ESA GPT – Trattamento dei dati ai sensi dell'art. 9 LPD

L'ESA – Organizzazione d'acquisto del settore svizzero dell'automobile e dei veicoli a motore società cooperativa (di seguito «mandatario») mette a disposizione del committente (di seguito «committente») il servizio ESA GPT – che comprende anche il trattamento dei dati personali e costituisce un responsabile del trattamento dei dati ai sensi dell'art. 9 LPD. Per l'utilizzo di ESA GPT, il presente Accordo per il trattamento dei dati (ATD) si applica in modo informale.
Versione 1.0 del 28.04.2025, la presente versione potrà essere sostituita da versioni future.

Categorie di persone interessate: Clienti, personale, partner commerciali del committente
Categorie di dati: Dati di contatto, dati di utilizzo e dati forniti dal committente
Trasferimento dati consentito (Paese): I dati vengono trattati in CH e nello SEE (DE, IRE, SWE)

Subresponsabili del trattamento autorizzati (nome, finalità): Microsoft Ireland Operations, hosting di Azure OpenAI (CH e SWE) e Statworx GmbH, partner di implementazione (DE)

Obblighi del mandatario

1. Il mandatario tratta i dati solo per le finalità e solo su istruzione documentata del committente (ad es. messa a disposizione di un ambiente IA); se li ritiene inammissibili, lo comunica al committente.

2. Il mandatario garantisce sempre un'adeguata sicurezza dei dati ai sensi del vigente diritto in materia di protezione dei dati e delle MTO. Segnala immediatamente qualsiasi violazione della sicurezza dei dati fornendo tutte le informazioni necessarie.

3. Il mandatario è tenuto a fare sì che tutto il personale ausiliario nonché le collaboratrici e i collaboratori mantengano la riservatezza, nella misura in cui non siano già tenuti a fare per legge.

4. Il mandatario si avvale di subresponsabili del trattamento solo previa autorizzazione (si veda sopra). Deve essere informato in merito a eventuali ulteriori subresponsabili del trattamento e, in assenza di opposizione entro 30 giorni, si intendono accettati. Anche tali subresponsabili sono tenuti al rispetto della protezione dei dati.

5. Il mandatario non esporta dati del committente senza la sua autorizzazione e, in tal caso, solo nel rispetto della legislazione vigente in materia di protezione dei dati.

6. All'occorrenza, il mandatario assiste il committente nel rispetto delle disposizioni in materia di protezione dei dati, in particolare per l'adempimento dei diritti delle persone interessate e per le valutazioni d'impatto sulla protezione dei dati.

7. Al termine della collaborazione, i dati vengono distrutti allo scadere dei termini di conservazione previsti dalla legge.

8. Il mandatario dimostra il rispetto del presente ATD e il committente ha la facoltà di verificarlo.

Sicurezza delle informazioni (MTO)

Di seguito le nostre misure tecniche e organizzative (MTO) per la sicurezza dei dati.

- Controllo degli ingressi e degli accessi
- Videosorveglianza magazzino merci e locale server
- UPS
- IAM
- Accesso ai dati solo con autenticazione
- MFA per tutti gli accessi
- Password forti
- Principio del privilegio minimo
- Principio del «need to know»
- Principio della «zero trust»
- Terminali codificati
- TLS enforced
- Test di penetrazione
- Audit esterni sulla sicurezza
- ISMS
- Backup
- Concetto BCM
- Firewall
- IDS
- EDR/XDR
- MDM
- Protezione contro i malware
- Gestione patch
- Separazione sistemi produttivi/altri sistemi
- Installazione controllata del software
- SOC
- Direttiva sulla sicurezza delle informazioni
- Security Awareness Training
- Registrazione di eventi rilevanti per la sicurezza

MTO dettagliate disponibili su richiesta