Istruzioni operative per la protezione dei dati personali non destinati alla diffusione e sulle relative misure di sicurezza informatiche.

Quelle che seguono sono le direttive a carattere operativo dettate dal SIRIT (Sistemi Informativi, Reti e Innovazione Tecnologica) della Città Metropolitana di Roma Capitale cui tutti i dipendenti devono attenersi tenuto conto delle attuali norme in materia di protezione dei dati personali.

1. Sistema di autenticazione informatica

a) **Segretezza password**: è indispensabile adottare le **necessarie cautele** per assicurare la segretezza della componente riservata (password) delle credenziali di accesso agli strumenti informatici atti al trattamento di dati personali.

b) **Segretezza password in caso di prolungata assenza dal servizio**: devono essere impartite **idonee e preventive disposizioni scritte** volte a individuare chiaramente le modalità con le quali viene assicurata la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente, per iscritto, i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

c) **Lunghezza password**: laddove i sistemi di autenticazione informatica non ne impongano una lunghezza minima, devono essere composte da **almeno otto caratteri** o nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.

d) **Gestione password**: **non deve contenere riferimenti** agevolmente riconducibili all'utente e deve essere **modificata almeno ogni sei mesi**. Se si viene dotati di una password standard per il primo accesso ad un applicativo, va **cambiata dopo il primo utilizzo**.

e) **Trattamento di dati sensibili e giudiziari**: in caso di trattamento di dati sensibili (dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale) e di dati giudiziari, la parola chiave deve essere **modificata almeno ogni tre mesi**.

f) **Credenziali inutilizzate**: le credenziali di autenticazione non utilizzate da almeno sei mesi vengono **di norma disattivate**, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. In tal evenienza occorre contattare il gestore dell'applicativo.

Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

2. Utilizzo postazione informatica

a) **Custodia**: la postazione informatica che si sta utilizzando **non va mai lasciata incustodita e accessibile**. Tale inadempienza risulta grave se avviene durante una sessione di trattamento di dati personali. Si consiglia di impostare un **salvaschermo con password** o meglio **bloccare manualmente il computer** quando si lascia incustodita la propria postazione (<Ctrl-Alt-Canc → Blocca computer> sui sistemi Windows).

b) **Antivirus**: ogni computer collegato alla rete intranet è protetto da un antivirus **centralizzato**. Controllare periodicamente tramite l'icona sullasystem tray (area in basso a destra sui sistemi Windows) l'esecuzione dello stesso sulla macchina e che la data di aggiornamento del database dei virus sia recente.

c) **Software**: è fatto **divieto** ad ogni utente **di installare sul computer** ad esso assegnato **programmi non autorizzati** dal SIRIT o dal proprio Dirigente. Se autorizzato, l'utente deve essere in possesso della licenza di utilizzo di detto software.

3. Salvataggio dei dati (backup)

a) **Dati che risiedono sui server centrali**: **sistemi automatici** si occupano del backup di tutti i dati che risiedono sui server centrali del CED (Centro Elaborazione Dati) gestito dal SIRIT.
b) Dati che non risiedono sui server centrali: i dati che risiedono sui computer (server e non) dislocati non centralmente presso i singoli uffici **devono essere periodicamente (almeno settimanalmente) salvati su supporti rimovibili** (floppy disk, CD o DVD scrivibili, pendrive USB, Hard Disk esterni, ecc.) e conservati in un ambiente separato e fisicamente distante dal luogo in cui si trovano i dati originali (almeno due copie e due luoghi diversi) in armadi chiusi a chiave. **Deve essere espressamente motivato ed autorizzato lo spostamento di dati sensibili al di fuori degli uffici dell'amministrazione**.
c) **Durata conservazione backup**: i **tempi** di conservazione delle copie di sicurezza debbono essere **congrui con le necessità del trattamento**. Qualora le copie di sicurezza debbano essere conservate per un lungo periodo, è necessario verificare periodicamente la loro integrità e leggibilità alla luce anche delle innovazioni tecnologiche.

4. Cartelle condivise sui server del CED

a) **Richieste**: la creazione di cartelle condivise sui server del CED presso il SIRIT deve necessariamente essere richiesta fornendo determinate informazioni. A tale scopo è stato predisposto un **apposito modulo**, richiedibile tramite l'indirizzo e-mail riportato in calce. Su tale modulo dovrà essere indicato:
- Il nominativo di ogni singolo dipendente che avrà accesso alla cartella (già designato come incaricato-autorizzato ai sensi del Regolamento UE n. 679/2016 art. 4 n. 10, 24 e 32 e del Codice della Privacy - d.lgs. 196/2003 e ss.mm. e ii. art. 2-quaterdecies nell'ipotesi che la archiviazione e/o visualizzazione e/o elaborazione etc. delle informazioni registrate nella cartella configuri un trattamento di dati personali così come definito dall'art. 4 del Regolamento UE n. 679/2016 e dal Codice della Privacy e ss.mm. e ii.);
- Il nominativo del dipendente che avrà il ruolo di **amministratore** (soggetto preposto alla gestione delle utenze, dei profili di accesso, etc. e già designato come incaricato- autorizzato/amministratore - ai sensi del Codice della Privacy e ss.mm. e ii. e dei provvedimenti del Garante - nell'ipotesi sopracitata).

b) **Trattamento di dati personali**: in tale ipotesi, art. 4 del Regolamento UE n. 679/2016 e Codice della Privacy e ss.m.e ii (registrazione, archiviazione, visualizzazione, elaborazione di dati, etc.), le attività espletate dagli utenti della cartella e dall'amministratore dovranno essere eseguite secondo le **modalità previste dalla normativa vigente in materia di tutela della riservatezza** (adozione di misure di sicurezza adeguate, ai sensi del Regolamento UE n. 679/2016, di misure e cautele previste dai provvedimenti del Garante, là dove coerenti con il citato regolamento europeo, adozione di quanto previsto dal Regolamento dell'Ente per il trattamento dei dati sensibili e giudiziari e dall'Ordinanza Presidenziale n. 274/P del 2005, là dove coerenti con il suddetto regolamento europeo).
c) **Ricognizione cartelle condivise**: si approfitta della presente per chiede a tutti i Servizi di effettuare una ricognizione delle proprie cartelle condivise, **controllandone contenuti e autorizzazioni**.

Chiarimenti

È possibile utilizzare il seguente indirizzo di posta elettronica: app.sirit@provincia.roma.it

Riferimento normativo

-Regolamento UE N. 679/2016
-d. lgs. n. 196/2003 e ss.mm.e.ii. – Codice della privacy

Trattamento dati senza l'ausilio di strumenti elettronici.

Gli Incaricati sono tenuti a custodire diligentemente gli atti e i documenti contenenti dati personali affinché essi siano preservati da danneggiamenti e/o smarrimenti ed a operare in modo da consentire l'accesso esclusivamente:

- all'Interessato a cui tali dati si riferiscono;
- al Responsabile del trattamento di quella tipologia di dato;
- agli altri incaricati a trattare quella tipologia di dato.

A tal fine, per evitare accessi non autorizzati è richiesto che:

1 I documenti contenenti dati personali, siano custoditi in archivi adeguatamente protetti, per evitare la lettura e/o il prelievo non autorizzato dei documenti, garantendo, quindi, la riservatezza e l'integrità dei dati in essi contenuti (es. armadi o cassetti chiusi a chiave);

2 Le chiavi siano riposte in un luogo sicuro e non lasciate nelle serrature stesse;

3 I documenti contenenti dati personali prelevati dagli archivi per l'attività quotidiana, siano in essi riposti a fine giornata e trasferiti presso gli archivi centrali quando non più operativamente necessari;

4 I documenti contenenti dati personali non rimangano incustoditi su scrivanie o tavoli di lavoro, soprattutto se accessibili al pubblico;

5 I documenti contenenti dati personali non siano condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (anche se queste persone sono a loro volta incaricate del trattamento);

6 Qualora sia necessario distruggere i documenti contenenti dati personali, questi vengano distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, siano sminuzzati in modo da non essere più ricomponibili;

7 L'archiviazione dei documenti cartacei contenenti dati sensibili e/o giudiziari avvenga in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave;

8 La conservazione dei dati che rivelano lo stato di salute e la vita sessuale sia effettuata separatamente da ogni altro dato personale trattato per finalità che non richiedano il loro utilizzo.

I dati personali archiviati su supporti di tipo magnetico e/o ottico devono essere protetti con le stesse misure di sicurezza previste per i supporti cartacei.

La riproduzione di documenti contenenti dati personali sensibili su supporti non informatici (ad esempio fotocopie) è vietata se non espressamente autorizzata preventivamente e specificatamente dal Responsabile competente o se richiesta dall'interessato. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.