Politica di sicurezza

1 Premessa

Oggetto, entità, tipo e scopo del trattamento dei dati si evincono dal rapporto commerciale sulla base del contratto di vendita concluso tra le parti e sostituiscono tutti gli accordi presi in precedenza in merito. Le presenti misure di sicurezza integrano il contratto di vendita concluso tra il cliente e Axess, se riferito al trattamento dei dati dei clienti e si applicano come parte integrante dello stesso. Axess garantisce le seguenti misure di sicurezza informatica nell'ambito del rapporto con il cliente.

2 Misure tecniche e organizzative generali

Axess ha costantemente accesso alle misure necessarie per il trattamento dei dati trasmessi nei sistemi di trattamento dei dati, in conformità al GDPR, e garantisce che l'organizzazione interna venga strutturata in modo da soddisfare i requisiti di protezione dei dati. Le seguenti disposizioni si applicano indipendentemente da dove sia ospitato il server.

2.1 Controllo della destinazione d'uso

Le seguenti misure garantiscono che i dati raccolti possano essere trattati a parte per scopi differenti:

> software-based (es. separazione dei clienti)
> separazione tramite controllo di accesso (principio della banca dati)
> separazione di dati di prova e attuali
> separazione di sistemi di prova e attuali (tecnica, programmi)

2.2 Pseudonimizzazione

Laddove possibile per il rispettivo trattamento dei dati, gli identificatori primari dei dati personali vengono rimossi nella rispettiva applicazione dei dati e salvati a parte.

2.3 Controllo di immissione

Si garantisce che sia possibile verificare e stabilire a posteriori se i dati personali siano stati immessi, modificati o rimossi e da chi nei sistemi di trattamento dei dati. Axess documenterà o registrerà dati/file di log a tale scopo.

2.4 Privacy by Design & Privacy by Default

Le rispettive preimpostazioni nell'ambito delle misure tecniche e organizzative garantiscono che vengano sostanzialmente trattati solo quei dati personali il cui trattamento sia necessario per la destinazione d'uso rispettivamente indicata.

> I dati personali vengono raccolti solo se necessari ai fini dell'esecuzione del contratto di vendita (es. abbonamenti, ecc.).
> L'impiego dei cookie nei webshop Axess è possibile solo con il consenso dell'utente.
> L'uso di dati personali a scopi di marketing è ammesso solo dietro consenso attivo dell'utente.

3 Misure tecniche e organizzative per hosting del server da parte di Axess

Se, nell'ambito del contratto di vendita, la prestazione del SERVIZIO DATA CENTER viene acquistata nell'ambito del contratto di vendita, si garantisce la definizione delle aree di sicurezza e della cerchia di persone autorizzate o delle autorizzazioni all'accesso, si assicurano le vie di accesso e i supporti dati vengono controllati e archiviati in modo sicuro. Le seguenti misure si applicano solo se il server è ospitato da Axess.

3.1 Controllo di accesso

Ai non autorizzati è vietato l'accesso ai sistemi di trattamenti dei dati in cui i dati vengono elaborati. Le sale di calcolo si trovano in un edificio di uffici classificato come antisismico. Solo i dipendenti dell'ufficio informatico, facility e management hanno accesso ai locali. Il controllo degli accessi fisici è garantito dalle seguenti misure:

> scheda di autorizzazione/chip card

La presenza viene registrata nella zona di sicurezza. Il personale non autorizzato e i non dipendenti (tecnici dell'assistenza, consulenti, personale addetto alle pulizie, ecc.) possono entrare nei locali solo accompagnati da persone autorizzate. Il controllo degli accessi fisici è supportato dalle seguenti misure tecniche/organizzative:

> impianto di allarme
> monitoraggio dell'edificio
> tecnologia video

3.2 Controllo degli accessi

Un uso dei sistemi di trattamento dei dati da parte di soggetti non autorizzati è impedito dalle seguenti misure:

> Password

Ogni persona autorizzata ha una propria password, nota solo a lei, che va modificata a intervalli regolari. Per tutte le attività dell'impianto di trattamento dei dati e telecomunicazione vengono creati protocolli automatici (file di log). L'uso dei sistemi di trattamento dei dati con l'ausilio di dispositivi per il trattamento dei dati da parte di soggetti non autorizzati è impedito dalle seguenti misure:

> VPN (rete privata virtuale)

3.3 Controllo degli accessi

Si garantisce che le persone autorizzate all'uso di un sistema di trattamento dei dati possano accedere esclusivamente ai propri dati autorizzati e i dati non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante il trattamento, l'uso e il salvataggio. Le seguenti misure garantiscono che la possibilità di accesso della persona autorizzata sia limitata ai dati soggetti esclusivamente alla sua autorizzazione all'accesso:

> verifica automatica dell'autorizzazione all'accesso (nel sistema)

3.4 Controllo di trasmissione

Si garantisce che i dati personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione durante la trasmissione elettronica, il trasporto o il salvataggio su supporti di dati e che sia possibile stabilire in che momento sia prevista una trasmissione dei dati personali tramite appositi dispositivi. La spedizione di supporti di dati è documentata e controllata mediante documenti di registrazione e accompagnamento. Non è ammesso portare supporti di dati privati nei locali e utilizzarli. I supporti di dati vengono distrutti come segue:

> supporti di dati magnetici mediante sovrascrittura e distruzione fisica (fornitore di servizi esterno)

se ci si avvale di internet per la trasmissione dei dati personali, vengono impiegate le seguenti misure di sicurezza:

> Firewall
> Rete Privata Virtuale (VPN)

3.5 Controllo della disponibilità

Le seguenti misure garantiscono che i dati raccolti possano essere protetti dalla distruzione accidentale e dalla perdita:

> backup quotidiano/settimanale/mensile/annuale dei dati
> Storage Area Network (SAN)
> mirroring del disco (RAID ecc.)
> gruppo di continuità (UPS)
> filtro contro le sovratensioni
> generatore di emergenza
> esternalizzazione dei dati
> dispositivi antincendio

3.6 Gestione della protezione dei dati

Si garantisce che venga impostata e implementata una gestione della protezione dei dati. La gestione della protezione dei dati si suddivide nei seguenti punti:

> elenco delle attività di trattamento
> trattamento dei dati
> valutazione dell'impatto sulla protezione dei dati
> gestione della risposta agli incidenti
> segnalazione di violazioni della protezione dei dati
> corsi di perfezionamento
> PDCA (Plan, Do, Check, Act): controlli regolari

3.7 Gestione degli incidenti

Sono state adottate misure su come i responsabili dovrebbero reagire a possibili scenari. Queste includono violazioni della sicurezza dei dati, DoS (Denial of Service), DDoS (Distributed Denial of Service), violazioni dei firewall, focolai di virus o malware e minacce interne.
L'Incident Response Management si suddivide in sei fasi importanti:

> Preparazione: sia gli utenti che i collaboratori informatici vengono formati o informati su potenziali incidenti che potrebbero verificarsi e sulle misure da adottare.
> Identificazione: si stabilisce se un evento sia un incidente relativo alla protezione dei dati.
> Contenimento: limitare i danni causati dall'incidente e isolare i sistemi interessati per prevenire ulteriori danni.
> Rimedio: determinazione della causa o dell'innesco dell'incidente e rimozione dei sistemi interessati dall'ambiente di produzione.
> Ripristino: riportare i sistemi interessati nell'ambiente di produzione dopo aver accertato che non esistono ulteriori minacce.
> Conoscenze acquisite: completare la documentazione dell'incidente e analizzare ciò che il team o l'organizzazione possono apprendere dall'incidente. Questo consente di migliorare eventuali risposte future in determinate circostanze.

4 Accesso ai dati dei clienti

Per poter fornire un supporto adeguato in caso di problemi, Axess si riserva il diritto, in qualità di responsabile del trattamento dei dati, di accedere al sistema o ai dati del cliente, se un tale accesso sia consentito dal contratto di vendita tra Axess e il cliente o se il cliente abbia acconsentito ad un simile accesso o se il rivenditore abbia inoltrato la domanda di assistenza a Axess in nome del cliente.
Axess garantisce che:

> un accesso fisico all'hardware del centro di calcolo avvenga solo quando il cliente acquista il Data center Service di Axess;
> l'accesso ai dati del cliente mediante lo strumento di manutenzione a distanza abbia luogo solo nel caso sopra descritto e in accordo o su incarico del rivenditore e/o del cliente;
> l'accesso ai dispositivi locali sia garantito solo in caso di supporto, su richiesta del cliente o del rivenditore.

5 Trattamento dei dati

A integrazione del presente rapporto commerciale, queste disposizioni sul trattamento dei dati assicura che tutti gli obblighi reciproci vengano soddisfatti in conformità al Regolamento generale sulla protezione dei dati ("GDPR").

Politica di sicurezza

Axess tratta i dati personali per conto del cliente, mentre l'oggetto, la portata, il tipo, le categorie di dati trattati, lo scopo del trattamento e le categorie di persone interessate (dati del cliente) risultano dal rispettivo contratto di vendita tra le parti contraenti. Le presenti disposizioni sul trattamento dei dati integrano pertanto tutti i contratti conclusi tra il cliente e Axess, se riferiti al trattamento dei dati personali.

Il trattamento dei dati da parte di Axess avviene esclusivamente in uno Stato membro dell'Unione Europea, per cui i trattamenti dei dati transfrontalieri ai sensi dell'articolo 4 Z 23 GDPR (all'interno dell'Unione) devono essere comunicati al cliente, in qualità di parte responsabile, in tempo utile prima dell'inizio del trattamento, in modo che il committente possa opporsi. Un'assenza di risposta a questa notifica significa un consenso al trattamento.

5.1 Obblighi del responsabile del trattamento
Con la sottoscrizione del contratto di vendita, il cliente accetta le misure tecniche e organizzative stabilite nella presente direttiva. Attuando questa politica e seguendo le istruzioni generali e individuali del cliente in merito ai dati personali (es. cancellazione dei dati del cliente, anonimizzazione dei dati), Axess garantisce un livello di protezione per le applicazioni dei dati contrattuali che corrisponde allo stato dell'arte, in modo che pretese di qualsiasi tipo possano essere accolte solo in caso di violazione.

Le modifiche delle misure tecniche e organizzative che garantiscono o aumentano un livello costante di protezione dei dati personali trattati si considerano approvate e vengono comunicate al cliente su richiesta, ma Axess non è tenuta a darne comunicazione al cliente.

Axess adotta le misure tecniche e organizzative sopra descritte affinché il cliente possa rispettare i diritti delle persone interessate ai sensi del capitolo III del GDPR (accesso, rettifica, cancellazione, limitazione, portabilità dei dati, opposizione e processi decisionali automatizzati in singoli casi) entro i termini di legge.

5.2 Trattamento dei dati
Axess si impegna a trattare i dati personali solo nell'ambito dei contratti esistenti e secondo le istruzioni individuali del cliente. Se Axess è obbligato per legge a cedere i dati a terzi, informerà il cliente in merito all'obbligo di legge sul rilascio dei dati. L'altro trasferimento di dati per scopi estranei al rapporto contrattuale avviene solo dietro istruzione del cliente, sulla base di un ordine scritto.

Axess garantisce che tutte le persone incaricate del trattamento dei dati saranno tenute a mantenere riserbo sui dati prima dell'inizio dell'attività (e anche al termine della stessa) o che saranno soggette a un relativo obbligo legale di segretezza.

5.3 Obbligo di informazione
Fornendo i dati, Axess supporta il committente nell'adempimento degli obblighi di cui all'art. da 32 a 36 del Regolamento generale sulla protezione dei dati (sicurezza del trattamento, notifica delle violazioni della protezione dei dati personali all'autorità di controllo, notifica della persona interessata da una violazione della protezione dei dati personali, valutazione d'impatto sulla protezione dei dati, consultazione preventiva).

Su richiesta, Axess mette a disposizione del committente tutte le informazioni necessarie (ad es. certificazioni esistenti, misure tecniche e organizzative, ecc.) per dimostrare il rispetto degli obblighi di cui all'art. 28 GDPR (obblighi del responsabile del trattamento). Inoltre, Axess consente e contribuisce all'esecuzione di audit (comprese le ispezioni) da parte del committente o di un altro auditor commissionato dal committente.

Axess informerà immediatamente il committente in caso di violazione del GDPR o se fosse del parere che un'istruzione impartita dal committente violi le disposizioni sulla protezione dei dati dell'Unione o degli Stati membri.

5.4 Controllo del trattamento
Si garantisce che i dati personali possono essere trattati solo su incarico del committente, in base alle sue istruzioni. Axess conclude contratti con le parti esterne per i seguenti tipi di trattamento dei dati:
> trattamento dei dati da parte di esterni
> distruzione del supporto dati / smaltimento da parte di esterni
> manutenzione e manutenzione a distanza da parte di esterni
> amministrazione / amministrazione a distanza da parte di esterni

Il trattamento dei dati personali su incarico del committente, in base alle sue istruzioni, è garantito dalle seguenti misure.
> Istruzioni scritte
> Conferma dell'offerta e dell'ordine
> Pseudonimizzazione

5.5 Subresponsabile del trattamento
Axess ha la facoltà di incaricare un sub-responsabile del trattamento dei dati personali. Le modifiche previste in merito al sub-responsabile del trattamento vanno comunicate al committente tempestivamente per iscritto, in modo che questi possa opporsi alla modifica. Sono escluse da questa disposizione le situazioni in cui una comunicazione non sia possibile o fattibile (soprattutto in caso di pericolo imminente). Axess conclude un contratto scritto con i sub-responsabili del trattamento e concorda con loro gli stessi obblighi di protezione dei dati descritti in questo capitolo.
I seguenti sub-responsabili del trattamento sono incaricati da Axess:
> CN Group CZ s.r.o.
> Agentur LOOP New Media GmbH
> conova communications GmbH
> SOTI Ireland Limited
> ilogs information logistics GmbH

Nel caso di un contratto di vendita con un rivenditore ufficiale di Axess, Axess consegna i dati solo al rispettivo partner contrattuale (partner o rivenditore).

6 Fine del contratto
Alla cessazione del rapporto commerciale, Axess fornisce al committente tutti i dati personali in un formato consueto per il trattamento dei dati oppure li elimina, salvo laddove sia presente un obbligo di conservazione dei dati personali ai sensi del diritto dell'Unione Europea o di uno Stato membro.

7 Disposizioni finali
Il concetto di sicurezza ha la medesima durata del rapporto commerciale tra Axess e il committente. Le loro disposizioni finali si applicano anche al contratto di trattamento dei dati.