Comune di Cameri

Provincia di Novara

CIRCOLARE N. 1 DEL 15/12/2022
AUTORIZZAZIONE AL TRATTAMENTO DEI DATI PERSONALI

Richiamato il Decreto del Sindaco n.9 del 15/12/2022
Vista la deliberazione di Giunta n.45 del 20/04/2022 di oggetto "Atto di adozione del registro dei trattamenti, di conferimento di poteri organizzativi e di autorizzazione in materia di trattamento dei dati personali".
Si comunica che i dipendenti del Comune di Cameri, di seguito definito Titolare del Trattamento dei dati ai sensi del Regolamento UE 2016/679 sono autorizzati al trattamento dei dati personali durante lo svolgimento delle proprie attività lavorative ai sensi dell'art. 2-quaterdecies del D.Lgs. 196/2003.
L'autorizzazione è relativa ai trattamenti di dati svolti negli ambiti lavorativi assegnati all'interno dell'organizzazione. La lista dei trattamenti relativi alle proprie assegnazioni lavorative ("Matrice Uffici/Trattamenti") è pubblicata in sito.
Qualsiasi attività lavorativa svolta dal soggetto è strumentale alle finalità perseguite dall'ente, per cui il trattamento di dati personali in tale contesto è autorizzato e dovrà sempre attenersi al principio di necessità, pertinenza e non eccedenza.
Per ogni trattamento il soggetto autorizzato dovrà relazionarsi al Titolare del Trattamento, tramite la PO designata all'area di appartenza, per tutti gli aspetti riguardanti la gestione in sicurezza dei dati.

Istruzioni specifiche sul trattamento dei dati

Si rammenta quanto disposto dall'art. 5 del Regolamento UE 2016/679. I dati personali oggetto di trattamento devono essere

- trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);
- 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»);
- adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

- 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»);
- 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»);
- 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»).

Inoltre si richiama particolare attenzione ai seguenti punti, aventi specifica attinenza con la sicurezza dei dati trattati:

- cautela in qualsiasi trattamento effettuato su dati personali;
- attenzione nella classificazione dei dati trattati, al fine di distinguere quelli per i quali è richiesta una cautela supplementare;
- trattamento esclusivo dei dati necessari all'attività lavorativa, astenendosi dal trattare i dati eccedenti le finalità.

Qualora nello svolgimento delle attività lavorative si dovesse venire a conoscenza di dati eccedenti l'autorizzazione al trattamento, occorre prontamente rivolgersi al Titolare per le opportune istruzioni.
Richieste eccedenti il proprio incarico dovranno essere prontamente segnalate al Titolare.
Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.
Inoltre occorrerà osservare scrupolosamente tutte le misure di sicurezza già in atto e quelle che saranno successivamente adottate dal titolare, nonché ogni ulteriore istruzione che sarà impartita in relazione a determinati trattamenti.
Infine si fa presente che tutte le disposizioni di futura emanazione correttive od integrative della normativa attualmente vigente in materia di protezione dei dati personali devono essere scrupolosamente osservate.
Le presenti indicazioni sono tassative.

Utilizzo dei supporti e degli strumenti di lavoro

Chiavi, uffici, scrivanie e armadi:

- E' necessario adottare tutte le cautele al fine di garantire la sicurezza dei dati trattati, a cominciare con il limitare l'accesso alle informazioni custodite.
- Qualora si disponga di chiavi di accesso agli uffici e alle sedi, è obbligatorio custodirle in sicurezza e segnalare immediatamente eventuali casi di furto o smarrimento.
- Nei casi in cui sia previsto dal servizio offerto, è necessario garantire il presidio degli uffici in cui si opera o chiudere a chiave gli uffici in caso di assenza.

- La scrivania e i tavoli di lavoro non devono mostrare in chiaro dati personali o informazioni riservate di cui possano venire a conoscenza visitatori occasionali. I documenti devono essere sempre presidiati o messi in sicurezza.
- I dati trattati devono essere custoditi in luoghi non accessibili a soggetti non autorizzati. La custodia in sicurezza può essere garantita attraverso la chiusura a chiave di armadi e/o interi locali.

Documenti e supporti, analogici e digitali:

- Durante l'attività lavorativa, è consentito solamente trattare soltanto i dati necessari, astenendosi dal trattare dati eccedenti le finalità.
- E' necessario procedere all'archiviazione definitiva, nei luoghi predisposti, dei supporti cartacei e dei supporti elettronici una volta terminate le attività di consultazione ed elaborazione.
- Occorre prestare attenzione ai documenti cartacei trattati tramite scanner, stampanti e fotocopiatrici: i supporti cartacei devono essere tolti prontamente da tali dispositivi, onde evitare che i documenti possano entrare in possesso di soggetti non autorizzati.
- I documenti cartacei non più utilizzati devono essere eliminati con macchine distruggi-documenti o ridotti a «coriandoli» che non rendano possibile la ricostruzione delle informazioni contenute.

Posta elettronica e internet:

- Non aprire messaggi di posta contenenti link, .zip, file eseguibili o contenenti macro.
- Non rispondere ai messaggi che propongono di disattivare l'invio di email successive, sono uno strumento di verifica di esistenza dell'email destinataria.
- Prestare cautele anche per i messaggi di utenti conosciuti, potrebbero loro aver contratto un malware.
- Non aprire comunicazioni contenenti sanzioni o cartelle esattoriali, avvisi di denuncia, ecc.
- Non aprire comunicazioni di consegna pacchi da parte di corrieri che contengano file "rischiosi".
- Verificare i link prima di aprirli, passandoci sopra con il mouse per vedere dove puntano veramente.
- Attenzione allo scrivere email in cc a molti indirizzi in contemporanea, si mette in conoscenza ognuno dei destinatari dell'indirizzo degli altri.
- Non inoltrare dati personali ad indirizzi di email personali (escono dal perimetro del Titolare) e non inviare dati «particolari»;
- Attenzione alla funzione di autocompletamento degli indirizzi dei destinatari.
- Verificare l'affidabilità dei siti visitati e tenere aggiornati i sistemi di protezione.
- Attenzione che l'utilizzo delle credenziali in dotazione venga effettuato nei corretti siti dedicati.
- Utilizzare piatteforme in cloud di file sharing solo se espressamente autorizzato dal Titolare.

Strumenti di elaborazione:

- La postazione di lavoro va spenta in casi di assenza prolungata (salvo eccezioni per motivate ragioni di servizio) o bloccata tramite la combinazione di tasti CTRL + ALT + CANC.
- Non lasciare incustoditi o accessibili a terzi non autorizzati la postazione di lavoro e gli strumenti elettronici mentre è in corso una sessione di lavoro.
- I sistemi di elaborazione devono sempre essere provvisti dei più recenti aggiornamenti di sicurezza e il soggetto autorizzato deve essere consapevole di quali dati sono sottoposti a backup e quali no.
- Se i notebook contengono documenti ed informazioni con dati personali, devono essere protetti da sistemi di cifratura.

- Se la posta viene consultata tramite smartphone, visto che le email possono contenere dati personali è necessario proteggerlo con sistemi di blocco. Prestare attenzione alle fotografie, che vengono salvate nelle memorie dei telefoni le quali possono essere accessibili in chiaro.
- E' possibile utilizzare dispositivi di proprietà (Bring Your Own Device - BYOD) per l'accesso ai dati di lavoro solo se tale utilizzo è espressamente autorizzato dal Titolare. Sul dispositivo dovranno essere applicate le medesime misure di sicurezza in uso per gli strumenti aziendali.
- Qualora un tecnico richieda di collegarsi alla postazione di lavoro tramite strumenti di controllo remoto, è indispensabile
    - verificare l'identità dell'operatore remoto (tramite conoscenza diretta o comunicazione preventiva)
    - controllare se è autorizzato allo svolgimento dell'intervento (tramite preventiva apertura di ticket, autorizzazione, ...)
    - presidiare la postazione durante l'intervento, a meno che non sia stato concordato diversamente.

Credenziali di accesso:

- Utilizzare password adeguatamente lunghe e complesse
- Non utilizzare password riconducibili alla propria realtà personale (data di nascita, nomi di parenti ecc)
- Cambiare le password secondo la frequenza prevista dagli standard di sicurezza
- Utilizzare credenziali differenti in contesti diversi, in modo da evitare che la violazione di una credenziale si possa «propagare» su altri perimetri di applicazione;
- Le credenziali personali di accesso ai sistemi non possono essere condivise e devono essere custodite in sicurezza (senza lasciarle scritte in prossimità della postazione di lavoro...).

Rapporto con soggetti terzi

- Prima di rilasciare documenti, dati o credenziali a soggetti terzi, verificare l'identità dei destinatari e la presenza di adeguate autorizzazioni al rilascio.
- Comunicare e/o diffondere solo i dati personali preventivamente autorizzati dal Titolare.
- Non fornire tramite email, fax, accesso remoto o telefonicamente dati, credenziali o accessi ai sistemi senza specifica e preventiva identificazione del richiedente e conseguente autorizzazione.
- In caso di richieste di informazioni o documenti confrontarsi prontamente con il referente del Titolare sul da farsi.
- Fornire agli interessati opportuna informativa quando richiesto dalla legge.

Incidenti di sicurezza

Qualora si riscontri un incidente di sicurezza sulle risorse informative del Titolare, che possa o meno sfociare in una violazione da notificare all'autorità Garante della Privacy, è necessario comunicarlo immediatamente al referente del Titolare, al fine di allestire prontamente adeguate misure di mitigazione del danno.

Interventi di emergenza che necessitino l'utilizzo di credenziali dell'incaricato

In caso di prolungata sua assenza o impedimento che renda indispensabile e indifferibile intervenire con le credenziali assegnate, per esclusive necessità di garantire la continuità dei servizi e/o la sicurezza dei dati, potrà essere consentito ad un soggetto specificamente designato l'accesso ai dati ed agli strumenti

informatici, tramite modifica delle password dell'utente. Non appena possibile il personale espressamente designato dall'azienda provvederà ad informare l'assegnatario delle credenziali dell'avvenuta procedura. Al suo rientro questi dovrà obbligatoriamente provvedere ad impostare nuove password di accesso.

Cameri,15.12.2022

Il Responsabile
Dell'Area Economico-Finanziaria
Dott.ssa Vecchio Tiziana

Il sottoscrittore dichiara di aver preso visione della Circolare N. 1 del 15.12.22 e delle istruzioni per il trattamento dei dati personali ivi contenute.

NOME, COGNOME	FIRMA