Società Cooperativa Sociale Il Cerchio

ISTRUZIONI
AGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI E DELLE CATEGORIE PARTICOLARI DI DATI

In ottemperanza alle disposizioni del Regolamento Europeo 2016/679 ed in relazione alle attività svolte nell'ambito della Struttura l'"AUTORIZZATO", dovrà effettuare i trattamenti di dati personali di competenza attenendosi scrupolosamente alle seguenti istruzioni e ad ogni ulteriore indicazione, anche verbale, che potrà essere fornita dal TITOLARE
I dati personali devono essere trattati:
a) in osservanza dei criteri di riservatezza;
b) in modo lecito e secondo correttezza;
c) per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
d) nel pieno rispetto delle misure di sicurezza, custodendo e controllando i dati oggetto di trattamento in modo da evitare i rischi, anche accidentali, di distruzione o perdita, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

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. Le misure di sicurezza applicate alle copie o alle riproduzioni dei documenti contenenti dati personali devono essere identiche a quelle applicate agli originali.

1.1 CUSTODIA

I documenti contenenti dati personali, devono essere custoditi in modo da non essere accessibili a persone non incaricate del trattamento (es. armadi o cassetti chiusi a chiave).
I documenti contenenti dati personali che vengono prelevati dagli archivi per l'attività quotidiana devono esservi riposti a fine giornata.
I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

1.2 COMUNICAZIONE

L'utilizzo dei dati personali deve avvenire in base al principio del "need to know" e cioè essi non devono essere condivisi, comunicati o inviati a persone che non ne necessitano per lo svolgimento delle proprie mansioni lavorative (I dati non devono essere comunicati all'esterno della struttura e comunque a soggetti terzi se non previa autorizzazione).

1.3 DISTRUZIONE

Qualora sia necessario distruggere i documenti contenti dati personali, questi devono essere distrutti utilizzando gli appositi apparecchi "distruggi documenti" o, in assenza, devono essere sminuzzati in modo da non essere più ricomponibili.
I supporti magnetici od ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati. Se ciò non è possibile, essi devono essere distrutti.

1.4 Ulteriori istruzioni in caso di trattamento di categorie particolari di dati (dati sensibili e/o giudiziari):
I documenti contenenti tali dati devono essere controllati e custoditi dagli Autorizzati in modo che non vi accedano persone prive di autorizzazione. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione/amministrazione del personale di dati relativi a permessi sindacali, assenze per malattie ecc., deve avvenire per il tempo

strettamente necessario alla digitazione stessa e, subito dopo, i documenti devono essere archiviati in base alle presenti istruzioni.
L'archiviazione dei documenti cartacei contenenti dati sensibili o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.
Per accedere agli archivi contenenti categorie particolari di dati fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Titolare oppure farsi identificare e registrare su appositi registri.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 Gestione delle credenziali di autenticazione

l'accesso alle procedure informatiche che trattano dati personali è consentito agli Autorizzati in possesso di "credenziali di autenticazione" che permettano il superamento di una procedura di autenticazione. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'Incaricato (user-id) associato ad una parola chiave riservata (password), oppure in un dispositivo di autenticazione (es. smart card).
Gli Autorizzati devono utilizzare e gestire le proprie credenziali di autenticazione attenendosi alle seguenti istruzioni:
Le user-id individuali per l'accesso alle applicazioni non devono mai essere condivise tra più utenti (anche se Autorizzati al trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Titolare del trattamento.
Gli strumenti di autenticazione (ad esempio le password) che consentono l'accesso alle applicazioni devono essere mantenute riservate. Essi non vanno mai condivisi con altri utenti (anche se Autorizzati al Trattamento).
Le password devono essere sostituite, a cura del singolo Autorizzato, al primo utilizzo e successivamente almeno ogni sei mesi.
Le password non devono contenere riferimenti agevolmente riconducibili all'Autorizzato (es. nomi di familiari) e devono essere scelte nel rispetto delle istruzioni indicate al successivo punto 3.

2.2 Protezione del PC e dei dati

Tutti i PC devono essere dotati di password rispondenti alle predette istruzioni
Tutti i PC devono essere dotati di software antivirus aggiornato costantemente
Sui PC devono essere installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle Strutture di appartenenza. Sono vietati i software scaricati da Internet o acquisiti autonomamente.
Per evitare accessi illeciti, deve essere sempre attivato il salva schermo con password.
Sui PC devono essere installati, appena vengono resi disponibili (e comunque almeno annualmente), tutti gli aggiornamenti software necessari a prevenirne vulnerabilità e correggerne i difetti.
Deve essere effettuato, con cadenza almeno settimanale un salvataggio di back-up di eventuali dati personali presenti unicamente sul PC personale (cioè non accessibili tramite i sistemi informatici della struttura).
I supporti di memoria utilizzati per il back-up devono essere trattati secondo le regole definite al punto "Trattamento senza l'ausilio di strumenti elettronici".

2.3 Cancellazione dei dati dai PC

I dati personali conservati sui PC devono essere cancellati in modo sicuro (es. formattando i dischi) prima di destinare i PC ad usi diversi.

2.4 Ulteriori istruzioni in caso di trattamento di categorie particolari di dati (dati sensibili e/o giudiziari)

Le password di accesso alle procedure informatiche che trattano dati sensibili e/o giudiziari devono essere sostituite, da parte del singolo incaricato, almeno ogni tre mesi.

L’installazione degli aggiornamenti software necessari a prevenire vulnerabilità e correggerne i difetti dei programmi per elaboratori deve essere effettuato almeno semestralmente.

3. ISTRUZIONI DI CARATTERE GENERALE

Come scegliere e usare la password

- Usare almeno 8 caratteri,
- Usare lettere, numeri e almeno un carattere “speciale” ad es.: ?. ; $! @ - > < ·
- Non utilizzare date di nascita, nomi o cognomi propri o di parenti. Non sceglierla uguale alla matricola o alla user-id
- Memorizzare la password per evitare che il supporto in cui è scritta vada perso o sia accessibile da terzi.
- Non divulgarla a terzi
- Non condividerla con altri utenti

Come comportarsi in presenza di ospiti o di personale di servizio

- Fare attendere gli ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e attivare il salvaschermo del PC.
- Non rivelare o fare digitare le password dal personale di assistenza tecnica.
- Non rivelare le password al telefono né inviarla via fax: nessuno è autorizzato a chiederle.
- Segnalare qualsiasi anomalia al Titolare.

Come gestire la posta elettronica e **Internet**

- Non aprire messaggi con allegati di cui non si conoscono l’origine, possono contenere virus in grado di cancellare i dati sul PC.
- Evitare di aprire filmati e presentazioni non attinenti l’attività lavorativa per evitare situazioni di pericolo per i dati contenuti sul vostro PC.

Come usare correttamente Internet

- Evitare di scaricare dalla rete file e software di uso non direttamente riferibile all’attività di lavoro, in quanto questo può essere pericoloso per i dati e la rete della Struttura. I software necessari all’attività lavorativa vanno richiesti alla Struttura
- Usare Internet solo per lavoro, i siti web spesso nascondono insidie per i visitatori meno esperti.
- Non leggere le caselle personali esterne via webmail in quanto alcuni provider esterni non proteggono dai virus.

Violazioni di dati personali (cd. “Data Breach”)

L’autorizzato deve informare immediatamente il Titolare di ogni violazione della sicurezza di cui abbia cognizione, che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai Dati Personali trasmessi, conservati o comunque trattati, tramite compilazione dell’apposito modulo di “descrizione della violazione dei dati “nei campi di spettanza

L’autorizzato dovrà prestare ogni necessaria collaborazione al Titolare in relazione all’adempimento degli obblighi sullo stesso gravanti di notifica delle suddette violazioni all’Autorità ai sensi dell’art. 33 del GDPR o di comunicazione della stessa agli interessati ai sensi dell’art. 34 del GDPR.