Security Policy

vom 27.04.2018

1 Technische und organisatorische Sicherheitsmaßnahmen

Axess verpflichtet sich bzw. in seinem Vertrag mit dem von Axess beauftragten externen Rechenzentrum den besonderen Anforderungen des Datenschutzes gerecht zu werden. Sowohl das interne als auch das externe Rechenzentrum befindet sich in Österreich. In diesem Zusammenhang bemüht sich die Axess stets, alle Maßnahmen zu treffen, die für die Verarbeitung der überlassenen Daten auf den Datenverarbeitungsanlagen nach der DSGVO für die Durchführung des Auftrags erforderlich sind sowie die innerbetriebliche Organisation so zu gestalten, dass den Anforderungen des Datenschutzes entsprochen wird.

Es wird sichergestellt, dass Sicherheitsbereiche und der Kreis befugter Personen bzw. Zutrittsberechtigungen festgelegt, Zugangswege entsprechend abgesichert sowie Datenträger kontrolliert und gesichert aufbewahrt werden.

Dabei handelt es sich derzeit insbesondere um die folgenden erforderlichen Maßnahmen:

1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, mit denen Daten verarbeitet oder genutzt werden, verwehrt. Die Serverräume befinden sich in einem als erdbebensicher eingestuften Bürogebäude eines Mischgebietes. Die Zutrittskontrolle – nur Mitarbeiter der IT, Facility und Geschäftsführung – wird durch ein folgende Maßnahmen gewährleistet.

> Berechtigung-/Chipkarte

Die Anwesenheit im Sicherheitsbereich wird aufgezeichnet. Nicht autorisiertes Personal und unternehmensfremde Personen (Servicetechniker, Berater, Reinigungskräfte, etc.) dürfen die Räume nur in Begleitung autorisierter Personen betreten. Die Zutrittskontrolle wird durch folgende weitere organisatorische/technische Maßnahmen unterstützt:

> Alarmanlage
> Gebäudeüberwachung
> Videotechnik

1.2 Zugangskontrolle

Eine Nutzung der Datenverarbeitungssysteme durch Unbefugte wird durch folgende Maßnahme verhindert:

> Passwort

Jeder Berechtigte verfügt über ein eigenes, nur ihm bekanntes Passwort, das in regelmäßigen Abständen gewechselt werden muss. Über sämtliche Aktivitäten auf der Datenverarbeitungs- und Telekommunikationsanlage werden automatische Protokolle (Logfiles) erstellt. Die Nutzung von Datenverarbeitungssystemen mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert:

> VPN (Virtual Private Network)

1.3 Zugriffskontrolle

Es ist gewährleistet, dass die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen ausschließlich auf ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Daten bei der Verarbeitung, Nutzung sowie der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Einschränkung der Zugriffsmöglichkeit des Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird durch folgende Maßnahmen gewährleistet:

> Automatische Prüfung der Zugriffsberechtigung (im System)

1.4 Verwendungszweckkontrolle

Es ist durch die folgenden Maßnahmen gewährleistet, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

> Software- basiert (z.B. Mandantentrennung)
> Trennung über Zugriffsregelung (Datenbankprinzip)
> Trennung von Test- und Aktualdaten
> Trennung von Test- und Aktualsystemen (Technik, Programme)

1.5 Pseudonymisierung

Sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und gesondert aufbewahrt.

1.6 Weitergabekontrolle

Es ist gewährleistet, 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, und dass überprüft und festgestellt werden kann, an welche Stelle eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. Der Versand von Datenträgern wird durch Registrierung und Begleitzettel dokumentiert und kontrolliert. das Mitbringen und die Nutzung privater Datenträger sind untersagt. Datenträger werden in folgender Weise vernichtet:

> Magnetische Datenträger durch Überschreiben und physikalische Zerstörung (externer Dienstleister)

Soweit das Internet zur Weitergabe personenbezogener Daten genutzt wird, werden folgende Sicherheitsmaßnahmen genutzt:

> Firewall
> Virtual Privat Network (VPN)

1.7 Eingabekontrolle

Es ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dazu wird der Auftragnehmer Eingaben dokumentieren bzw. protokollieren.

1.8 Verfügbarkeitskontrolle

Es ist durch die folgenden Maßnahmen gewährleistet, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Tägliche/wöchentliche/monatliche/jährliche Datensicherung
- Storage Areal Network (SAN)
- Plattenspiegelung (RAID u.a.)
- Unterbrechungsfreie Stromversorgung (USV)
- Überspannungsfilter
- Notstromaggregate
- Auslagerung von Daten
- Brandschutzvorrichtungen

1.9 Datenschutz-Management

Es wird sichergestellt, dass ein Datenschutz-Management eingerichtet und umgesetzt ist. Das Datenschutz-Management gliedert sich in folgende Punkte auf:

- Verarbeitungsverzeichnis
- Auftragsdatenverarbeitung
- Datenschutz-Folgenabschätzung
- Incident-Response-Management (Vorfallreaktionsplan)
- Meldung von Datenschutzverstößen
- Schulungen
- PDCA (Plan, Do, Check, Act): regelmäßige Überprüfungen

1.10 Incident-Response-Management

Es wurden Maßnahmen ergriffen, wie die zuständigen Personen auf potenzielle Szenarios reagieren soll. Dazu gehören Datensicherheitsverletzungen, DoS (Denial of Service), DDoS (Distributed Denial of Service), Lücken in der Firewall, Ausbrüche von Viren oder Malware und auch Bedrohungen durch Insider.

Der Vorfallreaktionsplan teilt sich in sechs wichtige Phasen auf:

- **Vorbereitung**: Sowohl die Anwender als auch die IT-Mitarbeiter werden geschult oder in Kenntnis gesetzt, dass potenzielle Vorfälle passieren und welche Schritte eingeleitet werden müssen.
- **Identifikation**: Bestimmung, ob es sich bei einem Ereignis tatsächlich um einen Datenschutzvorfall handelt.
- **Eindämmung**: Den durch den Vorfall verursachten Schaden begrenzen und die betroffenen Systeme isolieren, um weiteren Schaden zu vermeiden.
- **Ausmerzung**: Die Ursache oder den Auslöser des Vorfalls finden und die betroffenen Systeme aus der produktiven Umgebung entfernen.
- **Wiederherstellung**: Betroffene Systeme wieder in die produktive Umgebung integrieren, nachdem sichergestellt ist, dass keine weiteren Bedrohungen bestehen.
- **Gewonnene Erkenntnisse:** Vervollständigung der Vorfalldokumentation und Analyse, was das Team oder das Unternehmen aus dem Vorfall lernen kann. Auf diese Weise lassen sich künftige Reaktionen unter Umständen verbessern.

1.11 Privacy by Design & Privacy by Default

Es ist gewährleistet, dass geeignete technische und organisatorische Maßnahmen getroffen wurden, die sicherstellen, dass durch entsprechende Voreinstellungen grundsätzlich nur personenbezogene Daten verarbeitet werden, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist.

- Personenbezogene Daten werden erst dann erhoben, wenn sie für die Vertragsabwicklung erforderlich sind (Saisonkarten, etc.)
- Das Setzten von Cookies in Webshops ist nur mit Zustimmung des Nutzers möglich
- Die Verwendung der personenbezogenen Daten für Marketingzwecke ist nur durch aktive Zustimmung des Benutzers erlaubt

1.12 Auftragskontrolle

Es ist gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden. Es existieren Verträge für folgende Arten der Auftragsdatenverarbeitung:

- Datenverarbeitung durch Externe
- Datenträger-Vernichtung / Entsorgung durch Externe
- Wartung und Fernwartung durch Externe
- Administration / Fernadministration durch Externe

Die Verarbeitung personenbezogener Daten im Auftrag - nur entsprechend den Weisungen des Auftraggebers - wird durch folgende Maßnahmen gewährleistet.

- Schriftliche Weisungen
- Angebot und Auftragsbestätigung
- Pseudonymisierung

1.13 Sub-Auftragsverarbeiter

- CN Group CZ s.r.o.
- Agentur LOOP New Media GmbH
- DI Scheidl Alexander