Allegato A alla Nomina

ISTRUZIONI AGLI INCARICATI DEL TRATTAMENTO DEI DATI PERSONALI COMUNI E PARTICOLARI.

Dipendenti dell'Area 2 P.E.F.

Responsabile del trattamento dati: Trinchero dott.ssa Livia

Dal 25 maggio 2018 è entrato in vigore il Regolamento generale sulla protezione dei dati (GDPR); si tratta delle nuove norme europee in materia di privacy che permetteranno di tutelare la gestione delle informazioni personali rese dai cittadini e dalle aziende tramite soggetti già individuati ai quali ne è assegnata la responsabilità:

- RPD (Responsabile protezione dati) anche denominato DPO (Data Protection Officer) è la figura introdotta dal Regolamento generale sulla protezione dei dati 2016/679 GDPR, con competenze giuridiche, informatiche, di risk management e di analisi dei processi. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno dell'Ente, affinché questi siano trattati nel rispetto delle normative privacy europee e nazionali.
- Il Titolare del trattamento (data controller) è l'autorità pubblica che determina le finalità e i mezzi del trattamento di dati personali" (art. 4. par. 1, n. 7 GDPR). In sostanza il titolare è colui che tratta i dati senza ricevere istruzioni da altri, colui che decide "perché" e "come" devono essere trattati i dati; per il Comune è il Sindaco pro-tempore.
- Il Responsabile del trattamento dati ai sensi dell'art. 4, par. n. 8 del Regolamento generale sulla protezione dei dati UE 2016/679 (GDPR) è la persona preposta a fornire le "garanzie sufficienti" per mettere in atto le misure tecniche ed organizzative adeguate nonché garantisca per la tutela dei diritti dell'interessato. E' in sostanza colui che è preposto al trattamento dei dati personali per conto del titolare del trattamento.
- L'incaricato o autorizzato del trattamento è colui il quale, sotto la diretta autorità del Titolare e del Responsabile del trattamento, dietro apposito atto di nomina e contestuale autorizzazione, effettua materialmente le operazioni di trattamento sui dati personali. La definizione legislativa di "incaricati" la troviamo, in primo luogo, all'art. 4, comma 1, lett. h) del D.Lgs. 196/2003 (Codice Privacy) ancora in vigore, che li identifica gli incaricati come "le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile".

In questa sede trattiamo le competenze e le responsabilità di competenza degli incaricati/autorizzati al trattamento.

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 minime 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.

Le misure minime di sicurezza (di cui agli artt. 33 - 36 ed allegato B del citato Dlgs. 196/03) sono obbligatorie e sono distinte in funzione delle seguenti modalità di trattamento dei dati:

1. **senza l'ausilio di strumenti elettronici** (es. dati in archivi cartacei o su supporto magnetico/ottico);
2. **con strumenti elettronici** (PC ed elaboratori).

1. TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI

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 (anche se queste persone sono a loro volta incaricate del trattamento). I dati non devono essere comunicati all'esterno 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.

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

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

1.4 Ulteriori istruzioni in caso di trattamento di dati sensibili e/o giudiziari

- I documenti contenenti dati sensibili e/o giudiziari devono essere controllati e custoditi dagli Incaricati 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 e/o giudiziari deve avvenire in locali ad accesso controllato, utilizzando armadi o cassetti chiusi a chiave.

- Per accedere agli archivi contenenti dati sensibili e/o giudiziari fuori orario di lavoro è necessario ottenere una preventiva autorizzazione da parte del Responsabile oppure farsi identificare e registrare su appositi registri.

2. TRATTAMENTI CON STRUMENTI ELETTRONICI

2.1 Gestione delle credenziali di autenticazione

La legge prevede che l'accesso alle procedure informatiche che trattano dati personali sia consentito agli Incaricati 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) o in una caratteristica biometrica. Gli Incaricati 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 Incaricati del trattamento). Nel caso altri utenti debbano poter accedere ai dati è necessario richiedere l'autorizzazione al Responsabile 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 Incaricati del trattamento).
- Le password devono essere sostituite, a cura del singolo Incaricato, al primo utilizzo e successivamente almeno ogni sei mesi.
- Le password devono essere composte da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Le password non devono contenere riferimenti agevolmente riconducibili all'Incaricato (es. nomi di familiari) e devono essere scelte nel rispetto della normativa interna comunicata dall'Amministratore di sistema sulla costruzione ed utilizzo delle password (vedi successivo punto 3.1).

2.2 Protezione del PC e dei dati

I dipendenti assegnatari di PC devono:

- Dotare il proprio account di password rispondenti alle normative disicurezza;
- Conservare in via esclusiva le password di accesso al proprio account;
- Lavorare esclusivamente su dati memorizzati sugli archivi di rete dei server; **è responsabilità del singolo dipendente la perdita di dati eventualmente conservati sul proprio PC;**
- In caso di allontanamento dalla postazione di lavoro, bloccare l'account "utente";
- Evitare l'utilizzo di software non autorizzati dall'Amministratore di sistema.

Relativamente al Sistema Informatico dell'Ente, si dichiara che:

- Tutti i PC sono dotati di software antivirus aggiornato costantemente e con la funzione "Monitor" attiva;
- Sui PC sono installati esclusivamente software necessari all'attività lavorativa, dotati di licenza e forniti dalle strutture di appartenenza.
- Con cadenza giornaliera vengono eseguiti i salvataggi di back-up dei dati presenti nei server.

2.3 Cancellazione dei dati dai PC

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

3. ISTRUZIONI DI CARATTERE GENERALE

Come scegliere e usare la password (Normativa sulla costruzione ed utilizzo delle password)

- Usare almeno 8 caratteri, o nel caso in cui lo strumento elettronico non lo permetta, usare un numero di caratteri pari al massimo consentito.
- Usare lettere, numeri e almeno un carattere tra quelli speciali (ess. . ; $! @ - > <) Non utilizzare date di nascita, nomi o cognomi propri o di parenti
- Non sceglierla uguale alla user-id (nomeutente)
- Custodirla sempre in un luogo sicuro e non accessibile a terzi
- Non divulgarla a terzi
- Non condividerla con altri utenti

Come comportarsi in presenza di utenti

- Fare attendere gli utenti in luoghi in cui non siano presenti informazioni riservate o dati personali.
- Se è necessario allontanarsi dalla scrivania in presenza di utenti, riporre i documenti e bloccare l'account del PC.

Come gestire la posta elettronica

- Non aprire messaggi con allegati di cui non si è certi dell'origine: possono contenere virus in grado di cancellare i dati sul PC.
- L'account di posta elettronica, per quanto "nominale", deve essere utilizzato solo per scopilavorativi.

Come usare correttamente Internet

- E' vietato scaricare dalla rete file e software di uso non direttamente riferibile all'attività di lavoro. I software necessari all'attività lavorativa vanno richiesti al proprio Responsabile di Servizio.
- Usare Internet solo per scopi lavorativi: 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.

4. SANZIONI PER INOSSERVANZA DELLE NORME

- Le presenti istruzioni sono impartite ai sensi delle normative vigenti in materia di privacy.
- L'inosservanza da parte dell'Incaricato può comportare sanzioni disciplinari e di natura penale, così come previsto dalla normativa vigente.

Per presa visione:

Francesca Brambilla