Security Policy

1. Präambel

Gegenstand, Umfang, Art und Zweck der Datenverarbeitung ergeben sich aus der Geschäftsbeziehung auf der Grundlage des zwischen den Parteien geschlossenen Kaufvertrages und ersetzen alle diesbezüglichen früheren Vereinbarungen. Diese Sicherheitsmaßnahmen ergänzen den zwischen dem Kunden und Axess geschlossenen Kaufvertrag, soweit er sich auf die Verarbeitung von Kundendaten bezieht, und gelten als dessen Bestandteil. Axess gewährleistet die folgenden IT-Sicherheitsmaßnahmen im Rahmen der Kundenbeziehung.

2. Allgemeine technische und organisatorische Maßnahmen

Axess ergreift stets alle für die Verarbeitung der übermittelten Daten in den Datenverarbeitungssystemen erforderlichen Maßnahmen in Übereinstimmung mit der GDPR und gewährleistet, dass die interne Organisation so gestaltet ist, dass sie den Anforderungen des Datenschutzes entspricht. Die folgenden Bestimmungen gelten unabhängig davon, wo der Server gehostet wird.

2.1 Kontrolle des Verwendungszwecks:

Durch die folgenden Maßnahmen wird sichergestellt, dass die für unterschiedliche Zwecke erhobenen Daten getrennt verarbeitet werden:

> Softwarebasiert (z.B. Kundentrennung)
> Trennung durch Zugriffsregelung (Datenbankprinzip)
> Trennung von Test- und aktuellen Daten
> Trennung von Test- und laufenden Systemen (Technik, Programme)

2.2 Pseudonymisierung

Soweit für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenanwendung entfernt und separat gespeichert.

2.3 Eingabekontrolle:

Es ist gewährleistet, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder aus diesen entfernt werden. Axess wird zu diesem Zweck Eingaben/Logfiles dokumentieren bzw. aufzeichnen.

2.4 Privacy by Design & Privacy by Default

Durch entsprechende Voreinstellungen im Rahmen der technischen und organisatorischen Maßnahmen ist sichergestellt, dass grundsätzlich nur solche personenbezogenen Daten verarbeitet werden, deren Verarbeitung für den jeweils angegebenen Verarbeitungszweck erforderlich ist.

> Personenbezogene Daten werden nur dann erhoben, wenn sie für die Abwicklung des Kaufvertrages (z.B. Dauerkarten, etc.) notwendig sind.
> Das Setzen von Cookies in Axess Webshops ist nur mit Zustimmung des Nutzers möglich
> Die Nutzung der personenbezogenen Daten zu Marketingzwecken ist nur mit aktiver Zustimmung des Nutzers zulässig

3 Technische und organisatorische Maßnahmen bei Server-Hosting durch Axess

Wird im Rahmen des Kaufvertrages die Leistung des DATA CENTER SERVICE bezogen, so ist sichergestellt, dass Sicherheitsbereiche und der Kreis befugter Personen bzw. Zutrittsberechtigungen festgelegt, Zugangswege entsprechend abgesichert, sowie Datenträger kontrolliert und gesichert aufbewahrt werden. Die folgenden Maßnahmen gelten nur, wenn der Server von Axess gehostet wird.

3.1 Zutrittskontrolle:

Unbefugten ist der Zutritt zu Datenverarbeitungsanlagen, in denen Daten verarbeitet werden untersagt. Die Rechnerräume befinden sich in einem Bürogebäude, das als erdbebensicher eingestuft ist. Nur Mitarbeiter der IT, Facility und der Geschäftsleitung haben Zugang zu den Räumlichkeiten. Die Zutrittskontrolle wird durch die folgende Maßnahme gewährleistet:

> Berechtigung-/Chipkarte

Die Anwesenheit in der Sicherheitszone wird registriert. Nicht autorisiertes Personal und betriebsfremde Personen (Servicetechniker, Berater, Reinigungspersonal, etc.) dürfen die Räume nur in Begleitung von autorisierten Personen betreten. Die Zutrittskontrolle wird durch folgende weitere organisatorische/technische Maßnahmen unterstützt:

> Alarmanlage
> Gebäudeüberwachung
> Videotechnik

3.2 Zugangskontrolle:

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

> Passwort

Jede berechtigte Person hat ein eigenes, nur ihr bekanntes Passwort, das in regelmäßigen Abständen geändert werden muss. Über alle Aktivitäten an der Datenverarbeitungs- und Telekommunikationsanlage werden automatische Protokolle (Logfiles) erstellt. Die Nutzung von Datenverarbeitungssystemen mit Hilfe von Geräten zur Datenübertragung durch Unbefugte wird durch folgende Maßnahmen verhindert:

> VPN (Virtuelles Privates Netzwerk)

3.3 Zugriffskontrolle:

Es wird sichergestellt, dass die zur Nutzung einer Datenverarbeitungsanlage berechtigten Personen ausschließlich auf ihre zugriffsberechtigten Daten zugreifen können und dass Daten während der Verarbeitung, Nutzung sowie Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Beschränkung der Zugriffsmöglichkeit des Berechtigten auf die ausschließlich seiner Zugriffsberechtigung unterliegenden Daten wird durch folgende Maßnahmen gewährleistet:

> Automatische Überprüfung der Zugriffsberechtigung (im System)

3.4 Übermittlungskontrolle:

Es ist gewährleistet, dass personenbezogene Daten bei der elektronischen Übermittlung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, zu welchem Zeitpunkt eine Übermittlung personenbezogener Daten durch Geräte zur Datenübermittlung vorgesehen ist. Der Versand von Datenträgern wird durch Anmelde- und Begleitpapiere dokumentiert und kontrolliert. Es ist nicht gestattet, private Datenträger in die Räume mitzubringen und zu nutzen. Datenträger werden auf folgende Weise vernichtet:

> Magnetische Datenträger durch Überschreiben und physische Vernichtung (externer Dienstleister)

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

> Firewall
> Virtuelles Privates Netzwerk (VPN)

3.5 Verfügbarkeitskontrolle:

Durch folgende Maßnahmen wird sichergestellt, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind:

> Tägliche/wöchentliche/monatliche/jährliche Datensicherung
> Speicherbereichsnetzwerk (SAN)
> Plattenspiegelung (RAID u.a.)
> Unterbrechungsfreie Stromversorgung (USV)
> Überspannungsfilter
> Notstromaggregat
> Auslagerung von Daten
> Feuerschutzeinrichtungen

3.6 Datenschutzmanagement

Es ist sichergestellt, dass ein Datenschutzmanagement eingerichtet und umgesetzt wird. Das Datenschutzmanagement gliedert sich in die folgenden Punkte:

> Verzeichnis der Verarbeitungstätigkeiten
> Auftragsdatenverarbeitung
> Datenschutz-Folgenabschätzung
> Management der Reaktion auf Vorfälle
> Meldung von Datenschutzverstößen
> Fortbildungen
> PDCA (Plan, Do, Check, Act): regelmäßige Kontrollen

3.7 Vorfall-Management

Es wurden Maßnahmen getroffen, wie die Verantwortlichen auf mögliche Szenarien reagieren sollen. Dazu gehören Datensicherheitsverletzungen, DoS (Denial of Service), DDoS (Distributed Denial of Service), Lücken in der Firewall, Ausbrüche von Viren oder Malware und Bedrohungen durch Insider. Das Incident Response Management gliedert sich in sechs wichtige Phasen:

> Vorbereitung: Sowohl die Benutzer als auch die IT-Mitarbeiter werden geschult oder darüber informiert, dass potenzielle Vorfälle auftreten und welche Schritte eingeleitet werden müssen.
> Identifizierung: Feststellung, ob es sich bei einem Ereignis um einen Datenschutzvorfall handelt.
> Eingrenzung: Begrenzung der durch den Vorfall verursachten Schäden und Isolierung der betroffenen Systeme, um weitere Schäden zu vermeiden.
> Beseitigung: Ermitteln der Ursache oder des Auslösers des Vorfalls und Entfernen der betroffenen Systeme aus der Produktivumgebung.
> Wiederherstellung: Betroffene Systeme wieder in die produktive Umgebung zu integrieren, nachdem sichergestellt wurde, dass keine weiteren Bedrohungen bestehen.
> Erkenntnisse: Vervollständigung der Vorfallsdokumentation und Analyse, was das Team oder das Unternehmen aus dem Vorfall lernen kann. Auf diese Weise können künftige Reaktionen unter Umständen verbessert werden.

4 Zugriff auf Kundendaten

Um bei Problemen angemessenen Support leisten zu können, behält sich Axess als Datenverarbeiter das Recht vor, auf das System oder die Daten des Kunden zuzugreifen, sofern ein solcher Zugriff durch den Kaufvertrag zwischen Axess und dem Kunden abgedeckt ist oder der Kunde einem solchen Zugriff zugestimmt hat, oder der Reseller den gewünschten Serviceantrag im Namen des Kunden an Axess weitergeleitet hat.
Axess garantiert, dass:

> ein physischer Zugriff auf die Hardware des Rechenzentrums nur erfolgt, wenn der Kunde den Data Center Service von Axess bezieht;
> der Zugriff auf die Daten des Kunden über das Fernwartungstool nur

Security Policy

in dem oben beschriebenen Fall und mit Zustimmung oder im Auftrag des Resellers und/oder des Kunden erfolgt;
> Zugriff auf die lokalen Geräte wird nur im Supportfall auf Anfrage des Kunden oder des Resellers gewährt.

5 Auftragsverarbeitung:
Ergänzend zur vorliegenden Geschäftsbeziehung stellen diese Bestimmungen zur Auftragsverarbeitung sicher, dass alle gegenseitigen Verpflichtungen gemäß der Allgemeinen Datenschutzverordnung ("GDPR") erfüllt werden.

Axess verarbeitet personenbezogene Daten im Auftrag des Kunden, wobei sich Gegenstand, Umfang, Art, Kategorien der verarbeiteten Daten, der Zweck der Verarbeitung sowie die Kategorien der betroffenen Personen (Kundendaten) aus dem jeweiligen Kaufvertrag zwischen den Vertragsparteien ergeben. Diese Bestimmungen zur Auftragsverarbeitung ergänzen daher alle zwischen dem Kunden und Axess geschlossenen Verträge, soweit sie sich auf die Verarbeitung personenbezogener Daten beziehen.

Die Datenverarbeitung durch Axess erfolgt ausschließlich in einem Mitgliedstaat der Europäischen Union, wobei grenzüberschreitende Datenverarbeitungen gemäß Art. 4 Z 23 DSGVO (innerhalb der Union) dem Auftraggeber als Verantwortlichem rechtzeitig vor Beginn der Verarbeitung mitzuteilen sind, damit der Auftraggeber widersprechen kann. Das Schweigen auf diese Mitteilung bedeutet die Einwilligung in die Verarbeitung.

5.1 Pflichten des Auftragsverarbeiters:
Mit der Unterzeichnung des Kaufvertrags erklärt sich der Kunde mit den technischen und organisatorischen Maßnahmen einverstanden, die in dieser Richtlinie festgelegt sind. Durch die Umsetzung dieser Policy und die Befolgung der allgemeinen und individuellen Weisungen des Kunden in Bezug auf personenbezogene Daten (z.B. Löschung von Kundendaten, Anonymisierung von Daten) gewährleistet Axess ein dem Stand der Technik entsprechendes Schutzniveau der vertraglichen Datenanwendungen, so dass Ansprüche jeglicher Art nur im Falle einer Verletzung geltend gemacht werden können.

Änderungen der technischen und organisatorischen Maßnahmen, die ein gleichbleibendes Schutzniveau für die verarbeiteten personenbezogenen Daten gewährleisten oder dieses erhöhen, gelten als genehmigt und werden dem Kunden auf Verlangen mitgeteilt, müssen aber von Axess dem Kunden nicht mitgeteilt werden.

Axess ergreift die oben beschriebenen technischen und organisatorischen Maßnahmen, damit der Kunde die Rechte der betroffenen Personen nach Kapitel III der DSGVO (Auskunft, Zugang, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen wahrnehmen kann.

5.2 Datenverarbeitung
Axess verpflichtet sich, personenbezogene Daten nur im Rahmen bestehender Verträge und nach den individuellen Weisungen des Kunden zu verarbeiten. Soweit Axess gesetzlich verpflichtet ist, die Daten an Dritte herauszugeben, wird Axess den Kunden über die gesetzliche Verpflichtung zur Herausgabe der Daten informieren. Die sonstige Weitergabe von Daten zu Zwecken außerhalb des Vertragsverhältnisses erfolgt nur auf Weisung des Kunden auf der Grundlage eines schriftlichen Auftrags.

Axess stellt sicher, dass alle mit der Datenverarbeitung betrauten Personen vor Aufnahme ihrer Tätigkeit - und auch nach Beendigung ihrer Tätigkeit - auf das Datengeheimnis verpflichtet werden oder einer entsprechenden gesetzlichen Verschwiegenheitspflicht unterliegen.

5.3 Informationspflicht
Axess unterstützt den Auftraggeber bei der Erfüllung der in Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgenabschätzung, vorherige Konsultation).

Auf Anfrage stellt Axess dem Auftraggeber alle erforderlichen Informationen zur Verfügung (z. B. bestehende Zertifizierungen, technische und organisatorische Maßnahmen usw.), um die Einhaltung der in Artikel 28 DSGVO genannten Pflichten (Pflichten des Auftragsverarbeiters) nachzuweisen. Darüber hinaus ermöglicht Axess die Durchführung von Audits - einschließlich Inspektionen - durch den Auftraggeber oder einen anderen vom Auftraggeber beauftragten Prüfer und trägt dazu bei.

Axess wird den Auftraggeber unverzüglich informieren, wenn ein Verstoß gegen die DSGVO vorliegt oder wenn Axess der Ansicht ist, dass eine Weisung des Auftraggebers gegen die Datenschutzbestimmungen der Union oder der Mitgliedstaaten verstößt.

5.4 Auftragsverarbeitungskontrolle
Es wird sichergestellt, dass personenbezogene Daten, die im Auftrag des Auftraggebers verarbeitet werden, nur nach dessen Weisung verarbeitet werden. Axess unterhält Verträge mit externen Parteien für die folgenden Arten der Auftragsdatenverarbeitung:
> Datenverarbeitung durch Externe
> Datenträgervernichtung / Entsorgung durch Externe
> Wartung und Fernwartung durch Externe
> Administration / Fernadministration durch Externe

Die Verarbeitung personenbezogener Daten im Auftrag des Auftraggebers - nur nach dessen Weisung - wird durch folgende Maßnahmen gewährleistet.
> Schriftliche Weisungen
> Angebots- und Auftragsbestätigung
> Pseudonymisierung

5.5 Unterauftragsverarbeiter
Axess ist berechtigt, Unterauftragsverarbeiter für die Verarbeitung von personenbezogenen Daten einzusetzen. Beabsichtigte Änderungen in Bezug auf den Unterauftragsverarbeiter sind dem Auftraggeber so rechtzeitig schriftlich mitzuteilen, dass der Auftraggeber der Änderung widersprechen kann. Ausgenommen von dieser Regelung sind Situationen, in denen eine Benachrichtigung nicht möglich oder durchführbar ist (insbesondere bei Gefahr im Verzug). Axess schließt mit den Unterauftragsverarbeitern einen schriftlichen Vertrag ab und vereinbart mit ihnen mutatis mutandis die gleichen datenschutzrechtlichen Verpflichtungen wie in diesem Kapitel dargestellt.
Folgende Unterauftragsverarbeiter werden von Axess beauftragt:
> CN Group CZ s.r.o.
> Agentur LOOP New Media GmbH
> conova communications GmbH
> SOTI Ireland Limited
> ilogs information logistics GmbH

Im Falle eines Kaufvertrages mit einem offiziellen Reseller von Axess, liefert Axess Daten nur an den respektiven Vertragspartner (Partner oder Reseller).

6 Beendigung des Vertrages
Bei Beendigung der zugrundeliegenden Geschäftsbeziehung gibt Axess dem Kunden alle personenbezogenen Daten in einem für die Datenverarbeitung üblichen Format zurück oder löscht sie, es sei denn, es besteht eine Verpflichtung zur Aufbewahrung der personenbezogenen Daten nach Unionsrecht oder dem Recht eines Mitgliedstaats.

7 Schlussbestimmungen
Das Sicherheitskonzept hat die gleiche Laufzeit wie die Geschäftsbeziehung zwischen Axess und dem Kunden. Deren Schlussbestimmungen gelten entsprechend für den Auftragsverarbeitungsvertrag.