

Direttiva sulla sicurezza delle informazioni

1. Direttiva sulla sicurezza delle informazioni

Per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni e il rispetto di tutte le norme sulla protezione dei dati MediData SA ha istituito un apposito sistema di gestione. Ci impegnamo ad attuare e ad applicare i requisiti imposti dalle versioni in vigore della norma ISO 27001 e dall'OCPD (Ordinanza sulle certificazioni in materia di protezione dei dati) svizzera. MediData è certificata, quale organizzazione complessiva, ai sensi della norma ISO 27001 e dell'OCPD sin dal 2013 e intende mantenere tali certificazioni.

1.1 Finalità della sicurezza delle informazioni, della cybersecurity e della protezione dei dati

MediData SA ritiene assolutamente essenziale perseguire tali finalità sovraordinate nell'ambito della propria attività, in particolare nella sua veste di gestore di una piattaforma di scambio dati.

- Le informazioni e i dati, sia altrui che propri, devono essere protetti da accessi non autorizzati (riservatezza).
- Le informazioni e i dati devono essere protetti da manipolazioni sia volontarie che involontarie (integrità).
- La disponibilità dei prodotti e servizi deve corrispondere alle promesse fatte nelle relative descrizioni (disponibilità).
- Rispetto dei requisiti legali e contrattuali, con particolare riguardo per il rispetto delle norme sulla protezione dei dati.

Per il conseguimento di tali finalità devono essere applicate le seguenti regole:

- L'accesso ai locali di MediData deve essere regolamentato.
- Appliciamo il principio del need-to-know, secondo cui informazioni e funzioni sono disponibili solo ai dipendenti che hanno un incarico corrispondente.
- Le direttive e le istruzioni di lavoro devono essere rigorosamente osservate.
- Tutti i collaboratori devono essere obbligati a segnalare eventuali comportamenti contrari alle finalità suddette di cui vengano a conoscenza.

La direzione è consapevole del fatto che il rispetto delle regole rende alcune procedure di lavoro più complicate e quindi più costose.

1.2 Economicità

Le misure di conseguimento delle finalità devono essere adottate tenendo conto degli aspetti economici.

1.3 Ruoli e responsabilità

Quale supporto al sistema di gestione sono stati istituiti la mansione di «Chief Information Security Officer» (CISO) e il «Gruppo per la sicurezza integrale» (GSI). Blocchi di informazioni e corsi di formazione periodici garantiscono la necessaria consapevolezza di tutti i collaboratori e la diffusione del relativo know-how in tutta l'azienda. Le misure sono attuate seguendo l'organizzazione a linee. I responsabili dei reparti e dei team sono affiancati dal CISO.

1.4 Miglioramento continuo

La raccolta e la valutazione dei dati del sistema e del supporto forniscono informazioni importanti per il miglioramento dei nostri prodotti e servizi. MediData SA promuove e si impegna a favore di un processo di miglioramento continuo e sistematico.

1.5 Verifica del sistema di gestione

MediData verifica regolarmente l'efficacia e l'efficienza del sistema di gestione e fa confluire i risultati nel processo ai fini del miglioramento continuo. Eventuali violazioni delle direttive da parte dei collaboratori sono sanzionate con misure disciplinari.

1.6 Obbligo dei fornitori

I fornitori che possono entrare in contatto con informazioni soggette a protezione sono esplicitamente istruiti riguardo alle prescrizioni di MediData SA e obbligati per contratto ad applicare gli stessi standard rispetto alle informazioni. Con alcuni fornitori importanti selezionati è portata avanti una collaborazione intensiva per la verifica e il miglioramento dei processi.

2. Supporto all'attuazione del sistema di gestione

Con la presente la direzione di MediData SA dichiara che il sistema di gestione e il miglioramento continuo dello stesso sono supportati mediante risorse idonee, in modo da poter conseguire tutte le finalità indicate nella presente direttiva.

2.1 Rispetto degli obblighi

MediData SA mira a essere un'azienda affidabile per tutti i clienti, i partner e i fornitori e si impegna a rispettare tutte le norme di legge e gli accordi contrattuali.