AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
"Giorgio Gasparini" Vignola (Modena)

NORME COMPORTAMENTALI PER GLI INCARICATI DEL TRATTAMENTO DI DATI PERSONALI

Approvate con deliberazione dell'Amministratore Unico n. 34 del 28.12.2017

AZIENDA PUBBLICA DI SERVIZI ALLA PERSONA
"GIORGIO GASPARINI" VIGNOLA

Enti Pubblici Soci: Unione di Comuni Terre di Castelli I Castelnuovo Rangone Castelvetro di Modena I Guiglia I Marano sul Panaro I Montese I Savignano sul Panaro Spilamberto I Vignola I Zocca

Via Libertà, 823 41058 Vignola (Mo)
T 059 770 5211
F 059 770 5200
M info@aspvignola.mo.it
W www.aspvignola.mo.it
PEC aspvignola@pec.it
C.F. / P.I. 03099960365

PREMESSA

Finalità della presente procedura è illustrare le norme comportamentali cui gli incaricati devono attenersi nello svolgimento delle operazioni di trattamento di dati personali.

In particolare la procedura descrive:

- I riferimenti normativi per la gestione delle nomine degli incaricati sulla scorta di quanto dispone l'art. 29 del D.Lgs n. 196 del 2003 (Codice Privacy);
- Le regole di ordinaria diligenza che gli incaricati del trattamento sono tenuti ad osservare nel corso della loro prestazione lavorativa;
- Le misure di sicurezza per gli archivi elettronici e cartacei da adottare per la protezione dei dati personali.

Sono inoltre messi in risalto gli aspetti relativi alle misure di sicurezza previste dall'allegato B) "Disciplinare Tecnico" al Codice della Privacy , che ciascun incaricato è chiamato ad adottare per dare piena applicazione a quanto disposto dalla normativa in materia.

La procedura si applica indistintamente agli incaricati interni ed anche esterni che si trovino ad operare su dati personali la cui titolarità è dell'ASP "Giorgio Gasparini".

INDICE DEGLI ARGOMENTI

- riferimenti normativi e glossario
- lettera d'incarico e istruzioni operative per gli incaricati
- trattamento dei dati personali da parte dell'incaricato/informativa
- dati personali oggetto del trattamento
- regole di ordinaria diligenza per l'incaricato
- misure per la protezione dei dati personali da osservarsi da parte dell'incaricato
- trattamenti senza l'ausilio di strumenti elettronici
- trattamenti con strumenti elettronici

RIFERIMENTI NORMATIVI E GLOSSARIO

Le presenti norme comportamentali sono emanate in applicazione della normativa contenuta nel D.Lgs n. 196 del 2003, Codice in materia di protezione dei dati personali, il cosiddetto" Codice della Privacy" che disciplina compiutamente le modalità da adottarsi per il trattamento dei dati personali, affinchè tale attività si svolga (art. 2 del Codice) nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Di seguito, ai sensi dell'art. 4 del Codice riportiamo alcune definizioni importanti per comprendere la materia in argomento:

a) per **trattamento** si intende qualunque operazione o complesso di operazioni effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'eleborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca dati.

b) Per **dato personale** si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

c) Per **dati sensibili** si intendono i 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.

d) Per **dati giudiziari** si intendono i dati personali idonei a rivelare i provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

e) **Titolare** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Nel nostro caso il Titolare è la stessa ASP in persona del suo Direttore "pro tempore".

f) **Responsabile** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo eventualmente preposti dal titolare al trattamento di dati personali, in caso di mancata nomina il Responsabile coincide con il Titolare.

g) **Incaricati** sono le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile, da noi i singoli dipendenti a tal fine delegati In particolare il Titolare del trattamento nomina quale incaricato, con puntuale indicazione dell'ambito di trattamento consentito, tutto il personale dell'ASP che, per le proprie mansioni, viene chiamato a gestire dati personali. Allo stesso modo coloro che, trovandosi temporaneamente a prestare un'attività ad esempio di volontariato o di tirocinio o di collaborazione, all'interno dell'ASP, debbano gestire dati personali, dovranno essere nominati dal Titolare "incaricati" e dovranno operare adottando le medesime modalità stabilite per gli incaricati interni.

h) **Interessato** è la persona fisica cui si riferiscono i dati personali.

i) **Comunicazione** è il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal titolare e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

j) **Diffusione** è il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

k) **Garante per la protezione dei dati personali** è l'autorità istituita dalla legge per assicurare la tutela dei diritti e delle libertà fondamentali e il rispetto della dignità nel trattamento dei dati personali. Fra i compiti assegnati al Garante vi sono:

- Controllare che i trattamenti siano effettuati nel rispetto delle norme di legge

- Ricevere ed esaminare i reclami e le segnalazioni e provvedere sui ricorsi presentati dagli interessati
- Vietare anche d'ufficio i trattamenti illeciti o non corretti ed eventualmente disporne il blocco
- Esprimere pareri nei casi previsti
- Denunciare i fatti configurabili come reati perseguibili d'ufficio conosciuti nell'esercizio delle sue funzioni
- Predisporre una relazione annuale sull'attività svolta da presentare al Governo e al Parlamento
- Organizzare il proprio ufficio ed il proprio organico

LETTERA D'INCARICO E ISTRUZIONI OPERATIVE PER GLI INCARICATI

Gli incaricati ricevono una formale lettera d'incarico/autorizzazione da parte del Responsabile del trattamento di riferimento.

Con tale lettera si impegna l'incaricato a:

1. collaborare con il Titolare/Responsabile del trattamento
2. utilizzare i dati solo per gli scopi istituzionali, nello spirito della legge e secondo le istruzioni scritte ricevute
3. rispettare il segreto d'ufficio e professionale, oltre che i requisiti di riservatezza e sicurezza durante l'uso dei dati personali

E' opportuno ribadire che la formalizzazione scritta dell'incarico è obbligatoria in quanto l'art. 30 impone, a coloro che compiano direttamente le operazioni di trattamento, di assumere il ruolo di incaricati.

TRATTAMENTO DEI DATI PERSONALI DA PARTE DELL'INCARICATO E INFORMATIVA

Una volta ricevuta la lettera di nomina e la conseguente autorizzazione, l'incaricato può svolgere materialmente il trattamento attenendosi alle istruzioni operative ricevute ed alle presenti norme comportamentali.

Ogni acquisizione di dati deve essere preceduta dall'informativa all'interessato, utilizzando, a tal fine, gli appositi moduli forniti ad ogni servizio, da illustrare e far firmare all'interessato stesso.
L'informativa deve sempre contenere i seguenti dati: identità e dati di contatto del titolare e del suo rappresentante, finalità e base giuridica del trattamento, categorie di destinatari dei dati, periodo di conservazione dei dati, menzione dei diritti dell'interessato, incluso il diritto a proporre reclamo all'Autorità di Controllo, indicazione se la comunicazione dei dati risponde ad un obbligo legale o contrattuale o è requisito necessario per potere usufruire di determinati servizi/prestazioni e conseguenze della mancata comunicazione dei dati.

Con il termine trattamento ci si riferisce ad una qualunque operazione effettuata sui dati (quali la raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modifica, selezione, estrazione, raffronto, utilizzo, interconnessione, blocco, comunicazione, diffusione, cancellazione e distruzione) svolta con o senza l'ausilio di mezzi automatizzati.

Il trattamento comprende dunque l'intera vita del dato personale, dal momento della raccolta a quello della distruzione, abbracciando operazioni di utilizzo interno ed esterno.

DATI PERSONALI OGGETTO DEL TRATTAMENTO

Per "dato personale" si intende qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
E' stato escluso, a decorrere dal 2011, il riferimento a dati relativi a persone giuridiche, che era contemplato nella normativa precedente.
I dati personali possono essere suddivisi in:

- dati personali "**ordinari**";
- dati personali "**sensibili**", con ciò intendendosi quelli 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;
- dati "**giudiziari**" quelli idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale.

La distinzione fra le varie tipologie di dati personali assume notevole rilevanza in quanto i trattamenti vengono disciplinati in maniera differenziata in ragione della diversa natura del dato personale oggetto di trattamento, riflettendosi anche sulle misure di sicurezza che dovranno essere adottate e sulle sanzioni applicabili in caso di violazione delle norme relative.

REGOLE DI ORDINARIA DILIGENZA PER L'INCARICATO

Nell'esecuzione dei compiti assegnati l'incaricato deve attenersi ad alcune regole di ordinaria diligenza al fine di evitare che soggetti estranei possano venire a conoscenza dei dati personali oggetto del trattamento.
Per queste ragioni l'incaricato, nello svolgimento delle proprie mansioni, deve prestare particolare attenzione nel:

- non divulgare a terzi estranei le informazioni di cui viene a conoscenza;
- adoperarsi affinché terzi non entrino in possesso fraudolentemente di dati;
- non fare copie per uso personale dei dati su cui svolge operazioni d'ufficio;
- attenersi scrupolosamente alle istruzioni ricevute;
- osservare criteri di riservatezza;
- trattare i dati in modo lecito e secondo correttezza;
- trattare i dati per un periodo di tempo non superiore a quello necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- comportarsi 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;
- qualora l'incaricato abbandoni temporaneamente la propria postazione di lavoro deve provvedere a:

a) fare attendere eventuali ospiti in luoghi in cui non siano presenti informazioni riservate o dati personali
b) riporre nei cassetti o negli armadi la documentazione cartacea contenente dati personali
c) se è necessario allontanarsi dalla scrivania in presenza di ospiti, riporre i documenti e spegnere il p.c. o renderlo accessibile solo tramite password
d) non rivelare le password al personale di assistenza tecnica
e) non rivelare le password al telefono né inviarle via fax o mail: nessuno è autorizzato a richiederle
f) segnalare qualsiasi anomalia o stranezza al proprio Responsabile

MISURE PER LA PROTEZIONE DEI DATI PERSONALI DA OSSERVARSI DA PARTE DELL'INCARICATO

L'art. 31 del D.Lgs 196/2003 stabilisce che i dati debbano essere custoditi e controllati in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.
A tal fine, la legge richiede l'adozione di una serie di misure minime di sicurezza, individuate negli artt. da 31 a 36 e dal disciplinare tecnico di cui all'allegato B al Decreto stesso.
La mancata adozione delle misure minime di sicurezza comporta una responsabilità penale, (ai sensi dell'art. 169) a carico del titolare del trattamento.
Gli incaricati del trattamento sono comunque obbligati al rispetto delle misure minime di sicurezza, pena l'applicazione di sanzioni anche a loro carico.
E' necessario, quindi, che gli incaricati osservino le norme comportamentali di seguito descritte, che discendono dalle normative sopra citate e sono distinte a seconda che il trattamento dei dati avvenga: 1) senza l'ausilio di strumenti elettronici (ad es. dati in archivi cartacei, o su supporto magnetico/ottico, quali pellicola fotografica, microfilm, cassetta VHS, dischetto, lastra o pellicola radiologica), o 2) con strumenti elettronici (ad es. P.C. ed elaboratori)

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 riproduzioni di documenti devono essere identiche a quelle applicate agli originali.

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 vengano 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 da lavoro.

Comunicazione

- I dati personali 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) (principio della stretta necessità di diffusione).
- I dati non devono essere comunicati all'esterno dell'ASP e comunque a soggetti terzi se non per previsioni di legge o previa autorizzazione.

Distruzione

- Qualora sia necessario distruggere i documenti contenenti 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 o ottici contenenti dati personali devono essere cancellati prima di essere riutilizzati, se ciò non è possibile essi devono essere distrutti.

Ulteriori istruzioni in caso di trattamento di dati sensibili o giudiziari

- I documenti contenenti dati sensibili e/o giudiziari devono essere conservati in archivi ad accesso controllato. E' quindi necessario garantire che armadi, schedari e contenitori siano muniti di serratura e che gli incaricati del trattamento, qualora ricevano utenti anche interni, siano sempre presenti nel proprio ufficio avendo cura di evitare che le informazioni trattate possano essere visualizzate e rese conoscibili a terzi. I dati possono essere utilizzati solo da coloro che sono stati

espressamente autorizzati e solo per scopi determinati, legittimi ed espressi e per il tempo strettamente necessario. Ad esempio, la consultazione di documenti/certificati per l'inserimento in procedure informatiche di gestione del personale, di dati relativi ai loro emolumenti, a permessi sindacali, assenze per malattia ecc, deve avvenire per il tempo strettamente necessaio alla digitazione stessa e, subito dopo, i documenti devono essere archiviati nelle modalità sopra indicate.

2. Trattamenti Con strumenti elettronici

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 consistono in un codice per l'identificazione dell'incaricato (username), associato ad una parola chiave riservata (password). Tali credenziali devono avere le seguenti caratteristiche:

- Le **username** individuali non devono mai essere condivise tra più utenti
- Le **password** devono essere mantenute riservate, devono essere sostituite, a cura del singolo incaricato, almeno ogni 6 mesi, (ogni 3 mesi nel caso di dati sensibili o giudiziari) devono avere la lunghezza di almeno 8 caratteri, non devono essere basate su informazioni facilmente deducibili (quali il proprio nome, il nome di familari, la data di nascita ecc..), non vanno trascritte su fogli, post-it e simili facilmente accessibili a terzi

Condotta a protezione dei dati e del P.C.

- Tutti i PC devono essere dotati di password rispondenti alle norme sopra elencate;
- Tutti i PC sono dotati, a cura dell'azienda incaricata della gestione dei sistemi informatici aziendali (CED), di software antivirus aggiornati 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.
- La postazione di lavoro deve essere utilizzata solo per scopi legati alla propria attività di lavoro.
- Lo screen saver deve essere impostato con password in modo che si attivi dopo alcuni minuti di inattività e le applicazioni in uso vanno chiuse prima di allontanarsi dalla postazione di lavoro.
- Alla fine di ogni sessione di lavoro ogni incaricato dovrà salvare i files contenenti i dati sul proprio computer.
- I salvataggi o backup periodici (almeno settimanali) su supporti esterni saranno effettuati dagli incaricati al CED e saranno conservati in appositi archivi non accessibili a persone non autorizzate.

Gestione anti virus

- L'addetto al CED dovrà verificare che su ogni PC sia installato il programma antivirus e che sia costantemente attivo
- Ogni incaricato dovrà prestare sempre debita attenzione agli eventuali messaggi di segnalazione di virus e, in caso di anomalie, contattare immediatamente gli incaricati CED.
- In particolare nell'ambito della posta elettronica non si dovranno aprire messaggi con allegati di cui non si conosce l'origine poiché potrebbero contenere virus in grado di danneggiare i dati sul PC.