Allegato “Misure tecnico organizzative” ai sensi dell’art. 9 BDSG

Art. 1 Misure di sicurezza tecniche e organizzative

Ai sensi dell’art. 11 c. 2 cpv. 2 n. 3 BDSG e dell’art. 9 BDSG, le parti sono tenute a definire le misure di sicurezza tecniche e organizzative.

Art. 2 Organizzazione interna del commissionario

Il commissionario allestirà la sua organizzazione interna in modo da corrispondere ai particolari requisiti di tutela dei dati. In questo contesto devono essere attuate in particolare misure adeguate alla tipologia dei dati di natura personale o della categoria di dati da proteggere.

Art. 3 Specificazione delle misure concrete

N.	Misura	Attuazione della misura
1	Controllo all’ingresso Alle persone non autorizzate non deve essere concesso l’accesso agli impianti di elaborazione dei dati con cui vengono trattati o utilizzati i dati di natura personale.	• Definizione delle persone autorizzate • (Persone interne ed esterne all’azienda) • Regolamentazione dei chip d’accesso • Regolamentazione delle persone esterne all’azienda • Protezione anche al di fuori degli orari di lavoro con impianto dall’allarme • Protezione della porta (chiusura elettronica della porta, lettore documenti) • Formulazione adeguata delle misure per la protezione degli oggetti (ad es. sistema antieffrazione, sorveglianza dell’area)
2	Controllo dell’accesso fisico Deve essere evitato che i sistemi di elaborazione dei dati possano essere utilizzati da persone non autorizzate.	• Crittografia parziale • Assegnazione e protezione delle chiavi di identificazione (ID utente) • Gestione dei diritti utente • Vincolo alla segretezza dei dati ai sensi dell’art. 5 BDSG • Regolamentazione di accesso differenziata (ad es. con blocchi d’accesso per segmenti) • Verbalizzazione e analisi dell’utilizzo dei file
3	Controllo dell’accesso ai dati Deve essere assicurato che le persone autorizzate all’utilizzo del sistema di elaborazione dati abbiano accesso solo ai dati relativi alla loro autorizzazione e che nel corso dell’elaborazione, dell’utilizzo e dopo l’archiviazione i dati di natura personale non possano essere letti, copiati, modificati o rimossi senza autorizzazione.	• Crittografia • Gestione dei diritti d’accesso • Analisi dei protocolli • Possibilità di accesso parziale a basi di dati e funzioni

4	Controllo della trasmissione Deve essere assicurato che nel corso della trasmissione elettronica, durante il trasporto o l'archiviazione su supporti dati, i dati di natura personali non possano essere letti, copiati, modificati o rimossi senza autorizzazione e che sia possibile accertare dove è previsto l'inoltro dei dati di natura personale mediante impianti per il trasferimento dati.	• Crittografia • Definizione delle persone autorizzate • Ingresso del centro di calcolo protetto per fornitura e consegna • Consegna di supporti dati solo a persone autorizzate (ad es. ricevuta dell'incarico, documento d'accompagnamento) • Controllo dell'inventario gestione supporti dati • Chiusura separata dei supporti dati riservati • Armadi di sicurezza • Distruzione controllata dei supporti dati (ad es. stampe difettose) • Gestione della realizzazione di copie • Documentazione del richiamo dei programmi di trasmissione • Determinati utenti autorizzati • Disposizioni per l'imballaggio e la spedizione (tipo di spedizione ad es. in contenitori chiusi) • Ritiro diretto, servizio corriere, accompagnamento del trasporto • Cancellazione dei dati residui prima della sostituzione dei supporti dati
5	Controllo delle immissioni Deve essere assicurato che sia possibile eseguire un controllo successivo sull'immissione, la modifica e la rimozione dei dati di natura personale nei sistemi di elaborazione dati e sulle persone che hanno eseguito tali operazioni.	• Dimostrazione delle competenze organizzative definite per l'immissione • Verbalizzazione delle immissioni • Verbalizzazione dell'utilizzo dei file • Organizzazione dei processi, dei programmi e delle procedure • Vincolo alla segretezza dei dati
6	Controllo dell'incarico Deve essere assicurato che i dati di natura personale elaborati nell'ambito dell'incarico possano essere trattati solo in conformità alle istruzioni del committente.	• Rispetto dei contratti di elaborazione dei dati • Trasporto sicuro dei dati e dei supporti dati (di solito DHL) • Elaborazione sicura dei dati • Cancellazione sicura dei dati dopo il completamento dell'incarico • Processi interni per l'adempimento dell'incarico e monitoraggio dei processi • Processo standard di Change Management (secondo ITIL) • Misure per la protezione dei dati
7	Controllo della disponibilità Deve essere assicurato che i dati di natura personale siano protetti contro la distruzione o la perdita accidentale.	• Misure per la protezione dei dati (fisiche / logiche) • Backup • Procedure di salvataggio e archiviazione • Ripristino dell'infrastruttura (Desaster Recovery) • Protezione contro "malicious code"

8	Controllo della separazione Deve essere assicurato che i dati rilevati per scopi diversi siano trattati separatamente.	• Misure per l'elaborazione separata (archiviazione, modifica, cancellazione, trasmissione) di dati con scopi diversi. • Separazione dei mandati • Separazione delle funzioni • Separazione dei sistemi di test e di produzione