CITTA' DI COLLEGNO

Linee guida in materia di Amministratori di Sistema

REGOLAMENTO UE N. 679/2016 (GDPR)

CITTA' DI COLLEGNO

ART. 1 - SCOPO DEL DOCUMENTO

Le presenti Linee Guida definiscono le modalità operative per la nomina degli Amministratori di Sistema, per l'individuazione dei relativi ruoli e compiti nel rispetto dei principi e dei requisiti stabiliti dalla normativa in materia di protezione dei dati personali.

ART. 2 - CONTESTO NORMATIVO E REGOLAMENTARE DI RIFERIMENTO

Le presenti Linee Guida vengono redatte in applicazione del Provvedimento dell'Autorità Garante del 28 novembre 2008, successivamente modificato in data 25 giugno 2009: *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"*e sono da considerarsi quale misura organizzativa adottata, ai sensi dell'art. 32 del Regolamento UE n. 2016/679 (GDPR), dal Comune di Collegno in qualità di Titolare del Trattamento, con l'obiettivo di garantire un livello di sicurezza adeguato al rischio.

ART. 3 - DEFINIZIONI

Dati Personali: qualsiasi informazione riguardante una persona fisica identificata o identificabile (*interessato*); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale(art. 4, punto 1 GDPR).
Amministratore di Sistema (AdS): la figura professionale preposta alla gestione ed alla manutenzione di un impianto di elaborazione o di sue componenti, con cui vengono effettuati trattamenti di dati personali. Il Garante Privacy ha esteso tale definizione ad altre figure equiparabili all'AdS dal punto di vista dei rischi relativi alla protezione dei dati, quali amministratori di database, amministratori di reti e infrastrutture, amministratori di sistemi software complessi.
Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento di Dati Personali (art. 4, punto 7 GDPR). Nel prosieguo inteso come "Comune di Collegno".
Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto ol'interconnessione, la limitazione, la cancellazione o la distruzione (art. 4, punto 2 GDPR).
Responsabile del Sistema Informativo Comunale (SIC): il Responsabile del Sistema Informativo Comunale incaricato della gestione dei sistemi informativi.
Data Protection Officer (**DPO)**: la persona nominata Responsabile della protezione dei dati del Comune di Collegno ai sensi dell'art. 37 del GDPR.
Referente Privacy: coordinatore in materia di trattamento dei dati personali, individuato all'interno del Comune di Collegno nella persona del Segretario generale.
Ufficio Programmazione e Trasparenza: l'Ufficio del Comune di Collegno a supporto dell'attività del Referente Privacy.

ART. 4 - PROCEDURA OPERATIVA

4.1.1 Requisiti professionali

La designazione di un Amministratore di Sistema richiede una previa valutazione della sua esperienza, competenza e affidabilità. In particolare, il designando dovrà fornire garanzie appropriate in merita alla sua capacità di rispettare tutti i requisiti stabiliti dalla normativa vigente in materia di protezione dei dati nonché le policies e procedure interne adottate dal Comune di Collegno in relazione alla protezione dei dati personali.

4.1.2 Nomina

La nomina di Amministratore di Sistema è individuale e deve contenere una descrizione dettagliata delle attività che l'Amministratore di Sistema è autorizzato a svolgere, in base al profilo di autorizzazione assegnato.

Nomina diretta

L'Amministratore di Sistema nominato direttamente dal Comune di Collegno può essere interno o esterno all'Ente.

L'Amministratore interno è identificato nel Responsabile del SIC ed è nominato con atto ufficiale del Segretario Generale. A sua volta, il Responsabile del SIC identifica eventuali altri Amministratori di Sistema presenti nel Settore "Sistema Informativo Comunale".

L'Amministratore esterno viene designato dal Comune di Collegno, per il tramite del Responsabile del SIC, per iscritto attraverso apposita lettera di nomina. L'Amministratore di Sistema accetta per iscritto tale nomina e comunica l'accettazione al Responsabile del SIC. In qualsiasi momento, il Comune di Collegno, con il supporto del Responsabile del SIC, potrà revocare la nomina di Amministratore di Sistema o modificare il profilo di autorizzazione.

Nomina indiretta

Qualora il Responsabile Esterno del Trattamento dei dati abbia nominato gli Amministratori di Sistema esterni, il Responsabile del SIC deve richiedere copia della nomina della persona fisica ad Amministratore di Sistema e deve verificare il possesso dei requisiti professionali.

Il Responsabile del SIC, con il supporto dell'Ufficio Programmazione e Trasparenza, integra l'Elenco degli Amministratori di Sistema con l'inserimento dei nuovi amministratori esterni nominati.

Archiviazione

La valutazione dei requisiti professionali, la lettera di nomina e la relativa accettazione, a cura del Responsabile del SIC, sono depositati agli atti d'ufficio.

4.1.3 Compiti dell'Amministratore di Sistema

L'Amministratore di Sistema è responsabile dell'esecuzione di compiti ben identificati in relazione al funzionamento tecnico dei sistemi informativi.

In particolare, garantisce il corretto funzionamento e l'operatività dell'hardware e del software di propria competenza,in modo da garantire l'adozione di adeguate misure di sicurezza in conformità con l'articolo 32 del GDPR; verifica periodicamente l'efficienza dei sistemi tecnici adottati e redige relazioni che includono informazioni sulle verifiche effettuate, sui criteri adottati e sulle misure proposte per migliorare la sicurezza. La documentazione che descrive le verifiche dell'Amministratore di Sistema, è depositata, a cura del Responsabile del SIC, agli di ufficio.

I compiti dell'Amministratore di Sistema devono essere espressamente indicati nella lettera di nomina e devono includere almeno le seguenti attività:

- attuare tutte le misure necessarie per evitare la perdita o la distruzione di informazioni e dati personali;
- stabilire meccanismi appropriati in relazione alla manutenzione e custodia delle copie di backup;
- garantire che il trattamento dei dati personali effettuato in formato elettronico sia conforme a tutte le misure di sicurezza tecniche e organizzative di cui all'art. 32 del GDPR;
- fornire adeguate istruzioni al personale del Comunedi Collegno in relazione alla distruzione o eliminazione dei dispositivi informaticie alla cancellazione di dati personali, ove necessario;
- informare periodicamente il Titolare sulle attività svolte e supportarlo nel monitorare la conformità delle misure in vigore con i requisiti previsti dalla normativa in materia di protezione dei dati.

Qualora venga attribuita la gestione del processo di autenticazione degli utenti, all'Amministratore di Sistema spetterà, altresì, il compito di generare, sostituire e invalidare gli ID utente e le password assegnate alle persone autorizzate all'elaborazione dei dati sulla base degli strumenti e delle applicazioni utilizzate, fungendo anche da custode delle copie di eventuali credenziali (quando richiesto e applicabile).
Il Responsabile del SIC attiva, sulla base dei compiti assegnati, il profilo di accesso dell'Amministratore di Sistema e, come indicato al 4.1.5, le modalità di gestione dei log.

4.1.4 *Elenco degli Amministratori di Sistema*

Il Titolare del Trattamento deve tenere un Elenco con i dati identificativi degli Amministratori di Sistema (interni ed esterni), il profilo assegnato a ciascuno e le ulteriori informazioni come dettagliate nell' **Allegato 2)** al presente per farne parte integrante e sostanziale.
L'Elenco, in formato elettronico e/o cartaceo, deve essere regolarmente aggiornato a cura del Responsabile del SIC e reso disponibile per un'eventuale ispezione dell'Autorità Garante per la protezione dei dati personali.
L'Elenco deve essere archiviato nella cartella in cui è conservata la documentazione in ambito privacy (*Privacy\Amministratori_di_Sistema*). L'accesso a tale cartella è consentito all'Amministratore di sistema ed ai suoi delegati, al Responsabile SIC ed ai suoi delegati, al Referente Privacy, all'Ufficio Programmazione e Trasparenza.
Nel caso in cui le attività svolte dagli Amministratori di Sistema includano, direttamente o indirettamente, servizi o sistemi che elaborano e/o consentono l'elaborazione di dati personali relativi ai dipendenti, l'identità degli Amministratori di Sistema deve essere comunicata ai dipendenti stessi utilizzando la rete intranet.

Commento [v1]: Per Ilario predisporre cartella

4.1.5 *Registrazione dei log degli Amministratori di Sistema*

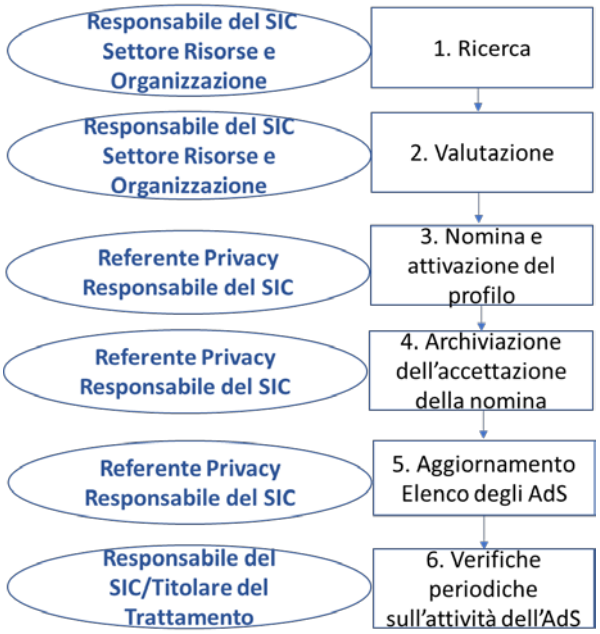
Il Comune di Collegno deve implementare misure adeguate a registrare e tracciare gli accessi dell'Amministratore di Sistema ai sistemi e alle banche dati. I log di accesso devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. I log di accesso includono ID utente, time stamp e descrizione degli eventi avvenuti (login, logout, sistema acceduto, terminale, eventuali condizioni di errore verificate e tutte le informazioni necessarie per identificare l'evento). Le registrazioni di ciascun evento devono essere conservate per un periodo non inferiore a sei mesi.

4.1.6 *Verifica delle attività degli Amministratori di Sistema*

Il Responsabile del SIC, con l'eventuale supporto di un consulente esterno, verifica annualmente le attività svolte dagli Amministratori di Sistema interni ed esterni, in relazione alla rispondenza dell'operato con le mansioni attribuite e le misure organizzative e tecniche adottate dal Comune di Collegno.Tali verifiche sono supportate anche dalle registrazioni dei log di cui al punto precedente.
L' esito delle verifiche viene comunicato al Referente Privacy documentato e archiviato in una cartella accessibile alle persone autorizzate (*Privacy\Amministratori_di_Sistema*).
In ogni caso il Titolare del Trattamento provvederà ad implementare adeguata misura per la verifica dell'attività del Responsabile del SIC tramite audit esterni ovvero identificazione di un soggetto interno con adeguate competenze.

Commento [v2]: cartella

4.2 Diagramma di flusso



Fase	Descrizione
Ricerca	Il Responsabile del SIC identifica la necessità di individuare un Amministratore di Sistema e le aree e relativi profili di accesso. Il Responsabile del SIC verifica se le risorse interne al Comune di Collegno siano idonee allo svolgimento del ruolo di Amministratore di Sistema e possano essere nominate; altrimenti segnala la necessità al Referente Privacy e al Responsabile della Sezione Personale.
Valutazione	A seconda della modalità di selezione (bando, selezione diretta), il processo potrà seguire modalità differenti. La valutazione dei profili viene effettuata dal Titolare del trattamento ed è inviata per iscritto al Referente Privacy per condivisione.
Nomina e attivazione dei profili di accesso	A seguito di valutazione positiva, il Referente Privacy, procede alla nomina dell'Amministratore di Sistema. Il Responsabile SIC contestualmente attiva il profilo di accesso e la registrazione dei log.
Archiviazione dell'accettazione della nomina	La lettera di nomina dell'Amministratore di Sistema, debitamente firmata, viene deposita agli di ufficio ed archiviata a cura del Referente Privacy, nella cartella di rete "\Privacy\Amministratori_di_Sistema".

Commento [v3]: cartella

Aggiornamento dell'elenco degli AdS	Il Responsabile del SIC aggiorna l'elenco degli Amministratori di Sistema e, in caso di accesso a dati dei dipendenti, garantisce la sua conoscibilità ai questi ultimi.
Verifiche periodiche delle attività degli AdS	Il Responsabile SIC esegue annualmente un piano di audit per verificare le attività degli Amministratori di Sistema. L'esito delle verifiche viene comunicato al Referente Privacy.

CITTA' DI COLLEGNO

Annex 1 – Fac simile Letteradi Nomina ad Amministratore di Sistema

Nota interna: da utilizzare per la nomina di AdS interni e da allegare ad eventuali contratti in caso di esternalizzazione delle attività di AdS

[carta intestata]

[luogo, data]

Comune di Collegno
Piazza del Municipio 1
10093 Collegno (TO)

Oggetto: Atto di nomina ad "Amministratore di Sistema"

Egregio Sig.

Premesso che:

- l'articolo 32 del Regolamento (UE) n. 2016/679 relativo alla tutela delle persone fisiche con riguardo al trattamento dei dati personali e sulla libera circolazione di tali dati (General Data Protection Regulation, in breve "GDPR")prevede cheil Titolare del trattamento, tenendo conto dello stato dell'arte, dei costi di implementazione, della natura, della portata, del contesto, delle finalità del trattamento e del rischio per i diritti e le libertà delle persone, attui misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio;
- il Comune di Collegno, in qualità di Titolare del Trattamento dei dati, intende designare un Amministratore di Sistema per svolgere taluni compiti per il funzionamento tecnico dei sistemi informativi.

Tutto ciò premesso, ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, successivamente aggiornato in data 25 giugno 2009, rilevato il possesso dei requisiti di idoneità professionale richiesti, il Titolare La designa "Amministratore di Sistema".

1. Scopo

Nelle sue qualità di Amministratore di Sistema, Le verrà richiesto di svolgere i seguenti compiti: [togliere i compiti non coerenti con la nomina]

- amministratore di database
-amministratore di rete e apparati infrastrutturali
-amministratore di softwarecomplessi.

I sistemi, database e software inclusi nel perimetro della nomina sono:

- [inserire i sistemi e/o database e/o software di competenza dell'Amministratore di sistema

- .....]

I Suoi compiti saranno:

[elenco eventualmente da modificare e/o integrare caso per caso]

A. gestire il sistema informativo in conformità con le istruzioni ricevute dal Comunedi Collegno e con i requisiti di legge sulla protezione dei dati, nonché con le politiche e le procedureinterne del Comune;

B. monitorare la sicurezza IT e garantire il corretto funzionamento e l'operatività dell'hardware e del software, in modo da garantire l'adozione di adeguate misure di sicurezza in conformità con l'articolo 32 del GDPR e la normativa vigente sulla protezione dei dati;

C. generare, sostituire e invalidare gli ID utente e le password assegnate alle persone autorizzate al trattamento dei dati, sulla base degli strumenti e delle applicazioni utilizzate, quando richiesto ed applicabile. L'Amministratore di Sistema deve anche agire come depositario delle copie di eventuali credenziali;

D. proteggere e gestire il processo di autenticazione e il rispettivo sistema di autenticazione in base alle seguenti linee guida:

(i) qualsiasi nome utente e password devono essere assegnati esclusivamente dall'Amministratore di Sistema. Al momento dell'assegnazione, le credenziali rilevanti saranno gestite dall'utente designato, salvo differenti specifiche ragioni tecniche e organizzative documentate;

(ii) qualsiasi codice identificativo assegnato a un utente specifico non può essere riassegnato ad altri utenti, in modo da garantire una registrazione storica dei codici identificativi dell'utente;

(iii) le credenziali devono essere disattivate dopo un periodo di inattività di sei mesi dell'utente designato (eccetto per motivi tecnici e organizzativi specifici e documentati). Le credenziali assegnate ad uno specifico utente devono essere disattivate anche nel caso in cui l'utente cessi di detenere la posizione, il ruolo o la qualifica professionale all'interno del Comune, alla luce del quale gli sono state attribuite le credenziali (es. cessazione del rapporto di lavoro);

(iv) nel caso in cui venga accertata (o sia probabile che venga accertata) che le credenziali assegnate a un utente sono state divulgate e/o sottratte da terze parti e/o utilizzate da persone non autorizzate, tali credenziali devono essere prontamente modificate. Qualsiasi password predefinita deve essere modificata dagli utenti interessati al loro primo accesso. Gli utenti devono essere obbligati a impostare una nuova password prima dell'accesso ai relativi sistemi;

E. utilizzare le credenziali di Amministratore di Sistema solo se necessario. ID utente e password degli Amministratori di Sistema devono essere creati e gestiti in base ai seguenti criteri:

(i) le credenziali saranno usate solo per eseguire operazioni che richiedono appropriati privilegi;

(ii) le password includeranno una lunghezza minima di 14 caratteri;

(iii) specifiche regole di complessitàsaranno incluse (maiuscole, numeri, speciali caratteri);

(iv) credenzialianonime, come “Administrator” per Windows, possono essere usate solo in caso di emergenzae in ogni caso devono essere documentate (es. via email);

(v) prima della creazione di un nuovo dispositivo, devono essere implementati meccanismi specifici per forzare la modifica delle credenziali di default in linea con le regole di complessità del Comune;

F. adottare appropriati programmi anti-virus, firewall e qualsiasi altro software in modo da garantire l'implementazione di adeguate misure di sicurezza e verificare che l'implementazione, l'aggiornamento e il funzionamento di tutti gli strumenti sia conformi alle politiche e alle procedure IT del Comune;

G. attuare tutte le misure necessarie per evitare la perdita o la distruzione, anche accidentale, di qualsiasi dato personale e stabilire meccanismi appropriati in relazione al mantenimento delle copie di backup. L'Amministratore di Sistema deve inoltre garantire la qualità delle copie di back-up e la conservazione degli stessi in un luogo idoneo e sicuro;

H. fornire adeguate istruzioni al personale in relazione alla distruzione o all'eliminazione dei dispositivi e degli strumenti IT e alla cancellazione di dati personali, ove necessario;

I. sorvegliare le operazioni di implementazione e manutenzione dei sistemi di propria competenza, anche quando tali operazioni sono eseguite da fornitori esterni. Nel caso in cui vengano riscontrate anomalie, le stesse devono essere segnalate al responsabile SIC e al responsabile gerarchico;

J. fornire supporto e assistenza al Titolare in relazione a comunicazioni e/o richieste dell'Autorità di Vigilanza;

K. comunicare tempestivamente qualsiasi rischio e/o potenziale rischio che possa influire sul corretto trattamento dei dati personali;

L. verificare periodicamente l'efficienza dei sistemi tecnici adottata e relazionare periodicamente il Titolare sulle verifiche effettuate, i criteri adottati e le misure proposte per migliorare la sicurezza tecnica e organizzativa.

In qualsiasi momento, il Titolare avrà il diritto di revocare l'Amministratore di Sistema, nonché di sostituirlo o di modificare il profilo di autorizzazione sopra descritto.

2. Registrazione dei log degli Amministratori di Sistema

2.1. Le attività svolte dall'Amministratore di Sistema sono monitorate dal Comune di Collegno e vengono implementate misure adeguate per tracciare e registrare gli accessi dell'Amministratore di Sistema ai sistemi di elaborazione e ai database elettronici.

2.2 I log di accesso devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità. I log di accesso includono le informazioni relative all'ID utente utilizzato, il timestamp, la descrizione dell'evento che li ha generati (ad es., Log-in, log-out, sistema / applicazione / database a cui si accede, dispositivo terminale, eventuali condizioni di errore verificate e tutte le informazioni necessarie per identificare l'evento). La registrazione di ciascun evento e le relative informazioni saranno conservati dal Comune di Collegno per il periodo necessario ad adempiere agli obblighi legali, per soddisfare i requisiti normativi, risolvere controversie, mantenere la sicurezza, prevenire frodi e abusi e, in ogni caso, per un periodo non inferiore ai sei mesi.

3. Verificheperiodiche

3.1. Il Comune di Collegno avrà il diritto di verificare regolarmente le attività dell'Amministratore di Sistema, almeno una volta l'anno, per controllarne laconformità alla normativa vigentee alle istruzioni indicatein questo documento.

3.2. L'Amministratore di Sistema deve cooperare con il Comune di Collegno nello svolgimento di tali attività di controllo e ispezione.

4. Responsabilitàdell'Amministratore di Sistema

4.1. L'Amministratore di Sistema assicura che tutte le attività oggetto della presente nomina saranno eseguite nel rispetto delle leggi applicabili in materia di protezione dei datipersonali e delle procedure interne del Comune di Collegno.

In nome e per conto del Comune di Collegno

_____
[Titolare]

*****

Per conoscenza e accettazione:

_____
[***Nome, Cognome dell'Amministratore di Sistema***]

CITTA' DI COLLEGNO

Annex2 – Fac Simile Elenco degli Amministratori di Sistema

Persona/ Società	Nome sistema	Ammistratore di Sistema di rete	Ammistratore di Sistema di database	Ammistratore di Sistema di software	Descrizioneattività	Data di Nomina	Data di Revoca
..	..	..	..	..	..		
..	..	..	..	..	..		