# Misure tecniche e organizzative Worldline Svizzera SA

(CHE IT)

## 1 Scopo del presente documento

Il presente documento contiene un elenco di misure tecniche e operative applicabili come standard. Le effettive misure adottate dipendono dal Servizio e dalla localizzazione del trattamento interessato per il fatto che non tutte le misure sono pertinenti per tutti i Servizi e tutte le localizzazioni. Worldline garantisce di avere adottato, per tutti i Servizi e per tutte le localizzazioni, le adeguate e necessarie misure tecniche e operative incluse nell'elenco sottostante in seguito a una valutazione d'impatto sulla protezione dei dati. Le misure sono intese a:

- garantire la sicurezza e la riservatezza dei dati personali;
- proteggere la sicurezza e l'integrità dei dati personali contro qualsiasi prevedibile minaccia o pericolo;
- proteggere i dati personali contro qualsiasi reale trattamento, perdita, utilizzo, divulgazione, acquisizione o accesso non autorizzato.

La pagina contiene inoltre un elenco di subcontraenti utilizzati da Worldline per l'esecuzione dei suoi servizi. Worldline garantisce che tutti i suoi responsabili subordinati del trattamento hanno fornito garanzie adeguate sulla protezione dei dati personali da essi trattati per suo conto impegnandosi al controllo dei subcontraenti: non è ammesso il trattamento dei dati commissionato, ai sensi dell'articolo 28 del regolamento GDPR, senza appropriate istruzioni dal contraente principale, ovvero: contratto chiaramente stipulato, gestione formale del subappalto, e selezione rigorosa degli addetti al trattamento (certificazione ISO, ISMS), competenza comprovata, monitoraggio di follow-up.
Worldline si impegna a monitorare costantemente l'efficacia delle sue salvaguardie delle informazioni e a procedere a un audit annuale di conformità condotto da una terza parte indipendente a garanzia delle misure e dei controlli in essere.

## 2 Misure tecniche e organizzative

**A Personale, consapevolezza, e Risorse umane:**

- Tutte le assunzioni seguono un processo di screening conformemente ai principi della politica di Worldline sul controllo dei precedenti;
- Il contratto di ciascun dipendente contiene clausole di riservatezza;
- La formazione al Codice di deontologia e sensibilizzazione (incluso un test) è un obbligo per tutto il personale, che è tenuto ogni anno a completare un modulo di e-learning;
- La politica del Gruppo sull'uso accettabile delle risorse informatiche, o una sua versione locale, è comunicata a tutto il personale;
- La dichiarazione sulla Politica per la sicurezza firmata dalla Direzione è comunicata a tutto il personale;
- Il personale di Worldline è tenuto a seguire ogni anno una formazione sulle politiche Worldline sulla protezione dei dati e sulla sicurezza delle informazioni (incluso un test);
- Formazione regolare di sensibilizzazione al regolamento GDPR per tutto il personale (oltre alla formazione sulle politiche Worldline sulla protezione dei dati e sulla sicurezza delle informazioni);
- L'accesso ai sistemi è concesso «a chi deve accedervi» tenendo conto della segregazione delle mansioni;
- Per verificare la sicurezza delle pratiche, vengono condotti regolarmente degli audit interni di sicurezza.

**B Sicurezza fisica e documenti cartacei:**

Conformità con la politica del Gruppo Worldline sulla sicurezza fisica e ambientale:

- Attuazione di sistemi di controllo dell'acceso e dei visitatori per tutti i visitatori/ospiti;
- Controllo fisico dell'accesso (protezione contro l'accesso non autorizzato al trattamento dei dati o a locali di archiviazione): in particolare mediante smart cards, carte magnetiche, apriporta elettrici, portieri, personale di sicurezza, sistemi di allarme, sistemi video;
- Revisione degli accessi fisici su base periodica;
- Adozione del processo scrivania vuota, schermo vuoto e stampa «follow me»;
- Le informazioni, inclusi i documenti cartacei, gestite dall'importatore dei dati, sono classificate, etichettate, protette e gestite conformemente alla politica Worldline sulla classificazione delle informazioni;
- Salvo specifica e previa approvazione, i desktop non vengono rimossi dal sito;
- Sorveglianza CCTV per proteggere le zone ad accesso limitato;
- Attuazione di sistemi di allarme di intervento antincendio per proteggere la sicurezza del personale;
- Esercitazioni di evacuazione antincendio vengono condotte periodicamente.

**C I dispositivi degli utenti finali da remoto sono protetti:**

Gli utenti da remoto lavorano con laptop e desktop collegati alla rete sicurizzata Worldline mantenuta da Global IT per il Gruppo Worldline. Sono inoltre incorporate le seguenti misure di sicurezza:

- Criptazione del disco rigido sui laptop aziendali;
- Autenticazione a 2 fattori (PKI/Alternativa);
- Protezione gestita centralmente e antivirus;
- Gestione e monitoraggio dei software per controllare eventuali installazioni di software non autorizzate;
- Controlli del nome utente e della password per accedere alle informazioni;
- Revisione periodica degli accessi;
- Scansione automatica delle e-mail e software antivirus e antispam.

**D Sicurezza dell'accesso da remoto**

In genere, per l'accesso ai sistemi target critici di Worldline si utilizza l'autenticazione a 2 fattori. Se la fonte della connessione da remoto è un sistema controllato da Worldline, si effettua un'autenticazione basata su un certificato incluso nel dispositivo.
Qualsiasi altra impostazione e connessione deve essere prima approvata dai servizi di sicurezza.

**E Alcune delle misure generiche di sicurezza:**

- I dati sono archiviati in data center ubicati nell'UE e in Svizzera o, nel caso dei laptop, criptati nel relativo dispositivo;
- Cessazione dell'accesso alla connessione in zone smilitarizzate;
- Tutta la connettività nell'area sicurizzata (zona PCI) è criptata;
- L'accesso alla zona PCI è possibile solo mediante autenticazione forte attraverso il security client fornito;
- Si deve passare attraverso molteplici livelli di firewall e rilevamento delle intrusioni;
- Accesso gestito secondo i principi del controllo dell'accesso in base alle mansioni;
- Gestione della privacy, compresa la formazione regolare del personale:
- Gestione della reazione agli incidenti;
- Impostazioni per difetto orientate alla privacy.

**F Controllo dell'accesso a dati personali**

I dipendenti con accesso a dati personali possono accedere solo ai dati necessari rispetto alla finalità delle attività sotto la loro responsabilità. L'autorizzazione all'accesso è concessa su base «a chi deve accedervi» ed è o nominale o basata sulle mansioni. Gli accessi vengono registrati e viene attribuita una responsabilità per il controllo dell'acceso.

Sono in essere le seguenti misure:

- Obbligo per il personale di rispettare le politiche sulla sicurezza e la protezione dei dati di Worldline e quelle vigenti localmente;
- Istruzioni di lavoro sul trattamento dei dati personali;
- Controllo elettronico dell'accesso (protezione contro uso non autorizzato dei sistemi di trattamento o di archiviazione dei dati): in particolare mediante password (con la relativa politica), meccanismi di blocco automatico, autenticazione a due fattori, criptazione dei vettori;
- Controllo dell'accesso interno (prevenzione della consultazione, copia, modifica o rimozione non autorizzata internamente a Worldline): nella fattispecie mediante il ricorso a profili standard di autorizzazione in base alla «necessità di sapere», processo standard di attribuzione dei diritti di utenza, registrazione degli accessi, revisione periodica dei diritti attribuiti, in particolare per quanto concerne gli account amministrativi;
- Distruzione controllata dei supporti;
- Procedure di controllo del rispetto delle procedure e delle istruzioni di lavoro.

110.0789.04 CHE_IT/12.2021

**G Sicurezza e riservatezza dei dati personali**

In base a una valutazione dei rischi (ed eventualmente a un DPIA addizionale), Worldline garantisce un livello di sicurezza adeguato al rischio, compresi tra l'altro, se opportuno:

- Uno schema di classificazione dei dati: categorizzazione dei dati personali secondo il livello di riservatezza in base alle disposizioni di legge o a un'autovalutazione;
- Nessuna consultazione, copia, modifica o rimozione non autorizzata durante la trasmissione elettronica o il trasporto, in particolare mediante criptazione e VPN (Virtual Private Networks);
- Capacità di garantire la riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento;
- Protezione contro la distruzione o la perdita accidentale o intenzionale, per esempio mediante strategie di backup (online/offline; on-site/off-site), Uninterruptible Power Supply – UPS (generatore diesel di emergenza), antivirus, firewall, canali di allerta e piani di emergenza, controlli di sicurezza sull'infrastruttura e sui livelli di applicazione, piano di sicurezza a più livelli con outsourcing dei backup a centri di backup dei dati, processi standard in caso di rotazione/dimissione di personale;
- Capacità di ripristinare tempestivamente la disponibilità e l'accesso ai dati personali in caso di incidenti fisici o tecnici;
- Processo di test, controllo e valutazione regolare dell'efficacia delle misure tecniche e organizzative adottate per garantire la sicurezza del trattamento (audit interni, PCI-DSS, ISO27001, enti nazionali di ispezione);
- Registri del processo ai sensi del regolamento GDPR;
- Sistemi di registrazione dell'accesso finalizzati a rilevare tentativi di accesso non autorizzato;
- I dati principali dei clienti e i metadati (inclusi back-up, archivi, registri dell'acceso, ecc.) saranno archiviati solo per il tempo necessario alle finalità per le quali sono stati raccolti, fatto salvo l'eventuale obbligo contrattuale o legale di conservare tali dati per un periodo più lungo.

**H Controllo dell'organizzazione**

Il responsabile del trattamento manterrà l'organizzazione interna in modo tale da rispondere ai requisiti della legislazione vigente nonché ai requisiti di sicurezza del titolare dei dati. A tal fine si attueranno:

Politiche e procedure interne per il trattamento dei dati, linee guida, istruzioni di lavoro, descrizioni dei processi e norme per la programmazione, il collaudo e il rilascio, qualora riguardino dati personali trasferiti dal titolare;

Realizzazione di un quadro di controllo della protezione dei dati che sarà sottoposto ogni anno a un audit di conformità;

Attuazione di un piano di emergenza con procedure e attribuzione di responsabilità (piano di emergenza alternativo).