



PRIVACY

cenni operativi per sapersi orientare

DI COSA PARLIAMO QUANDO PARLIAMO DI PRIVACY?



Parliamo di privacy ogni volta che prendiamo in considerazione informazioni e/o dati che si riferiscono a persone fisiche identificate o identificabili.

Pertanto **la privacy ci riguarda**

come soggetti i cui dati vengono gestiti da altri (provate a pensare a quante spunte privacy mettete ogni volta che navigate in internet).

come soggetti che trattano dati personali (nel ruolo di dipendenti comunali)

DI COSA PARLIAMO QUANDO PARLIAMO DI PRIVACY?



Le tipologie di dati trattati all'interno di un comune sono moltissime e possono essere diverse a seconda degli uffici in cui lavoriamo.

Tutti gli uffici trattano dati personali,

perché i dati personali sono

un nome e cognome, una data di nascita, un codice fiscale, un indirizzo fisico, un indirizzo di mail, un numero di telefono, un numero di targa, un'immagine o un video che riprende persone che sono riconoscibili.

LA NORMA DI RIFERIMENTO



General Data
Protection
Regulation, ovvero il
Regolamento della
Protezione dei Dati
entrato in vigore il
25 maggio 2018

LA NORMA DI RIFERIMENTO



LA NORMA DI RIFERIMENTO



MODELLO ORGANIZZATIVO PRIVACY

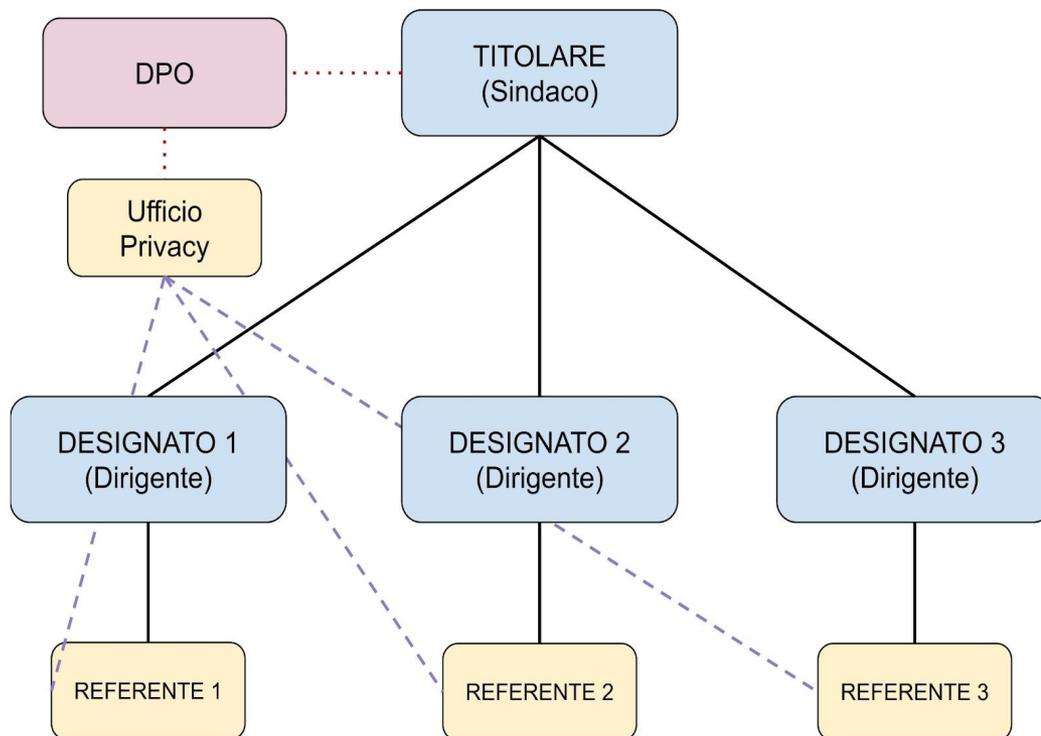


Il **TITOLARE** nomina dei suoi delegati (i designati).

I **DESIGNATI** a loro volta nominano un referente privacy e gli **AUTORIZZATI**.

I **REFERENTI PRIVACY** fanno riferimento ad un ufficio centrale, l'Ufficio Privacy, che li coordina.

Il **DPO** usa la rete composta dall'Ufficio privacy, dai referenti e dai designati per intervenire sulla struttura.



L' AUTORIZZATO AL TRATTAMENTO



TUTTI I DIPENDENTI
a tempo indeterminato, determinato, CFL,
volontari, interinali, servizio civile, alternanza
scuola lavoro ecc.

[Atto di nomina ad autorizzati](#): tutti voi dovrete aver ricevuto tale atto di nomina e lo dovrete ricevere in caso di cambio di Dipartimento/Divisione, essendo differenti i trattamenti dati che verrete ad operare.

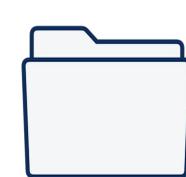
NON TUTTI I POSTI SONO UGUALI



Salviamo dati e documenti in continuazione e in moltissimi punti:

- applicativi gestionali (DOQUI, STILO, IRISWEB)
- share di rete
- mail
- google drive
- desktop del pc
- cellulari (personali e di servizio)
- chiavette o hard disk esterni

...e non dimentichiamo la carta



PROTEGGERE I DATI



I dati personali che trattiamo e gestiamo vanno protetti: il luogo in cui li salviamo condiziona le azioni per proteggerli.

Partiamo dalla carta.

Alcune buone pratiche:

- riporre documenti e fascicoli in armadi e cassetti
- non lasciare pratiche che possano essere lette da terze persone che per qualsiasi ragione si trovano a venire nel nostro ufficio (cittadini, fornitori, colleghi di altri uffici, ecc)
- non lasciare post-it con numeri di telefono, password ecc

PROTEGGERE I DATI



Dati in formato digitale

Il luogo più sicuro e deputato alla conservazione dei dati sono gli applicativi gestionali (trasversali o specifici degli uffici).

Altro ambito di salvataggio sono sono gli spazi di “collaboration” come le share di rete o i drive condivisi.

...ma su questo tema e sulla cybersecurity ne parlerete tra poco con il mio collega



ALCUNE BUONE PRATICHE: il computer



Ricordarsi di ripulire da file non più in uso il desktop del computer.
In generale evitare di salvare sul desktop troppi documenti per troppo tempo.

IL BUCO NERO dei dati personali nei nostri computer sono 2

la cartella download

la cartella cestino

RICORDATEVI DI PULIRLE/SVUOTARLE PERIODICAMENTE

ALCUNE BUONE PRATICHE: portatili e smartphone



Se vi viene dato in uso un computer portatile o un cellulare di servizio (o altro device aziendale)

ricordate che dovete averne cura, non solo per il valore dello strumento in sè, ma anche per tutti i dati e le informazioni che potrebbe contenere.

Impostare password o PIN

Per i cellulari le chat di WA o Telegram non dovrebbero essere usate per lo scambio di documenti contenenti dati personali. Nel qual caso si consiglia periodicamente la pulizia

ALCUNE BUONE PRATICHE: applicativi web gratuiti



Non utilizzare mai applicativi “FREE” su web se prevediamo di caricare dati personali o documenti contenenti dati personali.

Solitamente i programma FREE:

- non rispondono alle norme del GDPR (anche perché spesso risiedono fuori dallo spazio UE)
- in cambio della loro gratuità si tengono i nostri dati, come per esempio i social network

**ATTENZIONE A COME
USIAMO LA AI**



ALCUNE BUONE PRATICHE: le mail



Ogni giorno nel mondo vengono inviate circa 361 miliardi di email.

La mail è un mezzo che fa parte della nostra quotidianità ed è uno dei principali strumenti di lavoro.

Bisogna però prestare molta attenzione all'uso della mail, perché il loro contenuto (TESTO E ALLEGATI), o anche solo gli INDIRIZZI sono di fatto dati personali.



ALCUNE BUONE PRATICHE: le mail



Il contenuto dei messaggi di posta elettronica (allegati inclusi) è una forma di corrispondenza che si avvale di garanzie di segretezza costituzionalmente tutelate.

Senza una volontà esplicita o chiaramente desumibile dagli elementi di contesto, la corrispondenza non può essere oggetto di diffusione o di comunicazione a terzi. Sarebbe come aprire una lettera presa dalla buca delle lettere del vicino o della vicina di casa.

ATTENZIONE AGLI INOLTRI (sia all'interno che all'esterno dell'Ente): il

Garante ha più volte sanzionato il semplice inoltrato di e-mail, considerato come un vero e proprio trattamento illecito dei dati personali.

L'operazione di comunicazione di dati personali a terzi, da parte di soggetti pubblici, è ammessa solo quando prevista da una norma di legge.

ALCUNE BUONE PRATICHE: le mail



Come conciliare le aspettative di riservatezza del mittente con le esigenze di servizio o le funzioni istituzionali dell'ente?

Alcuni accorgimenti:

- 1) valutare sempre se il contenuto della e-mail e/o degli allegati contenga dati personali che siano necessari e non eccedenti rispetto alla finalità della conversazione
- 2) ricontrollare sempre i destinatari delle e-mail nei campi “rispondi”, “rispondi a tutti” e “cc”, per evitare invii massivi o indiscriminati
- 3) valutare se si è autorizzati all'inoltro della e-mail ad altri destinatari all'insaputa delle persone che hanno preso parte alla conversazione
- 4) utilizzare con criterio la funzionalità “ccn” onde evitare una diffusione di dati personali

ALCUNE BUONE PRATICHE: allo sportello



Per chi si trova a lavorare allo sportello, è necessario prestare molta attenzione.

Non solo va protetta la privacy della persona che abbiamo di fronte, ma spesso anche di quella che si è appena allontanata.

Non lasciare pratiche in vista che potrebbero essere lette da altri utenti

Non fare riferimenti che possano essere sentiti da persone non interessate dalla pratica

Usare un livello di voce adeguato e consono per evitare che terzi possano sentire informazioni personali di altri utenti

VIOLAZIONE DI DATI PERSONALI



La violazione di dati personali comporta una perdita, anche temporanea, di

INTEGRITA'
RISERVATEZZA
DISPONIBILITA'



Quando avviene deve esserne data TEMPESTIVA comunicazione al referente privacy, al designato e al DPO.

VIOLAZIONE DI DATI PERSONALI



- Pubblicazione (o indicizzazione sui motori di ricerca) di dati non essenziali o senza autorizzazione
- Invio di una mail contenente dati personali ad un destinatario sbagliato (o con i destinatari in chiaro invece che in CCN)
- Inoltro di una mail a un destinatario non autorizzato ad accedere ai dati contenuti



- Furto di cellulare o computer (contenente dati personali)
- Furto o smarrimento delle PW del computer e conseguente accesso non autorizzato
- Attacco hacker e furto di dati

VIOLAZIONE DI DATI PERSONALI



A chi deve essere comunicata la violazione di dati personali?

La violazione va comunicata tempestivamente al referente e al designato per la raccolta dei dati essenziali.

Il tutto va poi segnalato all'ufficio privacy e al DPO per le successive azioni:

- A. interventi per porre rimedio
- B. inserimento nel registro delle violazioni
- C. valutazione del rischio
- D. notifica al Garante della Privacy (dipende da C)
- E. notifica agli interessati (dipende da C)

ABBIAMO 72 ORE PER FARE TUTTO



IL BUON SENSO NON BASTA, MA AIUTA

Per dubbi, domande, confronti scrivere a

rpd-privacy@comune.torino.it

Grazie dell'attenzione

Dr. Roberto Breviario