANYLINE hat Prozesse für die Registrierung/De-Registrierung von Benutzern sowie für die Vergabe von Zugriffsrechten etabliert (ISO 27001 A.9.2.1, A.9.2.2, A.9.2.3)

Maßnahmen zum Schutz der Daten während der Übermittlung

- Der gesamte Datenaustausch personenbezogener Daten zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter erfolgt ausschließlich über sichere Dienste (ISO 27001 A.13.1.2, A.13.2.1, A.13.2.2)
- Die Weitergabe von personenbezogenen Daten ist auf vorab genehmigte Empfänger beschränkt (ISO 27001 A.13.2.1)
- Die Übertragungen personenbezogener Daten werden mittels Stand der Technik entsprechender Verschlüsselungsverfahren geschützt (ISO 27001 A.13.1.2, A.13.2.2, A.13.2.3)

Maßnahmen zum Schutz der Daten während der Speicherung

- ANYLINE verwendet eine dem Stand der Technik entsprechende Speicherverschlüsselung für die Infrastruktur- und Datenbankkomponenten, die personenbezogene Daten enthalten (ISO 27001 A.8.1.3, A.8.2.3, A.12.4.2)
- Die Speicherung von personenbezogenen Daten ist auf vorab genehmigte Speicherorte beschränkt, die anhand der internen Sicherheitsstandards überprüft werden (ISO 27001 A.8.2.1, A.8.2.3)
- Personenbezogene Daten, die für unterschiedliche Verarbeitungszwecke erhoben und/oder verarbeitet werden, sind in getrennten technischen Umgebungen gespeichert (ISO 27001 A.12.1.4, A.13.1.3)

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

- Ein sicheres Zonenkonzept für physische Standorte, an denen personenbezogene Daten verarbeitet werden, ist als Teil einer internen Richtlinie für die physische Sicherheit definiert (ISO 27001 A.11.1.1, A.11.1.2, A.11.1.3)
- Der Zutritt zu den Einrichtungen des Auftragsverarbeiters ist auf autorisiertes Personal beschränkt und durch Authentifizierung mittels Sicherheitstoken gesichert (ISO 27001 A.11.1.1, A.11.1.2)
- Regeln für das Arbeiten in Sicherheitsbereichen sind definiert (ISO 27001 A.11.1.5, A.11.2.8)
- ANYLINE hat klare Anlieferungs- und Ladezonen für ihre physischen Bürostandorte definiert (ISO 27001 A.11.1.6)
- Innerhalb der gesamten Organisation ist eine „Clean-Desk“ und „Clean Screen“-Richtlinie für etabliert (ISO 27001 A.11.2.9)

Maßnahmen zur Gewährleistung der Protokollierung von Ereignissen

- ANYLINE hat klare Anforderungen für die Protokollierung von sicherheitsrelevanten Ereignissen definiert, einschließlich der zu protokollierenden Ereignistypen, und hat entsprechende technische Maßnahmen umgesetzt (ISO 27001 A.12.4.1, A.12.4.2, A.12.4.3)
- ANYLINE führt fortlaufende Überprüfungen relevanter Protokolldaten durch, um potenzielle Sicherheitsprobleme frühzeitig zu erkennen (ISO 27001 A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.3)

Maßnahmen zur Gewährleistung der Systemkonfiguration, einschließlich der Standardkonfiguration

- Verfahren für den sicheren Betrieb, die Konfiguration und die Wartung von IT-Systemen sind definiert und dokumentiert (ISO 27001 A.12.1.1)
- ANYLINE hat ein internes Änderungsmanagement etabliert, welches Sicherheitsaspekte bei technischen Änderungen

Measures for user identification and authorisation

- ANYLINE has established an internal access control policy defining rules and security standards for the user identification and authorization on systems processing personal data (ISO 27001 A.9.1.1)
- ANYLINE established processes for the user registration/deregistration as well as access right provisioning (ISO 27001 A.9.2.1, A.9.2.2, A.9.2.3)

Measures for the protection of data during transmission

- All data exchange of personal data between the controller and the processor is done exclusively via secure services (ISO 27001 A.13.1.2, A.13.2.1, A.13.2.2)
- Personal data transfer is limited to pre-approved recipients (ISO 27001 A.13.2.1)
- All transfers or personal data are protected through state-of-the-art encryption (ISO 27001 A.13.1.2, A.13.2.2, A.13.2.3)

Measures for the protection of data during storage

- ANYLINE uses state-of-the-art storage encryption for the infrastructure and databases components containing personal data of customers (ISO 27001 A.8.1.3, A.8.2.3, A.12.4.2)
- Storage of personal data is limited to pre-approved storage locations, which are verified against the internal security standards (ISO 27001 A.8.2.1, A.8.2.3)
- Personal data collected and/or processed for different processing purposes are stored in separate technical environments (ISO 27001 A.12.1.4, A.13.1.3)

Measures for ensuring physical security of locations at which personal data are processed

- A security zone concept for physical locations, in which personal data is processed, is defined as part of an internal physical security policy (ISO 27001 A.11.1.1, A.11.1.2, A.11.1.3)
- The access to facilities of the processor is limited to authorized personnel and secured through authentication via security tokens (ISO 27001 A.11.1.1, A.11.1.2)
- Rules for working within secure areas are defined (ISO 27001 A.11.1.5, A.11.2.8)
- ANYLINE has defined clear delivery and loading areas for its physical office locations (ISO 27001 A.11.1.6)
- A clear desk and clear screen policy is established within the entire organisation (ISO 27001 A.11.2.9)

Measures for ensuring events logging

- ANYLINE defined clear requirements for the logging of security relevant events, including which event-types to log, and implemented respective technical capabilities (ISO 27001 A.12.4.1, A.12.4.2, A.12.4.3)
- ANYLINE performs ongoing reviews of relevant log events for early detection of potential security issues (ISO 27001 A.12.4.1, A.12.4.3, A.16.1.2, A.16.1.3)

Measures for ensuring system configuration, including default configuration

- Procedures for the secure operation, configuration and maintenance of IT systems are defined and documented (ISO 27001 A.12.1.1)
- ANYLINE has established an internal change management process to review and address security aspects of any

an IT-Systemen prüft und adressiert (ISO 27001 A.12.1.2)

- ANYLINE führt regelmäßig technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten eingesetzt werden, durch (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)

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

- ANYLINE hat ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2013 etabliert (ISO 27001 4 - 10)
- ANYLINE hat klare Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit und des Datenschutzes definiert (ISO 27001 A.6.1.1, A.6.1.2)
- ANYLINE hat eine Reihe interner Kennzahlen zur Informationssicherheit festgelegt und überwacht diese kontinuierlich (ISO 27001 9.1)
- Ein organisationsweiter Satz von Richtlinien für die Informationssicherheit und den Datenschutz ist definiert und innerhalb der Organisation kommuniziert (ISO 27001 A.5.1.1, A.5.1.2)

Maßnahmen zur Zertifizierung/Qualitätssicherung von Prozessen und Produkten

- ANYLINE hat ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2013 etabliert (ISO 27001 4 - 10)
- ANYLINE führt regelmäßig technische und organisatorische Sicherheitsaudits für Systeme, die bei der Verarbeitung personenbezogener Daten eingesetzt werden, durch (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)
- ANYLINE führt regelmäßig Audits sowie Performancemessungen zur Bewertung der Wirksamkeit des internen Informationssicherheitsmanagementsystems durch (ISO 27001 9.1, 9.2)

Maßnahmen zur Gewährleistung der Datenminimierung

- Die Erhebung personenbezogener Daten beschränkt sich auf die minimal erforderlichen Datenfelder
- Die Erhebung personenbezogener Daten erfolgt nach vordefinierten Verfahren zur Datensammlung
- Wo immer möglich, werden persönliche Identifikatoren während der Erhebung aus den Datensätzen ausgeschlossen

Maßnahmen zur Gewährleistung der Datenqualität

- ANYLINE hat klare Anforderungen für die Protokollierung von sicherheitsrelevanten Ereignissen definiert, einschließlich der zu protokollierenden Ereignistypen, und hat entsprechende technische Maßnahmen umgesetzt (ISO 27001 A.12.4.1, A.12.4.2, A.12.4.3)

Maßnahmen zur Gewährleistung einer begrenzten Vorratsdatenspeicherung

- Personenbezogene Daten, die für unterschiedliche Verarbeitungszwecke erhoben und/oder verarbeitet werden, sind in getrennten technischen Umgebungen gespeichert (ISO 27001 A.12.1.4, A.13.1.3)
- ANYLINE hat klare Aufbewahrungsfristen für alle erhobenen personenbezogenen Daten definiert

Maßnahmen zur Gewährleistung der Rechenschaftspflicht

- ANYLINE hat ein zertifiziertes Informationssicherheitsmanagementsystem nach ISO/IEC 27001:2013 etabliert (ISO 27001 4 - 10)
- ANYLINE hat klare Rollen und Verantwortlichkeiten im Bereich der Informationssicherheit und des Datenschutzes definiert (ISO 27001 A.6.1.1, A.6.1.2)
- ANYLINE hat eine Reihe interner Kennzahlen zur Informationssicherheit festgelegt und überwacht diese kontinuierlich (ISO 27001 9.1)
- Ein organisationsweiter Satz von Richtlinien für die

technical changes to IT systems (ISO 27001 A.12.1.2)

- ANYLINE performs regular technical and organisational security audits on systems used in the processing of personal data (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)

Measures for internal IT and IT security governance and management

- ANYLINE established a certified information security management system in accordance with ISO/IEC 27001:2013 (ISO 27001 4 – 10)
- A clear set of roles and responsibilities in the area of information security and privacy are defined (ISO 27001 A.6.1.1, A.6.1.2)
- ANYLINE established and monitors and internal set of information security related KPIs (ISO 27001 9.1)
- An organisation wide set of policies for information security and privacy is defined and communicated within ANYLINE (ISO 27001 A.5.1.1, A.5.1.2)

Measures for certification/assurance of processes and products

- ANYLINE established a certified information security management system in accordance with ISO/IEC 27001:2013 (ISO 27001 4 - 10)
- ANYLINE performs regular technical and organisational security audits on systems used in the processing of personal data (ISO 27001 A.14.2.8, A.18.2.2, A.18.2.3)
- ANYLINE performs regular audits regarding the effectiveness of the internal information security management system and monitors its performance (ISO 27001 9.1, 9.2)

Measures for ensuring data minimisation

- All personal data collection is limited to the minimal required data fields
- The collection of personal data follows defined collection procedures
- Where possible, personal identifiers are excluded from data sets during collection

Measures for ensuring data quality

- ANYLINE defined clear requirements for the logging of security relevant events, including which event-types to log, and implemented respective technical capabilities (ISO 27001 A.12.4.1, A.12.4.2, A.12.4.3)

Measures for ensuring limited data retention

- Personal data collected and/or processed for different processing purposes are stored in separate technical environments (ISO 27001 A.12.1.4, A.13.1.3)
- ANYLINE defined clear retention periods for all collected personal data

Measures for ensuring accountability

- ANYLINE established a certified information security management system in accordance with ISO/IEC 27001:2013 (ISO 27001 4 – 10)
- A clear set of roles and responsibilities in the area of information security and privacy are defined (ISO 27001 A.6.1.1, A.6.1.2)
- ANYLINE established and monitors and internal set of information security related KPIs (ISO 27001 9.1)
- An organisation wide set of policies for information security and privacy is defined and communicated within ANYLINE

Informationssicherheit und den Datenschutz ist definiert und innerhalb der Organisation kommuniziert (ISO 27001 A.5.1.1, A.5.1.2)

- ANYLINE hat die anwendbaren gesetzlichen und vertraglichen Anforderungen in Bezug auf Informationssicherheit und Datenschutz ermittelt (ISO 27001 A.18.1.1, A.18.1.2, A.18.1.4, A.18.1.5)
- ANYLINE hat relevante Aufzeichnungen zur Erfüllung geltender Compliance-Anforderungen bestimmt, dokumentiert, aktualisiert und schützt diese, um Rechenschaftspflichten im Bereich Datenschutz- und Informationssicherheit nachzuweisen (ISO 27001 A.18.1.1, A.18.1.3)

Maßnahmen zur Ermöglichung der Datenübertragbarkeit und zur Gewährleistung der Löschung

- ANYLINE hat Anforderungen und Verfahren für die sichere Entsorgung von Informationen und unterstützenden Assets festgelegt (ISO 27001 A.8.3.2, A.11.2.7)

Bei Datenübermittlungen an (Unter-)Auftragsverarbeiter sind auch die spezifischen technischen und organisatorischen Maßnahmen zu beschreiben, die der (Unter-)Auftragsverarbeiter zur Unterstützung des Verantwortlichen ergreifen muss:

- (Unter)-Auftragsverarbeiter, die personenbezogene Daten durch ANYLINE erhalten, sind zum Nachweis verpflichtet, dass sie über technische und organisatorische Sicherheitskontrollen verfügen, die zumindest in einem identen Sicherheits- und Datenschutzniveau resultieren, wie die oben angeführten Schutzmaßnahmen
- Darüber hinaus müssen alle (Unter-)Verarbeiter über definierte und Verfahren verfügen, um ANYLINE bei der effektiven Erfüllung aller Auftragsverarbeiter-Pflichten gemäß Art 28 DSGVO zu unterstützen

(ISO 27001 A.5.1.1, A.5.1.2)

- ANYLINE identified applicable legal and contractual requirements related to information security and privacy (ISO 27001 A.18.1.1, A.18.1.2, A.18.1.4, A.18.1.5)
- ANYLINE identified, documented, regularly updates and protects relevant compliance records to demonstrate accountability with applicable privacy and security regulations (ISO 27001 A.18.1.1, A.18.1.3)

Measures for allowing data portability and ensuring erasure

- ANYLINE defined requirements and procedures for the secure disposal of assets (ISO 27001 A.8.3.2, A.11.2.7)

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller:

- (Sub)-Processors receiving personal data from ANYLINE must provide proof for having technical and organisational security controls in place, which result in at least the same level of security and privacy as the controls listed above.
- In addition, all (sub)-processors must have defined processes for supporting ANYLINE in the fulfilment of its responsibilities as a processor of personal data outlined in Art 28 GDPR.