FORMAPER

DISCIPLINARE

PER DESIGNATI E AUTORIZZATI

AL TRATTAMENTO DEI DATI PERSONALI

Il presente documento si inserisce nel
piano di *accountability* dell'Ente,
in linea con i principi di cui al
Regolamento (UE) 2016/679 – GDPR

SOMMARIO

MATRICE DELLA REDAZIONE E DELLE REVISIONI

Data	Descrizione	Stato
29.11.2023	Disciplinare per designati e autorizzati al trattamento dei dati personali	Approvato da C.d.A. delibera n. 19

PREMESSA

Le indicazioni che seguono costituiscono la disciplina che gli Autorizzati e i Designati di FORMAPER debbono seguire nello svolgimento dei trattamenti di dati personali loro affidati, in ragione delle proprie mansioni.

Con il termine **Autorizzati** ci si riferisce a tutti quei soggetti (persone fisiche) inseriti nell'organizzazione di FORMAPER che operano materialmente sui dati personali in ragione delle mansioni a cui sono adibiti e dietro espressa autorizzazione da parte del Titolare, svolgendo i trattamenti sulla base delle indicazioni fornite dal Vertice dell'Ente e dai Designati di loro riferimento. A puro titolo esemplificativo e non esaustivo, sono Autorizzati i dipendenti dell'Ente, il personale in somministrazione, gli stagisti, ecc., purché l'Ente, in ragione delle mansioni loro attribuite, abbia provveduto ad autorizzarli al trattamento dei dati personali. A tale riguardo, si rimanda al Modello Organizzativo Privacy dell'Ente, adottato nella prima versione con Delibera 13 del 21.09.21 del CDA e successivamente implementato il 1.04.2022, con approvazione del Direttore Generale. Il personale di FORMAPER è stato nominato **Autorizzati** con Ods n° 8 del 23.12.2020.

Con il termine **Designati** ci si riferisce ai soggetti (anche in questo caso persone fisiche inserite nell'organizzazione di FORMAPER), a cui, ai sensi dell'art. 2-*quaterdecies* del Codice privacy, l'Ente ha attribuito specifici poteri, oltre che compiti e funzioni, ai fini non solo di dare esecuzione ad attività materiali di trattamento, ma anche e soprattutto di contribuire ad assicurare la *compliance* dell'Ente alla normativa in materia di *data protection*. Il personale di FORMAPER è stato nominato **Designati** con Modello Organizzativo Privacy dell'Ente, adottato nella prima versione con Delibera 13 del 21.09.21 del CDA e successivamente implementato il 1.04.2022, con approvazione del Direttore Generale

Fermi restando i profili di responsabilità personale del singolo individuo, sia di carattere disciplinare che di altra natura previsti per legge, il mancato rispetto delle istruzioni in materia di trattamento e protezione dei dati personali potrebbe comportare la violazione delle disposizioni normative nazionali ed europee in materia *privacy*, nonché delle regole interne previste per la protezione dei dati personali, con conseguenziale esposizione di FORMAPER a rischi sul piano delle responsabilità e delle sanzioni a livello civile, amministrativo e penale. Per tale ragione, risulta di fondamentale importanza conoscere ed attenersi alle indicazioni qui riportate.

PRINCIPI FONDAMENTALI

Ogni trattamento di dati personali deve avvenire nel rispetto primario dei seguenti principi di ordine generale, fissati dall'art. 5 del Regolamento (UE) 2016/679 (GDPR).

I dati devono essere:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato (principi di «liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità (principio di «limitazione della finalità»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati (principio di «minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati, adottando tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati (principio di «esattezza»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (principio di «limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (principio di «integrità e riservatezza»).

Ciascun trattamento deve, inoltre, avvenire nei limiti imposti dal principio fondamentale di riservatezza e nel rispetto della dignità della persona dell'Interessato, ovverosia di colui al quale i dati si riferiscono.

Ove si riscontri o sospetti che il trattamento dei dati personali sia operato dall'Ente in violazione dei summenzionati principi, occorre darne immediato avviso al Referente *privacy* e al proprio Designato di riferimento.

REGOLE GENERALI DI COMPORTAMENTO

Tutti i soggetti che operano sui dati personali sono tenuti a conoscere e ad attenersi scrupolosamente alle istruzioni loro fornite dal Vertice del Titolare, dal Direttore di FORMAPER e/o dal proprio Designato di riferimento.

Autorizzati e Designati sono altresì tenuti a prendere parte attiva alla formazione obbligatoria in materia di protezione dei dati personali.

Laddove si riscontri o si sospetti essere intervenuta una violazione di sicurezza sui dati personali, tale da comprometterne la riservatezza (accesso abusivo), l'integrità (alterazione indebita) o la disponibilità (perdita, definitiva o provvisoria, per cancellazione, eliminazione, distruzione dei dati, oppure per interruzione prolungata dei servizi che consentono l'accesso ai dati), occorre:

- darne immediato avviso al proprio Designato di riferimento;
- attenersi a quanto indicato nell'ambito dell'apposita **procedura di gestione *Data Breach***;
- rimanere a disposizione dell'Ente per la raccolta di informazioni relative all'evento;
- ove necessario, anche in relazione al ruolo svolto da ciascun Autorizzato, porre in essere le strategie di contenimento dei rischi e le eventuali azioni di *remediation* (azioni correttive) decise dall'Ente nel corso della gestione dell'evento *Data Breach*.

Ove pervenga una richiesta di esercizio dei diritti in materia di protezione dei dati personali, occorre procedere nel più breve tempo possibile, attenendosi a quanto previsto nell'apposita **procedura per la gestione dei diritti privacy**.

Ciascun soggetto che opera sui dati personali, sia esso Autorizzato o Designato, è tenuto a:

1) accedere ai dati personali nei limiti dell'autorizzazione ricevuta;

2) operare esclusivamente i trattamenti strettamente connessi e necessari allo svolgimento dei propri compiti;

3) non utilizzare, diffondere o comunicare per fini personali o per finalità diverse da quelle fissate dal Titolare e/o al di fuori dei casi consentiti dalla normativa, i dati personali di cui viene a conoscenza nell'esecuzione dei propri compiti/mansioni/attività, mantenendo il più assoluto riserbo in relazione ai dati e alle informazioni in qualunque forma appresi (per iscritto o oralmente, anche attraverso l'ascolto accidentale di colloqui, conversazioni, etc..);

4) conoscere e adottare con diligenza le misure di sicurezza previste dall'Ente, segnalando al proprio Designato di riferimento e al Referente *privacy* eventuali carenze sotto il profilo della protezione dei dati, in modo da ridurre al minimo i rischi, anche accidentali, di accesso non autorizzato ai dati, di impiego dei dati non consentito o non conforme alle finalità dichiarate agli Interessati, di modifica, alterazione o cancellazione/distruzione indesiderate dei dati;

5) informare immediatamente il proprio Designato di riferimento qualora per le operazioni di trattamento sorga la necessità di compiere attività ulteriori o assumere decisioni non contemplate dal proprio incarico;

6) adottare ogni possibile cura ed attenzione nello svolgimento delle operazioni di trattamento dei dati personali, tenendo conto che l'eventuale creazione di copie, in locale, in rete ovvero cartacee di documenti/archivi esistenti e contenenti dati personali, aumenta il livello di rischio per i diritti e le libertà degli interessati;

7) mantenere riservate le proprie credenziali di accesso ai sistemi informativi impiegati per ragioni lavorative, non comunicandole / diffondendole / condividendole con altri soggetti (compresi i colleghi di lavoro) e non trascrivendole (a titolo esemplificativo) in appunti, *post-it*, agende, prediligendo invece gestionali di *password* dotati di crittografia forte e protetti con *password* complessa;

8) custodire con cura e diligenza le chiavi fisiche (comprese le tessere/badge di accesso) che consentono l'apertura di armadi o l'accesso ad archivi e locali, evitando – salvo nei casi in ciò sia espressamente autorizzato – di effettuare copie, calchi o fotografie delle stesse e/o di consegnarle o prestarle ad altri soggetti (compresi i colleghi di lavoro, se non espressamente autorizzati a riceverle);

9) non comunicare e/o diffondere (a titolo meramente esemplificativo, a mezzo *social network* o sistemi di messaggistica personali) fotografie o dati, anche parziali, del proprio tesserino di riconoscimento e/o badge;

10) non lasciare in alcun modo incustoditi o accessibili documenti e strumenti di lavoro (compreso – a titolo esemplificativo – il computer o laptop impiegato per lo svolgimento delle proprie mansioni) al termine della sessione lavorativa, nonché in ogni occasione di allontanamento (anche se di brevissima durata) dalla propria postazione;

11) fornire assistenza e collaborazione al DPO e al Referente *privacy* in relazione a loro possibili richieste di informazioni o allo svolgimento di *audit*;

12) al termine del proprio rapporto di lavoro, provvedere alla restituzione delle chiavi fisiche, del tesserino di riconoscimento e/o badge e di tutto il materiale (cartaceo ed elettronico) contenente dati di carattere personale, cancellandone/distruggendone ogni eventuale copia.

REGOLE AGGIUNTIVE PER I DESIGNATI

Per quanto attiene, in particolare, alla figura dei Designati, questi devono:

i) individuare, nel proprio ambito di competenza, tutte le persone le cui mansioni lavorative implicano il trattamento di dati personali;

ii) assicurarsi che le autorizzazioni ad accedere, modificare o cancellare / distruggere i dati, assegnate a ciascun Autorizzato, siano esclusivamente quelle minime e strettamente necessarie rispetto alle mansioni lavorative che l'Autorizzato è chiamato a svolgere;

iii) assicurarsi che gli autorizzati operino nel rispetto delle istruzioni loro impartite, in relazione al trattamento e alla protezione dei dati personali;

iv) adoperarsi al fine di rendere effettiva la tutela della riservatezza, dell'integrità e della disponibilità dei dati, nonché e l'osservanza da parte degli Autorizzati, nel compimento delle operazioni di trattamento, dei principi di carattere generale che informano la vigente disciplina in materia;

v) stabilire modalità di accesso ai dati e l'organizzazione del lavoro degli autorizzati, come le modalità di trasmissione dei dati da parte degli stessi, avendo cura di adottare preventivamente le più opportune misure organizzative;

vi) stabilire delle modalità di accesso all'archiviazione dei dati che riduca il rischio di impatto sui dati, facendo in modo che l'accesso alle informazioni sia garantito esclusivamente agli autorizzati che ne hanno effettivo bisogno per lo svolgimento delle proprie mansioni lavorative e nei limiti delle stesse;

vii) organizzare le modalità di lavoro al fine di ridurre il rischio di impatto sui dati;

viii) comunicare al Referente *privacy* e al Direttore di FORMAPER eventuali problematiche che impattano sulla protezione dei dati personali;

ix) coinvolgere il Referente *privacy* nella eventuale progettazione di nuovi trattamenti di dati personali, secondo le logiche di *privacy by design*.

In relazione ai punti *viii)* e *ix)*, nonché alle più importanti segnalazioni pervenutegli direttamente dagli Autorizzati al trattamento dei dati, il Designato Referente privacy provvede a sua volta al coinvolgimento del DPO di FORMAPER.

REGOLE GENERALI PER LA CREAZIONE E LA GESTIONE DELLE PASSWORD

Ai fini dell'assolvimento delle proprie mansioni lavorative ciascun Designato / Autorizzato è chiamato a creare e ad aggiornare periodicamente una o più password. A tale riguardo, il Designato / Autorizzato, deve prestare particolare attenzione ai criteri mediante cui sceglie e conserva le proprie password, avendo cura in particolare di:

1. **Creazione**
   - in caso di assegnazione di una password temporanea, modificarla immediatamente o, ove ciò non sia obiettivamente possibile, nel più breve tempo possibile e comunque non oltre il primo accesso al servizio a cui tale password è collegata;

- evitare l'impiego di password già utilizzate in passato;
- evitare l'utilizzo di password impiegate nella propria vita privata;
- evitare sempre, nella propria password, riferimenti personali, familiari (es. nomi e/o date di nascita dei figli) e altre informazioni che possono essere facilmente recuperate dai profili social (es. nome del proprio animale domestico); tale accorgimento deve riguardare anche le risposte fornite nell'eventuale sistema di "recupero password", ove presente;
- evitare sempre che la password contenga riferimenti alla propria user-id o matricola;
- impiegare almeno 8 caratteri (si suggerisce caldamente l'impiego di almeno 15 caratteri), di cui almeno una lettera maiuscola, almeno una lettera minuscola, un numero e un carattere speciale;
- prediligere frasi complesse e parole o stringhe alfanumeriche di fantasia, evitando per quanto più possibile parole "da dizionario";
- ove possibile, attivare sempre il sistema di "verifica in due passaggi".

2. Gestione

- Cambiare la password regolarmente (almeno ogni 6 mesi) e comunque ogni volta che viene richiesto dal sistema;
- non condividere la propria password con nessuno, colleghi compresi;
- in caso di condivisione (volontaria o involontaria) della propria password, provvedere immediatamente a cambiarla;
- evitare sempre di annotare le proprie password su qualsivoglia supporto cartaceo (come fogli, foglietti, post-it, agende, diari, ecc.);
- evitare sempre di annotare le proprie password all'interno dei propri dispositivi (computer, smartphone, tablet, ecc.) in file non protetti da crittografia;
- evitare sempre il salvataggio/memorizzazione delle password da parte del browser di navigazione internet.

REGOLE AGGIUNTIVE PER LO *SMART WORKING*

Ferme le regole sopra indicate, in caso di attività lavorativa svolta in modalità Smart Working o similare, Autorizzati e Designati debbono operare esclusivamente impiegando gli strumenti informatici dati in dotazione da FORMAPER, prestando particolare attenzione a locali e postazioni di lavoro, in cui le condizioni di riservatezza potrebbero non sempre essere garantite.

Come hanno dimostrato i fatti di cronaca di inizio agosto 2021 (colpito il sistema informatico della Regione Lazio, per il tramite di un dispositivo di un dipendente in *Smart Working*), la tutela di *password*, stazioni di lavoro e documenti è di fondamentale importanza per non esporre tutta l'organizzazione a rischi, che possono talvolta essere anche catastrofici. Dall'inizio della guerra in Ucraina, in particolare, si è assistito ad un notevole incremento degli attacchi informatici, anche rivolti al settore pubblico, nell'ambito di quella che viene definita *cyberwarfare*. Ciò aumenta notevolmente i rischi per la tutela dei dati personali, specie se i trattamenti vengono operati su dispositivi ad uso promiscuo (personale/lavorativo), in quanto maggiormente esposti a malware.

Al fine di garantire un ragionevole livello di sicurezza si ricorda, oltre a quanto di seguito indicato, di prestare sempre la massima attenzione alle operazioni che vengono effettuate, posto che l'errore umano (spesso dovuto a fretta o stanchezza) rappresenta oggi il principale fattore di rischio, anche e soprattutto in quanto sfruttabile da eventuali attaccanti.

A. Connettività

- Utilizzare unicamente connettività fornita dal proprio fornitore di servizi contrattualizzati (ISP).

- Evitare l'utilizzo di reti WiFi pubbliche e, soprattutto, di "reti aperte" e/o sconosciute.
- Verificare che la propria rete domestica sia adeguatamente protetta con cifratura, in caso di WiFi, almeno wpa2 e *password* di almeno 8 caratteri alfanumerici, comprensiva di almeno un carattere speciale (*, #, +, _, -, @, ?, !...), una lettera minuscola, una lettera maiuscola e un numero.
- Non utilizzare mai la *password* di fabbrica del proprio router/modem: procedere sempre a personalizzarla *prima* di impiegare la rete per attività lavorative; una volta personalizzata, la *password* può rimanere la stessa per diverse sessioni di lavoro, purché non sia stata volontariamente o accidentalmente condivisa con altri soggetti (in tal caso, procedere alla modifica della *password*, avendo cura che la nuova *password* non sia facilmente intuibile o similare alla precedente).
- In caso di utilizzo di una rete LAN, verificare che i cavi siano direttamente collegati al proprio modem/switch.

B. Sessione di lavoro

- Per tutta la durata delle attività in *Smart Working* evitare attività parallele di navigazione web per finalità personali tramite i browser installati o attività che possano mettere a rischio la sicurezza del sistema e, di conseguenza, delle risorse dell'Ente accessibili in remoto.
- La sessione di lavoro deve svolgersi mediante l'impiego della VPN assegnata; in ogni caso devono essere rispettate le consuete regole di salvataggio dei dati sui server di FORMAPER.
- L'accesso alla VPN deve avvenire attraverso il *client* pre-installato o indicato da FORMAPER.

C. Terminale / Stazione di lavoro

- Nel caso in cui FORMAPER fornisca dispositivi con caratteristiche certificate, tali dispositivi sono gli unici strumenti da usare per effettuare l'attività lavorativa.
- Utilizzare unicamente stazioni di lavoro dotate di sistema operativo e di anti-virus costantemente aggiornati.
- Per l'esecuzione delle attività in *Smart Working* non utilizzare utenze amministrative locali. Utilizzare utenze con privilegi elevati solo in caso di effettiva e comprovabile necessità.
- Nel caso di utilizzo di dispositivi condivisi, verificare che l'utenza di lavoro sia l'unica connessa e, in caso contrario disconnettere, per tutta la durata della sessione, gli altri utenti connessi.
- Disabilitare tutti i protocolli di trasmissione dati non strettamente legati ad attività lavorative (es. connessione con *Smart-TV*, *personal assistance*, ecc).
- Nel caso di dispositivi dotati di Bluetooth, mantenere quest'ultimo disattivato a meno che lo stesso non sia costantemente collegato ad altro dispositivo o periferica necessario/a ai fini della sessione di lavoro.

D. Applicazioni

- Verificare che TUTTI i software presenti sul terminale utilizzato per le attività in *Smart Working* siano leciti, licenziati e aggiornati; in caso contrario procedere con la rimozione di tutto il software privo di licenza o obsoleto prima di accedere a risorse lavorative.
- Per tutte le credenziali coinvolte in attività di autenticazione su sistemi di FORMAPER, è fatto obbligo di impostare il sistema in modo da NON salvare nei browser nessuna informazione (*username*, *password*, completamento campi automatico, ecc.).

E. Supporti cartacei

- Nel caso sia necessario utilizzare, in *input* o *output* dell'attività lavorativa, supporti cartacei in cui siano riportate informazioni contenenti dati di carattere personale, è

necessario che questi supporti, terminato l'uso, se non più necessari vengano distrutti in maniera tale che non sia possibile risalire alle informazioni presenti nel documento: non è sufficiente strappare a metà e accartocciare i fogli prima di gettarli. Ove l'effettiva distruzione dei supporti non sia possibile, è necessario custodirli temporaneamente in luoghi chiusi a chiave e procedere alla distruzione sicura mediante apparecchiature "distruggi documenti" presso la sede dell'Ente.

- Tutta la documentazione cartacea che sia stata portata a casa dall'ufficio per supportare l'attività lavorativa, o che deve essere conservata, deve essere riposta in spazi chiusi a chiave per evitare l'accesso e la visibilità a persone che non ne hanno titolo o ruolo (familiari compresi).

F. Ambiente di lavoro

- Lavorare in ambienti che non permettano a terzi di carpire informazioni inerenti l'attività professionale: a questo proposito, porre particolare attenzione agli spazi di confine con altre unità immobiliari, ambienti non insonorizzati e luoghi pubblici (attenzione, specie in questo caso, alla visibilità/leggibilità da parte di terzi delle informazioni visualizzate sul monitor del dispositivo impiegato), cercando di mantenere un livello di volume di voce il più possibile contenuto e non comunicando dati personali di rilievo.

G. Tavolo / scrivania

- Il tavolo o la scrivania su cui ci si posiziona per operare deve essere tenuto sgombro da materiale e documenti che possano essere utilizzati impropriamente da terzi per risalire alle attività svolte o che possano essere di aiuto per individuare credenziali o altri criteri di accesso.

H. Sistemi di messaggistica

- Utilizzare sempre ed esclusivamente i canali ufficiali di comunicazione, anche con i colleghi di lavoro, evitando l'impiego di caselle mail personali, strumenti di *instant messaging* (compresi *WhatsApp*, *Telegram*, ecc.) o *social network*.