MISURE TECNICHE E ORGANIZZATIVE IN CONFORMITÀ A LPD/OPDA

Il presente documento fornisce una panoramica delle misure tecniche e organizzative concernenti la protezione dei dati (MTO) di Health Info Net AG. Gli obblighi legali derivano dalla Legge federale sulla protezione dei dati (LPD) e dalla relativa Ordinanza (OPDa), in particolare dagli artt. 7 e 8 LPD e dall'art. 3 OPDa.

Le misure coprono necessità di protezione normali ed elevate e riguardano dati personali e dati personali degni di particolare protezione. Se, dopo l'applicazione delle MTO, emergono ulteriori rischi dal trattamento di dati personali degni di particolare protezione, viene effettuata una valutazione dei rischi per stabilire quali misure aggiuntive debbano essere adottate.

La seguente tabella elenca i requisiti dell'Ordinanza sulla protezione dei dati, le rispettive misure adottate da HIN e i corrispondenti requisiti per la certificazione secondo la norma ISO/IEC 27001. Questa tabella serve alla clientela di HIN, oltre che per la Dichiarazione sulla protezione dei dati e per i contratti base, come attestazione delle misure adottate; lo stesso vale per il rapporto tra HIN e i suoi fornitori, per cui vi si fa riferimento negli accordi per un trattamento di dati su incarico con i fornitori.

OPDa art. 3	**Breve descrizione e attuazione presso HIN**	**Requisiti di riferimento ISO/IEC 27001:2017[1]**	**Requisiti di riferimento ISO/IEC 27001:2022[2]**
1 Per garantire la **confidenzialità**, il **titolare del trattamento** e il **responsabile del trattamento** adottano provvedimenti adeguati affinché: a. le persone autorizzate abbiano accesso solo ai dati personali di cui abbisognano al fine di adempiere i loro compiti (**controllo dell'accesso ai dati**);	Il controllo dell'accesso ai dati comprende misure organizzative e tecniche finalizzate a garantire che solo gli utenti autenticati e autorizzati possano accedere ai dati e che i dati personali siano protetti da accessi non autorizzati. Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio.	A.6.1.2 Ripartizione delle funzioni A.6.2 Dispositivi mobili e telelavoro A.7.2.2 Sensibilizzazione, formazione e corsi in	A.5.3 Ripartizione delle funzioni A.5.12 Classificazione delle informazioni A.5.15 Gestione degli accessi

	Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, identificazione univoca, autenticazione sicura, processi per l'ottenimento, la modifica e la revoca delle autorizzazioni di accesso, accesso remoto in sicurezza, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	materia di sicurezza delle informazioni A.8.2 Classificazione delle informazioni A.9.1 Requisiti aziendali per la gestione degli accessi A.9.2 Gestione dell'accesso degli utenti A.9.3 Responsabilità dell'utente A.9.4 Gestione degli accessi per sistemi e applicazioni A.12.4 Registrazione e monitoraggio	A.5.16 Gestione dell'identità A.5.17 Informazioni di autenticazione A.5.18 Diritti di accesso A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.6.7 Lavoro da remoto A.8.2 Diritti di accesso privilegiati A.8.15 Registrazione
b. solo le persone autorizzate abbiano accesso ai locali e agli impianti utilizzati per il trattamento dei dati personali (**controllo dell'accesso ai locali e agli impianti**);	Il controllo dell'accesso ai locali e agli impianti comprende misure organizzative e tecniche finalizzate a proteggere i sistemi di trattamento dei dati da parte di utenti non autorizzati. Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, identificazione univoca, processi per l'ottenimento, la modifica e la revoca delle autorizzazioni di accesso, zone fisiche, sistemi di chiusura e accesso sicuri, armadietti chiusi a chiave per i dati personali fisici, accompagnamento dei visitatori, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.6.1.2 Ripartizione delle funzioni A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.2 Classificazione delle informazioni A.9.1 Requisiti aziendali per la gestione degli accessi A.11.1 Aree sicure A.12.4 Registrazione e monitoraggio	A.5.3 Ripartizione delle funzioni A.5.12 Classificazione delle informazioni A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.7.1 Perimetri di sicurezza fisica A.7.2 Accesso fisico

			A.7.3 Mettere in sicurezza uffici, locali e apparecchiature A.7.4 Monitoraggio della sicurezza fisica A.8.15 Registrazione
c. le persone non autorizzate non possano utilizzare i sistemi di trattamento automatizzato di dati personali con l'ausilio di impianti di trasmissione (**controllo degli utenti**);	Il controllo degli utenti comprende misure organizzative e tecniche che assicurino l'accesso ai dati personali solo alle persone che dispongono delle autorizzazione necessarie. Ciò si ottiene attraverso misure di controllo dell'accesso ai dati.	Si veda controllo dell'accesso ai dati.	Si veda controllo dell'accesso ai dati.
2 Per garantire la **disponibilità** e l'**integrità**, il **titolare del trattamento** e il **responsabile del trattamento** adottano provvedimenti adeguati affinché: a. le persone non autorizzate non possano leggere, copiare, modificare, spostare, cancellare o distruggere supporti di dati (**controllo dei supporti di dati**);	Il controllo dei supporti di dati comprende misure organizzative e tecniche finalizzate a proteggere i dati memorizzati (data at rest). Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, asset management, crittografia dei supporti di dati, processi di cancellazione o distruzione quando la finalità non è più valida, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.1 Responsabilità per gli asset A.8.2 Classificazione delle informazioni A.8.3 Trattamento dei supporti di dati A.11.2.6 Sicurezza di dispositivi, apparecchiature e asset all'esterno dei locali A.11.2.7 Smaltimento o riutilizzo sicuro di dispositivi e apparecchiature A.12.4 Registrazione e monitoraggio	A.5.9 Inventario delle informazioni e degli altri asset correlati A.5.12 Classificazione delle informazioni A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.7.10 Supporti di archiviazione A.7.14 Smaltimento o riutilizzo sicuro di dispositivi e apparecchiature A.8.10 Cancellazione di informazioni

			A.8.12 Prevenzione della fuga di dati A.8.15 Registrazione
b. le persone non autorizzate non possano salvare, leggere, modificare, cancellare o distruggere dati personali nella memoria (**controllo di memoria**);	Il controllo di memoria comprende misure organizzative e tecniche finalizzate a proteggere i dati nelle memorie volatili (data in use). Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene attraverso misure di integrità dei dati.	Si veda integrità dei dati.	Si veda integrità dei dati.
c. le persone non autorizzate non possano leggere, copiare, modificare, cancellare o distruggere dati personali in occasione della comunicazione degli stessi o del trasporto di supporti di dati (**controllo del trasporto**);	Il controllo della trasmissione e del trasporto comprende misure organizzative e tecniche finalizzate a proteggere i dati durante il trasporto logico e fisico (data in transit). Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, mittenti e destinatari autenticati, trasporto crittografato, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.1 Responsabilità per gli asset A.8.2 Classificazione delle informazioni A.8.3 Trattamento dei supporti di dati A.10.1 Misure crittografiche A.11.2.6 Sicurezza di dispositivi, apparecchiature e asset all'esterno dei locali A.12.4 Registrazione e monitoraggio A.13.2 Trasferimento delle informazioni A.12.4 Registrazione e monitoraggio	A.5.9 Inventario delle informazioni e degli altri asset correlati A.5.12 Classificazione delle informazioni A.5.14 Trasmissione delle informazioni A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.7.14 Smaltimento o riutilizzo sicuro di dispositivi e apparecchiature A.8.10 Cancellazione di informazioni A.8.12 Prevenzione della fuga di dati

			A.8.15 Registrazione A.8.24 Uso della crittografia
d. la disponibilità e l'accesso ai dati personali possano essere rapidamente ripristinati in caso di incidente fisico o tecnico (**ripristino**);	La disponibilità comprende misure organizzative e tecniche finalizzate a proteggere i dati dalla perdita. Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, gruppi di continuità, sistemi ridondanti, archiviazione dati regolare, test di ripristino periodici, piani di emergenza e audit.	A.8.2 Classificazione delle informazioni A.12.3 Archivio dati A.17.1 Mantenimento della sicurezza delle informazioni A.17.2 Ridondanze A.12.4 Registrazione e monitoraggio	A.5.12 Classificazione delle informazioni A.5.30 Prontezza delle TIC per la continuità operativa A.8.13 Tutela delle informazioni A.8.14 Ridondanza delle apparecchiature di elaborazione delle informazioni A.8.15 Registrazione
e. siano disponibili tutte le funzioni del sistema di trattamento automatizzato dei dati (disponibilità), siano segnalati eventuali malfunzionamenti (affidabilità) e i dati personali registrati non siano danneggiati da malfunzionamenti del sistema (**integrità dei dati**);	L'integrità comprende misure organizzative e tecniche finalizzate a garantire l'accuratezza e la completezza dei dati. Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, considerazione dei requisiti di sicurezza nello sviluppo e nella gestione, segmentazione delle reti e dei supporti di memoria, hardening dei sistemi, gestione delle vulnerabilità, protezione da malware, monitoraggio, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.2 Classificazione delle informazioni A.12.1 Procedure e responsabilità operative A.12.2 Protezione contro software dannosi A.12.4 Registrazione e monitoraggio A.14.1 Requisiti di sicurezza per sistemi informatici	A.5.12 Classificazione delle informazioni A.5.33 Protezione delle registrazioni A.5.34 Protezione dei dati e protezione dei dati personali A.5.37 Procedure operative documentate A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.9 Gestione della configurazione A.8.15 Registrazione

		A.14.2 Sicurezza nei processi di sviluppo e supporto A.18.1.3 Protezione delle registrazioni	A.8.32 Controllo delle modifiche
f. sia sempre aggiornato il livello di sicurezza dei sistemi operativi e delle applicazioni e siano colmate le lacune critiche riscontrate (**sicurezza del sistema**).	La sicurezza del sistema copre tutti gli aspetti della sicurezza operativa. Questo riguarda i server, i database, i sistemi di archiviazione, di backup e di rete nei nostri datacenter, nonché i sistemi client in ufficio e in viaggio. Ciò si ottiene attraverso misure per il controllo dell'accesso ai dati e dell'accesso ai locali e agli impianti, misure per il controllo dei supporti di dati, di memoria e del trasporto, nonché misure per la disponibilità e l'integrità.	Si veda controllo dell'accesso ai dati e controllo dell'accesso ai locali e agli impianti, controllo dei supporti di dati, di memoria e del trasporto, nonché disponibilità e integrità.	Si veda controllo dell'accesso ai dati e controllo dell'accesso ai locali e agli impianti, controllo dei supporti di dati, di memoria e del trasporto, nonché disponibilità e integrità.
3 Per garantire la **tracciabilità**, il **titolare del trattamento** e il **responsabile del trattamento** adottano provvedimenti adeguati affinché: a. si possa verificare quali dati personali sono stati introdotti o modificati nel sistema di trattamento automatizzato dei dati, in quale momento e da chi (**controllo dell'introduzione**);	Il controllo dell'introduzione comprende misure organizzative e tecniche finalizzate a garantire la tracciabilità del trattamento dei dati, ossia registrazione, archiviazione, modifica, trasferimento, backup, archiviazione e cancellazione. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, un elenco delle operazioni di trattamento dei dati, monitoraggio, registrazione, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.1 Responsabilità per gli asset A.8.2 Classificazione delle informazioni A.12.4 Registrazione e monitoraggio A.18.1.3 Protezione delle registrazioni	A.5.9 Inventario delle informazioni e degli altri asset correlati A.5.12 Classificazione delle informazioni A.5.33 Protezione delle registrazioni A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.8.15 Registrazione A.8.16 Monitoraggio delle attività

b. si possa verificare a chi sono stati comunicati dati personali con l'ausilio di impianti di trasmissione (**controllo di comunicazione**);	Il controllo di comunicazione comprende misure organizzative e tecniche finalizzate a garantire la tracciabilità del trattamento dei dati, ossia registrazione, archiviazione, modifica, trasferimento, backup, archiviazione e cancellazione. Ciò si ottiene attraverso misure di controllo dell'accesso ai dati, controllo del trasporto e controllo dell'introduzione.	Si veda controllo dell'accesso ai dati, controllo del trasporto e controllo dell'introduzione.	Si veda controllo dell'accesso ai dati, controllo del trasporto e controllo dell'introduzione.
c. si possano individuare rapidamente le violazioni della sicurezza dei dati (**individuazione**) e adottare provvedimenti per ridurre o eliminare le conseguenze (**eliminazione**).	L'individuazione e l'eliminazione comprendono misure organizzative e tecniche finalizzate a garantire che le violazioni potenziali ed effettive della sicurezza dei dati siano rilevate, analizzate, valutate, gestite e comunicate. Ciò si ottiene, tra l'altro, attraverso linee guida appropriate, responsabilità chiaramente definite, obbligo di segnalazione di rischi per la sicurezza e di accadimenti correlati alla sicurezza, contatti con le autorità, corsi di formazione Security Awareness iniziali e ricorrenti e controlli e audit periodici.	A.6.1.3 Contatti con le autorità A.7.2.2 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.7.2.3 Processo disciplinare A.16.1 Gestione degli accadimenti correlati alla sicurezza delle informazioni e miglioramenti	A.5.24 Pianificazione e preparazione per la gestione degli accadimenti correlati alla sicurezza delle informazioni A.5.25 Valutazione e decisione in relazione agli eventi correlati alla sicurezza delle informazioni A.5.26 Reazione agli accadimenti correlati alla sicurezza delle informazioni A.5.27 Conoscenze apprese dagli accadimenti correlati alla sicurezza delle informazioni A.5.28 Raccolta delle prove A.5.33 Protezione delle registrazioni

			A.5.34 Protezione dei dati e protezione dei dati personali A.6.3 Sensibilizzazione, formazione e corsi in materia di sicurezza delle informazioni A.6.4 Processo disciplinare

[1] entro e non oltre ottobre 2025
[2] al più tardi da ottobre 2025