Contenuti

Sicurezza dell'informazione e protezione dei dati

Campo di applicazione

I seguenti capitoli descrivono le misure tecniche e organizzative adottate da Trasfusione CRS Svizzera in materia di sicurezza dell'informazione e protezione dei dati personali. Si applicano a tutti i casi in cui Trasfusione CRS Svizzera stessa, in quanto responsabile, tratta i dati rilevanti. Se i dati vengono trattati da terzi su suo mandato, Trasfusione CRS Svizzera provvede mediante accordi contrattuali adeguati a garantire che questi terzi osservino misure equivalenti.

Controllo degli accessi fisici

Per controllo degli accessi fisici si intendono tutte le misure volte a prevenire l'ingresso di persone non autorizzate nelle aree, negli edifici o nei locali nei quali vengono trattati dati o si trovano sistemi di trattamento dei dati.

Misure tecniche	Misure organizzative
• Messa in sicurezza di finestre e porte • Sistemi di chiusura con tessere o chiavi fisiche • Ingresso alle sale server reso sicuro mediante tessera elettronica / lettore di accesso biometrico • Videosorveglianza conforme ai dati nella sala dei server esterna	• Registrazione dei visitatori all'entrata principale (citofono) e alla ricezione • Accompagnamento dei visitatori e protocolli di visita • Selezione accurata del personale delle pulizie • Istruzioni sulla sicurezza fisica e dell'ambiente • Suddivisione in zone delle sale

Controllo degli accessi elettronici

Per controllo degli accessi elettronici si intendono tutte le misure volte a prevenire l'utilizzazione non autorizzata di archivi e sistemi per il trattamento dei dati. Questi sistemi (ad es. applicazioni) devono essere utilizzati soltanto da persone aventi le apposite autorizzazioni.

Misure tecniche	Misure organizzative

• Connessioni VPN sicure per amministratori e collaboratori • Cifratura di supporti dati e dispositivi mobili • Firewall sicuri • Programmi antivirus / Endpoint Detection and Response • Autenticazione mediante nome utente e inserimento della password • Autenticazione a 2 fattori • Blocco automatico del desktop	• Regolamento sulle chiavi • Direttive complete, tra cui • regole per la password, incl. direttive sulla complessità • direttive «Clean Desk»/ blocco dello schermo • regole per l'accesso di esterni / interni

Personale affidabile per i settori sicurezza e pulizia
Generazione di profili utenti
Assegnazioni di diritti di utente

Controllo degli accessi autorizzati

Per controllo degli accessi autorizzati si intendono tutte le misure volte a garantire il mantenimento delle autorizzazioni di accesso.

Misure tecniche	Misure organizzative
• Verbalizzazione / log degli accessi a applicazioni e processi come ad es. cancellazione di dati • Distruzione di supporti dati conforme alla protezione dei dati (ad es. atti, dischi) • Cifratura di supporti dati e dispositivi mobili • Sistemi di identificazione e autenticazione • Conservazione sicura di supporti dati e documenti in locali protetti • Archiviazione sicura di documenti con diritti di accesso stabiliti • Pseudonimizzazione di dati su sistemi di test	• Piani sulle autorizzazioni • Piani sugli utenti e i ruoli • Adeguamento del numero degli amministratori con pieni diritti di accesso • Distruzione di dati (supporti dati e atti cartacei) mediante fornitori di prestazioni esterni certificati

Controllo della trasmissione

Per controllo della trasmissione si intendono tutte le misure che garantiscono la sicurezza dei dati personali durante una trasmissione di dati. Trasmissione di dati significa in questo senso trasmissioni elettroniche, trasporto e memorizzazione di dati personali.

Misure tecniche	Misure organizzative
• Tecnologia VPN sicura • Cifratura del trasporto (SSL ecc.) • Cifratura di e-mail nello scambio con EMDI	• Aggiornamento di un elenco delle attività di trattamento • Controllo periodico dei destinatari di dati, aggiornamento dei destinatari nel CRM • Impiego di servizi di trasporto esterni affidabili • Qualificazione dei fornitori di servizi di trasporto che hanno accesso ai dati personali particolarmente degni di protezione

Controllo dell'immissione

Il controllo dell'immissione serve a verificare a posteriori il trattamento dei dati; le misure devono garantire il controllo di immissioni, modifiche e cancellazioni di dati.

Misure tecniche	Misure organizzative

• Allestimento automatico di un verbale / log sull'immissione, sulla modifica e sulla cancellazione di dati, se necessario e sostenuto dal sistema	• Allestimento e impiego di nomi utenti individuali • Allestimento e impiego di nomi utenti-amministratori individuali • Assegnazione di diritti di accesso

Controllo dei mandati

Il controllo dei mandati si applica ad ogni elaborazione di un mandato. Serve a garantire che il trattamento dei mandati venga eseguito esclusivamente secondo le istruzioni del datore di lavoro.

Misure tecniche	Misure organizzative
• nessuna	• Selezione accurata del mandatario • Istruzioni scritte al mandatario • Conclusione di contratti di mandati di trattamento conformi alla protezione dei dati • Convenzione sui diritti di controllo efficaci presso il mandatario • Valutazione periodica del mandatario (valutazione dei fornitori)

Controllo della disponibilità

Nel controllo della disponibilità e recuperabilità i dati personali devono essere protetti da perdita o distruzione di modo che in caso di problemi tecnici possano essere recuperati.

Misure tecniche	Misure organizzative
• Back up • Antivirus • Firewall • Server ridondanti • Climatizzazione delle sale server • Monitoraggio della temperatura delle sale server e dei server • Gruppo di continuità ininterrotto • Generatore di emergenza di corrente • Allarme antifumo e antincendio • Impianti di estinzione • Piano sulla protezione dei dati • Gestione delle emergenze informatiche • Gestione delle crisi	• Collocamento adeguato delle sale server (protezione da rischi, ad es. inondazione, incendio) • Disposizioni sul back up • Test per la recuperabilità dei dati

Controllo della separazione

Se i dati personali vengono rilevati per finalità diverse, occorre garantire che siano trattati anche separatamente.

Misure tecniche	Misure organizzative
• Separazione dell'ambiente produttivo e di test • Chiara separazione dei dati memorizzati per finalità diverse • Separazione dei committenti su server / sistemi	• Separazione dei committenti • Diritti delle banche dati e piani sulle autorizzazioni adeguati alle serie di dati • Gestione del controllo della separazione tramite un piano sulle autorizzazioni

Verifica e valutazione

Misure per la verifica e la valutazione garantiscono che le misure di protezione stabilite siano applicate e osservate.

Misure tecniche	Misure organizzative
• Test di penetrazione periodici e audit ISDS da parte dell'UFSP • Monitoraggio del sistema	• Gestione delle modifiche • Gestione dei rischi • Helpdesk e servizi di assistenza informatica / sistema di notifiche • Gestione dei fornitori