

Report di Mappatura GDPR

Analisi degli strumenti informatici e dei flussi di dati aziendali

Data analisi: 16/09/2026 — Utenti censiti: 2

1. Dispositivi e strumenti

I PC in uso sono in parte personali e in parte assegnati dall'azienda. Un dispositivo risulta ancora con Windows 10, mentre un altro risulta aggiornato dal tecnico. Sono in uso chiavette USB per lo spostamento dei file. Vengono utilizzati anche strumenti di videosorveglianza/allarmi e di geolocalizzazione.

2. Software e applicativi

Gli strumenti principali di lavoro sono browser, gestionale, Excel e canali social. Risulta l'uso non ufficiale di ChatGPT e di WhatsApp Web per comunicare con i colleghi. L'accesso al programma principale avviene con password personale, mnemonica.

3. Banche dati e condivisione file

I documenti vengono salvati in cartelle condivise di rete e archiviati anche nel NAS. L'invio di file a colleghi o clienti avviene tramite WhatsApp, WeTransfer o altri canali non tracciati, senza l'uso della posta elettronica aziendale. Le banche dati citate includono appunti personali ed elenchi prospect.

4. Dati trattati

Tra i dati trattati figurano dati di contatto e documenti sanitari, provenienti da banche dati ed Excel. La cancellazione dei dati avviene su richiesta, con informativa all'interessato in almeno un caso.

5. Misure tecniche e organizzative

Un utente spegne il PC in caso di assenza; non risulta confermato il blocco automatico su tutte le postazioni. Le password sono conservate in un file sul PC. Un utente dichiara di condividere la propria password con i colleghi, mentre un altro dispone del blocco automatico con richiesta password.

6. Ruoli e formazione

L'attività si svolge in sede. I ruoli sono descritti anche nel mansionario privacy. Un utente non ha ricevuto formazione specifica sul trattamento dei dati personali, mentre l'altro dichiara di sapere come comportarsi.

Tabella di sintesi: rischi e soluzioni

Area	Rischio rilevato	Soluzione consigliata
Dispositivi	Un utente su due opera ancora su Windows 10 (fine supporto)	Pianificare l'aggiornamento del sistema operativo o l'adozione di misure compensative
Password	Un utente condivide la propria password con i colleghi; le password sono salvate in un file sul PC	Adottare un password manager e vietare la condivisione di credenziali personali
Blocco dispositivo	Non risulta configurato il blocco automatico su tutte le postazioni	Impostare il blocco automatico dello schermo su ogni dispositivo
Dati particolari	Trattati dati sanitari e di contatto senza una procedura dedicata	Definire una procedura specifica per le categorie particolari di dati (art. 9 GDPR)
Condivisione file	File inviati a clienti/colleghi tramite	Adottare uno strumento aziendale di

	WhatsApp e WeTransfer, senza canale aziendale controllato	condivisione file tracciato e sicuro
Strumenti IA	Uso di ChatGPT non censito ufficialmente tra gli strumenti aziendali	Definire una policy interna sull'uso di strumenti di intelligenza artificiale
Formazione	Un utente su due non ha ricevuto formazione specifica sulla privacy	Programmare una formazione periodica obbligatoria in materia GDPR

Raccomandazioni prioritarie

- Vietare la condivisione delle password personali tra colleghi e adottare un password manager aziendale
- Configurare il blocco automatico dello schermo su tutte le postazioni
- Sostituire i canali di condivisione file non controllati (WhatsApp, WeTransfer) con uno strumento aziendale tracciato
- Formalizzare una procedura per il trattamento dei dati sanitari e di contatto
- Pianificare l'aggiornamento dei dispositivi con Windows 10
- Erogare formazione GDPR a tutto il personale, inclusi gli utenti privi di formazione specifica
- Definire una policy interna sull'uso di strumenti di intelligenza artificiale non ufficiali