Via Carlo Salvioni 14
telefono 091 814 17 11
fax 091 814 17 19
e-mail di-sel@ti.ch
www.ti.ch/sel

Repubblica e Cantone Ticino
Dipartimento delle istituzioni

Funzionario incaricato C. Biasca/G. Costa

Sezione degli enti locali
6501 Bellinzona

telefono di-sel@ti.ch
e-mail protezionedati@ti.ch

Ai
Municipi dei Comuni ticinesi

Tramite portale AC

Bellinzona
17 settembre 2019

Ns. riferimento Vs. riferimento

Circolare SEL n. 20190917-10

Protezione dei dati dei dipendenti comunali – Adattamento dei regolamenti organici dei dipendenti (ROD)

Signore e signori Sindaco e Municipali,
signore e signori Segretari comunali,

come vi abbiamo preannunciato lo scorso 18 aprile, il 1. luglio 2019 sono entrate in vigore alcune modifiche del Regolamento di applicazione della legge organica comunale (RALOC), fra cui una modifica **dell'art. 39 cpv. 1 let. u RALOC che impone ora di definire nel ROD le modalità di elaborazione dei dati per la gestione del personale e degli stipendi**.

Ricordiamo che l'obbligo generale della base legale per le elaborazioni sistematiche di dati personali meritevoli di particolare protezione e per la loro accessibilità è fissato dalla Legge cantonale sulla protezione dei dati[1].

Per facilitare il vostro compito - in collaborazione con l'Incaricato cantonale della protezione dei dati - vi alleghiamo alcune indicazioni per completare i Regolamenti organici dei dipendenti del vostro Comune. Più precisamente nel documento allegato trovate:

- **gli esempi di articoli ROD (riportati su sfondo grigio e con relativo commento) che possono essere utilizzati come base di partenza, da adeguare alla vostra puntuale organizzazione;**
- **un esempio di articolo sulla sorveglianza sul posto di lavoro da introdurre nel caso in cui il vostro Comune sorvegliasse l'uso delle risorse informatiche da parte dei dipendenti.**

La proposta di modifica del ROD va sottoposta al Consiglio comunale in occasione della prossima revisione del ROD.

[1] Articoli 6 e 14 cpv. 3 LPDP

Restiamo a disposizione, unitamente all'Incaricato cantonale della protezione dei dati, per eventuali vostre domande.

Certi della vostra attenzione su quanto precede, ci è gradita l'occasione per porgervi i migliori saluti.

PER LA SEZIONE DEGLI ENTI LOCALI

Il Capo Sezione:

M. Della Santa

La Capo Ufficio amministrativo e del contenzioso:

C. Biasca

L'INCARICATO DELLA PROTEZIONE DEI DATI

G. Costa

Allegato:
- Progetto di articoli ROD sulla protezione dei dati del personale con relativo commento

Copia per conoscenza a:
- Incaricato cantonale della protezione dei dati (protezionedati@ti.ch)
- Direzione del Dipartimento delle istituzioni (di-dir@ti.ch)
- Segreteria generale del Dipartimento delle istituzioni (di-sg@ti.ch)

ALLEGATO

Modelli articoli ROD sulla protezione dei dati dei dipendenti e relativo commento

Articoli base

[2]Art. 1

Sistemi d'informazione

[1] *Il servizio ... (indicare il o i servizi comunali competenti per la gestione del personale) ...* è responsabile dell'elaborazione dei dati necessari alla gestione del personale e degli stipendi. Esso gestisce sistemi d'informazione e di documentazione informatizzati per:

a) la gestione delle candidature ai concorsi pubblici
b) la gestione e l'amministrazione del personale
c) *se del caso l'allestimento di statistiche*
d) *se del caso evt. altre esigenze comunali*

(se vi sono più servizi aggiungere:
I servizi possono accedere ai sistemi d'informazione in funzione delle necessità informative per l'adempimento dei rispettivi compiti legali o di servizio).

[2] I sistemi d'informazione possono in particolare contenere dati relativi alla candidatura, alla carriera professionale, alle procedure amministrative, agli stipendi, alla gestione delle presenze e assenze, compresi dati personali meritevoli di particolare protezione; sono segnatamente tali i dati relativi alla sfera familiare, allo stato di salute, alle valutazioni sulle prestazioni e sul comportamento professionali e alle procedure e sanzioni disciplinari e penali.

[3] Il/I servizio/i del cpv. 1 garantisce/scono la gestione e la sicurezza tecnica dei sistemi d'informazione.
oppure
Tramite mandato esterno il Municipio garantisce la gestione e la sicurezza tecnica dei sistemi di informazione.

Commento

Il cpv. 1 definisce il servizio o i servizi (denominati anche organi) responsabili dell'elaborazione dei dati dei dipendenti ai sensi dell'art. 4 cpv. 6 LPDP e gli scopi dell'elaborazione. Essi assumono il compito di una gestione delle informazioni a carattere personale relative ai dipendenti, conforme alla legge sulla protezione dei dati.
Si precisa inoltre che, se vi sono più servizi responsabili, essi sono legittimati a elaborare dati personali, limitatamente a quanto necessario per l'adempimento dei loro rispettivi compiti legali o di servizio[3].

Il cpv. 2 prevede le principali categorie di dati personali elaborati:
- dati anagrafici, sulla formazione e sull'esperienza professionale e sullo stato familiare e della salute

[2] Gli articoli sono qui numerati da 1 a 8; saranno poi da rinumerare in base al puntuale ROD.

[3] Secondo i principi della proporzionalità e della finalità: ad esempio l'Ufficio degli stipendi di un Comune accede unicamente ai dati indispensabili per il calcolo del loro salario, ecc.

- dati riguardanti le varie tappe e eventi del rapporto lavorativo, dal concorso di assunzione, alla carriera professionale, all'uscita
- dati amministrativi riguardanti le presenze/assenze
- dati inerenti alle procedure amministrative o disciplinari
- dati necessari al calcolo e al versamento del salario e delle indennità
- tutti i documenti rilevanti per il rapporto d'impiego, dalla candidatura alla conclusione dello stesso.

Il cpv. 2 prevede anche la facoltà del servizio competente di elaborare dati meritevoli di particolare protezione in relazione alla sfera familiare, alle valutazioni sulle prestazioni e sul comportamento professionali nonché a procedimenti amministrativi, disciplinari o penali.
Per quanto riguarda i dati sulla salute: il servizio del cpv. 1 gestisce unicamente le risultanze generiche fornite dal medico di fiducia del dipendente rispettivamente, se del caso, dal servizio medico comunale (vedi art. 6 – Dati riferiti alla salute).

Il cpv. 3 prevede l'organo responsabile del buon funzionamento e della sicurezza tecnica dei sistemi contenenti i dati del personale.

Art. 2

Digitalizzazione dei documenti cartacei

Il/I ... *servizio/i dell'art. 1 cpv. 1* ... può/possono digitalizzare e riprendere nei sistemi d'informazione i documenti cartacei. La copia digitale del documento, con le necessarie misure di sicurezza, è presunta equivalente all'originale cartaceo. In seguito, l'originale cartaceo può essere restituito o se date le premesse distrutto.

Commento

L'art. 2 prevede la digitalizzazione di documenti cartacei, in particolare dei dossier dei dipendenti.

Partendo dal documento cartaceo, originale o in copia, e con l'ausilio di specifiche tecnologie (ad esempio la firma digitale), è creata una copia digitale identica (o equivalente) del documento cartaceo, tramite digitalizzazione, o scansione, dello stesso. È così garantita l'integrità della copia. Poiché identico, il documento elettronico può quindi espletare gli stessi effetti giuridici del documento cartaceo, in particolare presentare lo stesso valore probatorio. Si crea così un documento elettronico presunto equivalente a quello cartaceo.
Come per il documento cartaceo, anche per la sua copia elettronica la presunzione di autenticità può però essere contestata. Il documento cartaceo può, infatti, essere stato manipolato o falsificato prima della sua digitalizzazione. In una simile ipotesi, la copia elettronica rappresenta unicamente una copia identica, o equivalente, di un documento cartaceo precedentemente modificato.

Art. 3

Trasmissione sistematica di dati

[1] ***Il/I ... servizio/i dell'art. 1 cpv. 1 ...*** **può/possono trasmettere regolarmente, se del caso attraverso procedura di richiamo, i dati personali necessari all'adempimento dei seguenti compiti legali:**

a) al Municipio per l'espletamento delle sue competenze di legge in base alla Legge organica comunale, alle leggi settoriali e ai regolamenti comunali

b) ai funzionari dirigenti e al personale espressamente designato delle unità amministrative ... (*evt. specificare diversamente in base all'organigramma del Comune*), per gli aspetti di gestione del personale

c) all'Istituto di previdenza ..., per la gestione della previdenza professionale degli assicurati

d) *evt. altri servizi/persone in base a specifiche esigenze comunali da indicare ... .*

Commento

L'art. 3 prevede la trasmissione sistematica, vale a dire regolare e/o duratura, di dati riguardanti il personale, necessari per specifici compiti legali e di servizio. Tale necessità è segnatamente data per i funzionari dirigenti delle unità amministrative, i quali organizzano/dirigono/coordinano i loro subordinati e verificano la prestazione lavorativa, oppure per il Municipio, nell'ambito della sua competenza generale in tema di gestione del personale (artt. 106 let. d e 110 let. e LOC).
La necessità di dati personali da parte di altri servizi deve essere valutata in funzione dei compiti.
La norma prevede anche la facoltà di procedere alla trasmissione sistematica di dati tramite procedura di richiamo, **vale a dire tramite accesso diretto al sistema d'informazione secondo l'art. *1* direttamente da parte dei destinatari dei dati**.

Art. 4

Trasmissione puntuale di dati

Il/i ... *servizio/i dell'art. 1 cpv. 1* ... può/possono trasmettere in singoli casi dati personali ad organi pubblici o a privati se è previsto dalla legge, se sussiste una necessità per l'adempimento di compiti legali o se la persona interessata ha dato il suo consenso scritto, libero e informato.

Commento

Sono definite le condizioni per la trasmissione di dati in singoli casi e riguardante un set definito di dati personali di una o più persone per uno scopo specifico e limitato nel tempo.

La trasmissione presuppone giustificati motivi, che possono essere una base legale, la necessità d'adempimento di un compito legale oppure il consenso scritto, libero e informato della persona interessata (art. 6 cpv. 2 LPDP).

Per la trasmissione di dati occorre una richiesta scritta e motivata, con indicazione del compito legale addotto e delle concrete necessità di dati. Il servizio responsabile dei dati procede con la valutazione della richiesta, in particolare per quanto attiene all'estensione dei dati richiesti, prima di procedere alla trasmissione[4].

Art. 5

Altre elaborazioni di dati

Il/I .... ***servizio/i dell'art. 1 cpv. 1 ....*** può/possono elaborare dati del personale per scopi che esulano da quelli dell'art. 1, se ciò è necessario per l'adempimento di compiti legali o a garanzia d'interessi legittimi dei dipendenti o dell'amministrazione comunale.

Commento

Questa norma conferisce la base legale per elaborare dati personali dei dipendenti pubblici per l'esecuzione di puntuali compiti, mansioni o iniziative d'interesse legittimo per i dipendenti, l'Amministrazione pubblica o anche la cittadinanza[5].
Tali elaborazioni devono avvenire nel rispetto dei principi generali del diritto, in particolare del principio della proporzionalità.
In assenza di questi motivi giustificativi, dovrà essere richiesto e ottenuto il consenso libero e informato dei dipendenti interessati, valido comunque solamente per elaborazioni puntuali e non sistematiche (vedi art. 6 LPDP).

Art. 6

Dati personali relativi alla salute

[1] Il medico di fiducia del dipendente (*oppure se presente il servizio medico del personale*), è responsabile dell'elaborazione dei dati personali sulla salute dei dipendenti, in particolare quelli relativi alla valutazione della loro idoneità lavorativa e al loro accompagnamento medico.

[2] Esso può comunicare al servizio responsabile dell'art. 1 unicamente le conclusioni attinenti a idoneità o inidoneità lavorativa della persona interessata, al grado, alla causa e alla durata presumibile dell'inabilità lavorativa e eventuali altre conclusioni necessarie all'assunzione e alla gestione del rapporto d'impiego.

[4] Esempi in tal senso sono la trasmissione di dati relativi al versamento degli oneri sociali (AVS e AI) ai servizi preposti della Confederazione, di dati sui casi d'infortunio alle assicurazioni incaricate della gestione ai sensi della LAINF, oppure di dati inerenti alla previdenza professionale trasmessi all'Istituto collettore secondo la Legge sulla previdenza professionale (LPP).

[5] Si citano quali esempi: la pubblicazione all'interno dell'Amministrazione comunale (intranet) della lista degli avvicendamenti dei dipendenti, l'elaborazione puntuale di dati per misure d'interesse per i dipendenti o per l'Amministrazione pubblica.

Commento

Al cpv. 1, a garanzia del segreto medico, si indica in sostanza che il medico di fiducia del dipendente (o se presente il servizio medico comunale), è autonomo e indipendente dal servizio responsabile secondo l'art. 1; quest'ultimo riceve unicamente le informazioni generiche necessarie alla gestione amministrativa del rapporto d'impiego, senza dettagli di tipo medico-clinico.
Per la procedura di assunzione, se vengono raccolti dati sullo stato di salute tramite un formulario per l'assunzione, il Municipio o i servizi responsabili del personale forniscono il formulario medico alla persona interessata, la quale lo sottoporrà debitamente compilato al proprio medico di fiducia, con la richiesta di fornire al comune le indicazioni relative all'idoneità lavorativa, senza dettagli di tipo medico-clinico.
La gestione dei dati sulla salute può avvenire sia in modo cartaceo, sia in modo elettronico.

Al cpv. 2 è trattato lo scambio di dati medici con il Comune quale datore di lavoro, quindi le informazioni che le persone sottoposte al segreto medico del cpv. 1 possono comunicargli.
Il medico di fiducia del dipendente (o il servizio medico comunale), è di per sé autorizzato a comunicare al servizio responsabile del personale/Municipio unicamente le conclusioni relative alla capacità lavorativa in generale o per l'esercizio di una determinata funzione, al grado d'inabilità (espressa in percentuale), alla sua causa generica (malattia o infortunio) e alla durata presumibile dell'inabilità. Le risultanze concrete di ordine medico, e quindi eventuali problemi di salute, sono invece di esclusivo dominio del medico del personale, rispettivamente del medico di fiducia del dipendente, e tutelate dal segreto medico.

Art. 7

Conservazione dei dati

[1] I dati dei candidati non assunti sono restituiti o con il loro consenso eliminati dopo tre mesi dal termine della procedura di assunzione, ad eccezione della lettera di candidatura e dei dati anagrafici ivi contenuti che sono conservati per un anno. Possono essere conservati oltre questo termine con il consenso scritto, libero e informato del dipendente, se ne è dato un interesse per quest'ultimo.

[2] I dati personali dei dipendenti possono essere conservati per dieci anni dalla fine del rapporto d'impiego. Altri dati possono essere conservati oltre questo termine con il consenso scritto, libero e informato del dipendente.

[3] Sono conservati per una durata di trent'anni dalla fine del rapporto di impiego ai fini di un'eventuale riassunzione i dati anagrafici, l'allocazione organizzativa, la funzione ricoperta, l'entrata in servizio e le mutazioni nella carriera del dipendente.

[4] I dati del personale possono essere conservati in forma anonimizzata a scopo statistico e di ricerca in base alla legge sulla protezione dei dati.

Commento.

Per i dossier di candidatura - riservato il diritto procedurale speciale in caso di ricorso - i documenti dei candidati non assunti vengono restituiti oppure, con il loro consenso, sono eliminati, trascorsi 3 mesi dal termine della procedura di assunzione (cpv. 1), ad eccezione dei dati anagrafici (nome, cognome, indirizzo e dati di contatto) e della lettera di motivazione e presentazione del candidato, che – quali parti integranti della corrispondenza indirizzata al datore di lavoro e di proprietà di quest'ultimo – sono conservati per 1 anno.

I dati dei dipendenti sono conservati di principio per 10 anni dalla cessazione del rapporto d'impiego (cpv. 2). Tale periodo di conservazione – previsto anche presso l'Amministrazione cantonale del Canton Ticino, altri Cantoni e la Confederazione – permette la ricostruzione del passato lavorativo in caso di necessità (ad esempio nel contenzioso). Oltre il termine di 10 anni, i dati possono essere conservati unicamente con il consenso scritto, libero e informato del dipendente.

Al cpv. 3 sono definiti i dati la cui conservazione si protrae oltre i 10 anni. In caso di riassunzione tali dati permettono al Comune di adempiere, nell'interesse del dipendente, a compiti previsti dalle normative in vigore, quali ad esempio il computo degli anni di servizio per la gratifica d'anzianità.

Al cpv. 4 si indica che la conservazione di dati a scopi statistici e di ricerca è disciplinata dalla LPDP (art. 15).

Art. 8

Disposizioni esecutive

Il Municipio può disciplinare tramite direttiva i particolari, segnatamente i diritti e le modalità di accesso ai sistemi d'informazione, la digitalizzazione dei documenti cartacei, le modalità di conservazione e le misure di sicurezza dei dati.

Commento

L'art. 8 delega, in via potestativa, al Municipio il disciplinamento degli aspetti esecutivi, quali:

- per i sistemi d'informazione, i diritti di accesso tramite procedura di richiamo (segnatamente le categorie di dati accessibili e l'utenza) con le rispettive giornalizzazioni e le ulteriori modalità;
- le modalità della candidatura elettronica e della digitalizzazione dei documenti cartacei e le misure di garanzia dell'autenticità del documento scansionato;
- le misure di sicurezza a garanzia della confidenzialità, dell'integrità e dell'autenticità dei dati e la loro conservazione;
- la procedura di analisi dei dati sull'utilizzo dell'infrastruttura elettronica secondo l'art. 7 e il servizio responsabile.
- se del caso, la procedura di analisi dei dati sull'utilizzo dell'infrastruttura elettronica e il servizio responsabile.

Art. 9

Diritto suppletivo

Rimangono riservate le disposizioni della legge sulla protezione dei dati personali del 9 marzo 1987.

Commento

Nella misura in cui il ROC non disciplina determinati aspetti della protezione dei dati nell'ambito del personale pubblico, si applica la LPDP.

Articoli particolari

Art. ...

Sorveglianza sul posto di lavoro

[1] Non è ammesso l'impiego di sistemi di sorveglianza nominativa, durevole e in tempo reale della sfera privata o personale dei dipendenti sul posto di lavoro.

[2] La violazione di norme comportamentali sull'uso delle risorse informatiche, o il relativo sospetto, va costatato tramite una sorveglianza non nominativa dei dati raccolti o grazie ad indizi fortuiti.

[3] È ammessa l'analisi nominativa puntuale dei dati personali raccolti tramite sistemi di sorveglianza, in caso di costatazione o di relativi sospetti concreti di violazione delle norme comportamentali secondo il cpv. 2.

[4] Il responsabile della sicurezza adotta le misure tecniche e organizzative necessarie per prevenire gli abusi.

[5] I sistemi di sorveglianza o di controllo, se sono necessari per altre ragioni, devono essere concepiti e disposti in modo da non pregiudicare la salute e la libertà di movimento dei dipendenti.

Commento

Al cpv. 1 si esclude la sorveglianza intesa come misura di controllo personale (nominativo), in tempo reale e prolungato della sfera privata o personale del dipendente pubblico.
In altre parole - in particolare sull'uso d'internet sul posto di lavoro - non è lecito mettere sotto sorveglianza nominativa e in tempo reale un dipendente a partire dalla costatazione di un abuso o dalla nascita di un rispettivo sospetto concreto.
È invece lecito, per confermare un sospetto di abuso, controllare in modo nominativo e retrospettivo le giornalizzazioni (logfiles) delle attività passate in internet.

È pure legittima lecita (cpv. 2) la sorveglianza non nominativa, vale a dire il controllo in tempo reale e prolungato in modo anonimo o pseudanonimizzato (quest'ultimo comunque non a tempo indeterminato) del rispetto delle norme sul corretto uso delle risorse informatiche.

La sorveglianza avviene in modo anonimo quando i dati ripresi nelle giornalizzazioni delle attività in internet o di posta elettronica non sono a carattere personale e non permettono un'identificazione dell'utente (sorveglianza anonima).
La sorveglianza avviene invece in modo pseudoanonimizzato quando i dati soggetti a controllo contengono informazioni (ad esempio l'indirizzo IP dei computer) che possono essere ricondotte a specifiche persone con l'ausilio di una tabella di corrispondenza.

La sorveglianza in modo pseudanonimizzato avviene come fase successiva alla sorveglianza anonima, allorquando quest'ultima ha rivelato degli abusi e l'organo responsabile intende chiarire se essi sono ripartiti su tutta l'unità amministrativa oppure unicamente su singoli dipendenti. Nel primo caso, l'organo responsabile della sorveglianza si limita di principio a segnalare in via generale la constatazione d'abusi e a richiamare i dipendenti al rispetto delle norme sul corretto uso delle risorse informatiche.

Nel caso di abusi (cpv. 3) l'organo responsabile della sorveglianza, d'intesa con i servizi responsabili, può procedere all'identificazione del o dei responsabili, nell'ottica delle relative misure[6].

L'identificazione di un dipendente può avvenire anche successivamente alla constatazione di altri indizi quali il ritrovamento di stampati privati presso la stampante di servizio. In ogni caso, però, il datore di lavoro (e per esso i servizi informatici che garantiscono la disponibilità e il buon funzionamento delle risorse informatiche) devono prevedere la prevenzione degli abusi con adeguate misure di sicurezza (cpv. 4) tese, ad esempio, a bloccare l'accesso a determinati siti internet. La sorveglianza e l'eventuale successiva identificazione di persone deve rimanere una misura del tutto secondaria (ultima ratio) rispetto alle misure di sicurezza.

Infine, più in generale, il cpv. 5 riprende l'art. 26 cpv. 2 dell'Ordinanza federale 3 concernente la legge federale sul lavoro[7], che verte a garantire la salute e la libertà di movimento dei dipendenti, e con ciò la loro personalità[8], qualora sistemi di sorveglianza e di controllo sono implementati per altri fini (ad esempio, per il controllo della sicurezza tramite videosorveglianza).

---

[6] L'identificazione può avvenire con l'ausilio di una tabella di corrispondenza, che deve essere conservata separatamente dalle giornalizzazioni. La tabella di corrispondenza contiene la lista degli indirizzi IP e dei relativi nominativi dei dipendenti. La comparazione delle giornalizzazioni con la lista delle corrispondenze, definibile anche come de-pseudonimizzazione o re-identificazione, può avvenire unicamente successivamente al rilevamento di un abuso delle risorse informatiche o alla nascita di un sospetto concreto di abuso durante la sorveglianza anonima o pseudonima.

[7] OLL 3; RS 822.113.
[8] DTF 130 II 425, consid. 3.3.