Ministero dell'Istruzione dell'Università e Ricerca

C.P.I.A. 3 TORINO
Centro Provinciale Istruzione Adulti
Via Ponchielli n. 18 bis – 10024 MONCALIERI (TO)
C.F. 94071240017 - C.M. TOMM32500B
TEL. 011-6822922 – TOMM32500B@ISTRUZIONE.IT - TOMM32500B@PEC.ISTRUZIONE.IT

SEDE BRACCINI
TOCT701004
Corso Tazzoli 215/1
Torino
Tel. 011-3118386

SEDE CASTELLO MIRAFIORI
TOCT706007
Str. Castello di Mirafiori 55
Torino
Tel. 011-01133760

SEDE DI CHIERI
TOCT71000V
Via Santa Clara 8
Chieri
Tel. 011-9428480

SEDE DI MONCALIERI
TOCT71100P
Via San Matteo 14
Moncalieri
Tel. 011-6060475

SEDE I.P.M. FERRANTE APORTI
TOEE70601G
Via Berruti e Ferrero 3
Torino
Tel. 011-6194201
Fax 011-6194249

SEDE DI CARMAGNOLA
TOCT71800D
C.so Sacchirone 47
Carmagnola (TO)

C.P.I.A. 3 TORINO - -MONCALIERI
Prot. 0000146 del 10/01/2019
(Uscita)

Istruzioni per il trattamento dei dati ai sensi del Regolamento UE 679/2016 e del decreto legislativo n. 196/2003 e s.m.i.

Le presenti istruzioni costituiscono una serie organica di prescrizioni, orientate a garantire la sicurezza dei dati e delle informazioni detenute dall' Istituto CPIA 3 TORINO.

Tali prescrizioni devono intendersi come istruzioni impartite dal titolare del trattamento ai sensi dell'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati e autorizzati) del D.Lgs. 196/03 e s.m.i.

Lo scopo delle prescrizioni è quello di garantire un livello di sicurezza adeguato al rischio ai sensi dell'art. 32 del GDPR, tenendo conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

Principi generali

Il trattamento dei dati deve avvenire secondo i principi generali di cui all'art. 5 del Regolamento UE 679/2016, secondo i quali i dati personali sono:

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

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

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

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («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 («integrità e riservatezza»).

Segreto professionale e riservatezza

Il trattamento dei dati deve avvenire nel rispetto del segreto professionale.

I soggetti "designati" e quelli "autorizzati" al trattamento dei dati non possono divulgare, pubblicare o comunicare in alcun modo a terzi, direttamente o indirettamente, in toto o in parte, le informazioni apprese in occasione dello svolgimento delle mansioni per le quali sono stati incaricati, né potranno usarle, sfruttarle o disporne in proprio o tramite terzi o per finalità eccedenti rispetto a quelle per le quali sono stati raccolti o trattati.

Inoltre, il trattamento dei dati da parte dei soggetti "designati" e di quelli "autorizzati" al trattamento dei dati deve avvenire garantendo la riservatezza dei dati.

Premesso che per "informazioni riservate" si intendono tutte le informazioni di qualsivoglia natura riferite o apprese in occasione dello svolgimento di mansioni per le quali il soggetto è stato incaricato, ne deriva che i soggetti "designati" e quelli "autorizzati" al trattamento dei dati si impegnano a:

- considerare le informazioni riservate come strettamente private e riservate e ad adottare tutte le misure necessarie per non pregiudicare la riservatezza di tali informazioni;
- utilizzare le informazioni riservate unicamente allo scopo di effettuare lo svolgimento dell'attività cui sono preposti e di conseguenza a non usare tali informazioni in alcun modo né per alcun altro scopo di qualsiasi natura.

L'impegno di riservatezza si protrarrà anche dopo la cessazione del rapporto di lavoro o di collaborazione e sino a quando le informazioni in oggetto non saranno rese di pubblico dominio.

Misure di sicurezza per il trattamento dei dati senza l'ausilio di strumenti elettronici

Il trattamento dei dati senza strumenti elettronici coinvolge i dati contenuti in tutti i supporti cartacei o simili che non richiedano l'uso di elaboratori elettronici.

Ove esistano copie o riproduzioni di documenti che contengono dati personali, le medesime devono essere protette con le stesse misure di sicurezza applicate agli originali.

Criteri tecnici e organizzativi per la protezione delle aree e dei locali

I dati e le informazioni di carattere sensibile e/o giudiziario devono essere trattati in aree protette, anche fisicamente, dall'accesso di persone non autorizzate, in conformità a quanto previsto all'art. 9 del GDPR. Sono perciò individuati spazi, dotati di un sistema di controllo all'ingresso e di eventuali chiusure di sicurezza.

Il personale in servizio ha accesso ai locali esclusivamente per l'adempimento della prestazione lavorativa. Il personale che espleta servizi strumentali (es: pulizia dei locali) o si occupa della manutenzione e dei servizi accessori, deve essere espressamente autorizzato ad accedere alle aree di sicurezza.

Il personale dipendente ha accesso ai dati esclusivamente sulla base delle esigenze di servizio, conformemente ai seguenti principi:
- la necessità di trattamento;
- il minimo livello di conoscenza dei dati.

I soggetti "designati" e quelli "autorizzati" al trattamento dei dati personali devono vigilare affinché venga disciplinato e controllato l'accesso, il transito e la permanenza di persone estranee all'attività lavorativa nelle aree e nei locali adibiti a luoghi di lavoro, con particolare attenzione agli spazi in cui vengono custodite banche dati o dove vengono trattati dati sensibili o giudiziari. E' altresì loro compito vigilare sull'introduzione in tali aree di oggetti, apparecchiature, sostanze o materiali che possono favorire il sorgere di rischi.

Devono essere previsti accorgimenti per:
- consentire l'accesso alle aree dove vengono custoditi e trattati i dati al solo personale;
- ostacolare l'accesso abusivo ai dati;
- segnalare la presenza di intrusi.

Custodia

I documenti contenenti dati personali devono essere custoditi in modo da non essere accessibili alle persone non designate né autorizzate al trattamento, mediante localizzazione presso spazi con accesso riservato (es. armadi o cassetti chiusi a chiave).

I documenti contenenti dati personali, prelevati dagli archivi per l'attività quotidiana, devono essere ivi collocati al termine della giornata.

I documenti contenenti dati personali non devono rimanere incustoditi su scrivanie o tavoli di lavoro.

Comunicazione

La diffusione dei dati personali deve avvenire in base al principio della "minimizzazione", talché non devono essere condivisi, comunicati o inviati a soggetti o istituzioni che non ne abbiano bisogno per lo svolgimento delle funzioni lavorative, a prescindere dall'eventuale qualifica di responsabili o incaricati di altra struttura.

I dati personali non devono essere comunicati a soggetti terzi, se non previa autorizzazione da parte del titolare e per finalità strettamente connesse all'attività istituzionale.

Distruzione

Qualora sia necessario distruggere i documenti contenti dati personali questi devono essere soppressi mediante apparecchi "distruggi documenti" o, in assenza, attraverso modalità che impediscano qualsiasi ricomposizione.

Istruzioni per il trattamento di dati sensibili e/o giudiziari

I documenti contenenti dati sensibili e/o giudiziari devono essere sottoposti al controllo del designato al trattamento dei dati il quale, a sua volta, potrà avvalersi di ulteriori soggetti "designati" ed "autorizzati" per la custodia e/o il trattamento.

Il designato deve impedire l'accesso a persone prive di autorizzazione nei luoghi e nei momenti in cui si trattano dati sensibili e/o giudiziari.

Il trattamento di dati sensibili e/o giudiziari contenuti in documenti cartacei deve avvenire per il tempo strettamente necessario al trattamento, con successiva immediata archiviazione dei dati.

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

Misure di sicurezza per il trattamento dei dati con l'ausilio di strumenti elettronici

Utilizzo delle password

In caso di allontanamento dalla propria postazione informatica di lavoro, è fatto obbligo al dipendente di attivare il salva-schermo protetto da password.

Il dipendente dotato di credenziali di autenticazione si connette alla rete tramite autenticazione univoca personale.
Le credenziali di autenticazione alla rete devono essere custodite e preservate dalla conoscibilità di colleghi o soggetti esterni. In nessun caso devono essere annotate password in chiaro sia su supporto cartaceo che informatico.

I requisiti minimi di complessità delle password sono:
- redazione con caratteri maiuscoli e/o minuscoli;
- composizione con inclusione di simboli, numeri, punteggiatura e lettere;
- caratteri non inferiori a 8 (ad eccezione dei sistemi operativi che non supportano tali requisiti);
- password non agevolmente riconducibile all'identità del soggetto che la gestisce.

Pertanto la password non deve essere basata su informazioni personali, riferimenti familiari o comunque dati inerenti direttamente il soggetto titolare della password stessa.

Qualora l'intestatario della password ritenga che un soggetto non autorizzato possa essere venuta a conoscenza della propria password, dovrà provvedere immediatamente a cambiarla dandone comunque comunicazione all'amministratore di sistema.
Non debbono essere utilizzate nella configurazione delle caselle di posta elettronica le opzioni di "compilazione automatica" o "remember password", presenti nei browser o in altre applicazioni.

Utilizzo rete interna

La rete interna, istituita appositamente per permettere collegamenti funzionali tra utenti che prestano servizio all'interno della struttura lavorativa, non può esser utilizzata per scopi diversi da quelli ai quali è destinata. Qualora nella rete interna debbano circolare dati, notizie e informazioni aziendali, deve essere premura di ciascun dipendente preservare gli stessi dalla conoscibilità di terzi soggetti non espressamente autorizzati ad aver notizia di tali dati.

Utilizzo posta elettronica

E' fatto divieto di divulgare le notizie, i dati e qualsiasi altra informazione appresa in occasione della ricezione o invio di posta elettronica, in quanto coperte dal segreto professionale cui sono tenuti i dipendenti in ottemperanza agli obblighi di fedeltà e correttezza.
La posta elettronica diretta all'esterno della rete informatica aziendale può essere intercettata da estranei e, dunque, è preferibile non usarla per inviare documenti di lavoro "Strettamente Riservati".