COMUNE DI FIRENZE

Privacy - Ordinamento degli uffici e dei servizi comunali: criteri e modalità organizzative in materia di trattamento dei dati personali.

(Delibera G.C. n. 411 del 10.09.2019)

TITOLO I
NORME INTRODUTTIVE

ART. 1
Oggetto

1. Il presente Regolamento ha ad oggetto la disciplina dell'ordinamento degli uffici e dei servizi comunali in attuazione delle disposizioni del Regolamento europeo n. 679 del 27 aprile 2016 (di seguito "GDPR") e del "Codice in materia di protezione dei dati personali" approvato con D.Lgs. 30 giugno 2003, n.196, di seguito denominato "Codice" come modificato dal D.Lgs 101 del 10 agosto 2018 ed in particolare:

a) individua i compiti del Titolare e dei Responsabili, nonché degli Autorizzati del trattamento dei dati personali esistenti e gestiti presso gli uffici comunali;
b) disciplina il trattamento dei dati personali effettuato dall'Amministrazione comunale nello svolgimento dei propri compiti istituzionali.

ART. 2

Definizioni

1. Ai fini del presente Regolamento si intende per:

«titolare del trattamento»: il Comune di Firenze quale entità organizzativa complessa;
«soggetti che esercitano le funzioni del Titolare»: i singoli Dirigenti del Comune di Firenze (qualificabili anche come sub-titolari) per i rispettivi ambiti di competenza ovvero, in ragione delle specificità organizzative della struttura di appartenenza, i titolari di PO da questi individuati;
«autorizzati»: i soggetti interni autorizzati per competenza da parte del Dirigente al trattamento dei dati personali;
«responsabile del trattamento»: la persona fisica o giuridica, o altro organismo, estraneo al Comune di Firenze, che tratta dati personali per conto del titolare del trattamento;
«sub-responsabile del trattamento»: la persona fisica o giuridica o altro organismo, estraneo al Comune, a cui fa ricorso il responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento;
«amministratore di sistema»: la figura professionale dedicata alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi

di gestione delle banche dati informatiche, i sistemi software complessi, le reti locali e gli apparati di sicurezza;
«responsabile della protezione dei dati (RPD)»: il soggetto che svolge i compiti di cui all'art. 39 del GDPR o gli ulteriori compiti affidati dal titolare del trattamento.

2. Per le altre definizioni si rinvia all'art. 4 GDPR.

Art. 3
Finalità del trattamento

1.I trattamenti sono compiuti dal Comune per le seguenti finalità:
a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri;
b) l'adempimento di un obbligo legale al quale è soggetto il Comune;
c) l'esecuzione di un contratto con soggetti interessati o per la conclusione dello stesso;
d) per la salvaguardia degli interessi vitali dell'interessato o di altra persona fisica;
e) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

2. Rientrano nelle finalità di cui al comma 1 lett. a) i trattamenti compiuti per:
a) l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;
b) la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;
c) l'esercizio di ulteriori funzioni amministrative affidate al Comune per servizi di competenza statale o regionale in base alla vigente legislazione, ovvero per altri servizi in base a convenzione;
d) la tutela in giudizio del Comune.

TITOLO II

ORGANIZZAZIONE DEL TITOLARE

ART. 4
Titolare del trattamento

1.Il Comune di Firenze è il Titolare del trattamento dei dati personali compiuto per lo svolgimento delle relative funzioni istituzionali dalle proprie articolazioni organizzative o da parte di terzi per suo conto.

2.Il Titolare definisce, fin dalla fase di progettazione, le necessarie misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento dei dati personali è effettuato in modo conforme al GDPR e al Codice.

3.Gli interventi necessari per l'attuazione delle misure di cui al precedente comma sono inseriti nell'ambito degli strumenti di programmazione.

4.Le funzioni di titolare del trattamento sono esercitate da ciascun Dirigente nel rispettivo ambito di competenza, in conformità all'assetto organizzativo del Comune di Firenze e alle disposizioni del presente regolamento.

Art 5
Compiti dei Dirigenti

1. I Dirigenti, nell'ambito delle strutture organizzative cui sono preposti, assicurano il rispetto degli obblighi normativi previsti in capo al Titolare del trattamento in relazione ai trattamenti di loro competenza.

2. Tali soggetti provvedono in particolare a:

a) censire e monitorare costantemente le singole attività di trattamento dei dati personali facenti capo alla Direzione/Servizio;
b) fornire prontamente ogni elemento necessario alla regolare tenuta del Registro unico delle attività di trattamento predisposto dal Comune di Firenze ai sensi dell'art. 13 del presente regolamento al fine di consentire il costante aggiornamento dello stesso;
c) designare con atto scritto gli autorizzati al trattamento dei dati personali con le modalità di cui all'art. 10 del presente regolamento;
d) vigilare sulle attività dei soggetti autorizzati di cui al precedente punto e garantirne una adeguata formazione nell'ambito delle iniziative predisposte dall'Ente e dal RPD;
e) disciplinare il rapporto con il Responsabile del Trattamento e procedere per iscritto alla sua nomina secondo le modalità previste dall'art 9 del presente regolamento;
f) prima di procedere al trattamento, effettuare l'analisi del rischio e, ove necessario, la valutazione di impatto ai sensi dell'art. 35 del GDPR e dell'art. 19 del presente regolamento;
g) provvedere, in relazione alla natura dei dati e alle specifiche caratteristiche del trattamento, a monitorare l'adeguatezza delle misure di sicurezza adottate;
h) notificare al Garante la violazione dei dati personali (data breach) e provvedere alla comunicazione della violazione agli interessati dandone informativa alla Direzione Segreteria Generale e Affari Istituzionali e al RPD ai sensi dell'art. 20 del presente regolamento;
i) collaborare con il RPD al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
j) garantire l'esercizio dei diritti degli interessati previsti agli articoli da 15 a 18 e da 20 a 22 del GDPR e dar corso alle relative richieste;
k) predisporre le informative e curarne il costante aggiornamento;
l) designare gli amministratori di sistema secondo quanto previsto dall'art.11 del presente Regolamento.

Art. 6
Compiti di Coordinamento delle Direzioni

1.Ciascuna Direzione tiene il registro dei trattamenti delle strutture organizzative che ad essa afferiscono e fornisce prontamente ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico di cui all'art. 13 del presente regolamento.

2. Ciascuna Direzione predispone un elenco dei Responsabili del trattamento che condivide con la Segreteria Generale, e lo aggiorna periodicamente; tiene altresì un elenco degli Amministratori di sistema che condivide con la Direzione Sistemi Informativi.

3. Ciascuna Direzione nomina uno o più "referenti privacy" per la gestione degli adempimenti connessi alla protezione dei dati, nonché come punto di contatto con il RPD e la Direzione Segreteria Generale e Affari Istituzionali.

4. Qualora all'interno della Direzione vi siano banche dati o applicativi condivisi tra più strutture spetta al Direttore decidere in ordine agli adempimenti previsti dal GDPR e dal Codice.

5. Qualora all'interno dell'Amministrazione Comunale vi siano banche dati o applicativi condivisi tra più Direzioni, le decisioni in ordine agli adempimenti previsti dal GDPR e dal Codice spettano al Dirigente a cui competono le funzioni ed attività per il cui svolgimento è stato sviluppato il software o la banca dati informatica.

6. In ipotesi in cui vi sia una committenza plurima gli adempimenti di cui al comma 5 spettano al dirigente a cui competono le funzioni e attività prevalenti.

7. Qualora sotto l'area di Coordinamento sia allocato un Servizio e/o una Posizione Organizzativa, le funzioni di cui ai precedenti commi sono attribuite al Direttore dell'Area di Coordinamento.

Art. 7
Compiti della Direzione Segreteria Generale e Affari Istituzionali

1. Alla Direzione Segreteria Generale e Affari Istituzionali compete l'adozione delle misure volte a garantire l'uniformità di applicazione del GDPR all'interno dell'ente. Tale Direzione si avvale di un ufficio amministrativo in materia di privacy che fornisce adeguato supporto alle Direzioni, anche predisponendo l'opportuna modulistica.

2. La Direzione Segreteria Generale e affari istituzionali raccoglie i registri di competenza delle Direzioni al fine di formare il Registro unico dei trattamenti di cui all'art. 13 del presente regolamento, approvandone periodicamente gli aggiornamenti e disponendo eventualmente modalità operative per l'organizzazione dello stesso.

3.La Direzione Segreteria Generale e affari istituzionali collabora con le Direzioni alla tenuta dell'elenco dei Responsabili dei trattamenti.

4.La Direzione Segreteria Generale e Affari Istituzionali collabora e fornisce adeguato supporto al RPD.

Art. 8
Compiti della Direzione Sistemi Informativi

1. Alla Direzione Sistemi Informativi competono lo sviluppo e la gestione delle applicazioni e dei sistemi informatici dell'Ente. Nello svolgimento di tali attività, alla Direzione Sistemi Informativi spettano i seguenti compiti:

a) provvedere, in relazione alle conoscenze acquisite in base al processo tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, ad adottare e ad aggiornare le idonee e preventive misure di sicurezza per i dati informatici in relazione ai trattamenti di diretta competenza ed a collaborare con gli altri Dirigenti dell'Ente per la definizione delle misure di sicurezza inerenti i trattamenti di competenza degli stessi;
b) programmare e realizzare gli interventi in materia di sicurezza informatica;
c) impartire ai Dirigenti le necessarie istruzioni operative per la sicurezza delle banche dati;
d) curare il coordinamento delle operazioni relative alla sicurezza delle categorie particolari di dati personali di cui agli artt. 9 e 10 del GDPR oggetto di trattamento con modalità informatica, provvedendo a prevenire i rischi di distruzione o perdita, anche accidentale;

e) fornire supporto ai Dirigenti, sui profili informatici, per lo svolgimento della Valutazione di impatto di cui all'art. 35 del GDPR;
f) collaborare con le Direzioni alla tenuta dell'elenco degli amministratori di sistema ed assisterle nella nomina, nella formulazione delle istruzioni e nell'attività di verifica sull'operato degli amministratori stessi;
g) svolgere, anche su richiesta di un dirigente, sessioni di audit interno o esterno, in modo casuale e/o a campione, sui trattamenti informatici svolti, sul corretto uso dei dispositivi di lavoro, sui sistemi informatici di competenza e sulle misure di sicurezza poste in essere per verificare l' affidabilità e sicurezza delle stesse, il corretto utilizzo degli strumenti e il rispetto di quanto previsto dalla normativa di settore, dai regolamenti dell'Ente e dei provvedimenti del Garante della protezione dei dati personali, in attuazione dei principi di necessità, pertinenza e non eccedenza dei controlli o degli audit condotti.

Art. 9

Responsabile del trattamento

1. Il Dirigente nomina quali responsabili del trattamento i soggetti pubblici o privati affidatari, per conto del Comune, di attività e servizi che per la loro realizzazione rendono necessario il trattamento di dati personali o i soggetti terzi che trattano dati sulla base di specifiche convenzioni.

2. Il Dirigente provvede a dare adeguate istruzioni per i trattamenti nel contratto di affidamento o con separato atto giuridico che definisca la materia, la durata, la natura e la finalità del trattamento, il tipo di dati personali, le categorie di interessati oltre agli obblighi che il Responsabile si impegna a rispettare con la sottoscrizione.

3. La nomina del responsabile del trattamento è fatta al momento dell'inizio dell'esecuzione se anteriore alla stipula del contratto.

4. I Responsabili del trattamento sono nominati tra soggetti che forniscono le garanzie di cui all'art. 28 par. 1 GDPR. La sussistenza di tali garanzie deve essere espressamente dichiarata.

5. E' consentita, previa autorizzazione del Dirigente di cui al comma 1, la nomina di sub-responsabili da parte di ciascun Responsabile per l'esecuzione di specifiche attività di trattamento ai sensi dell'art. 28 par.4 GDPR.

ART. 10
Autorizzati al trattamento

1. Il Dirigente procede a designare, all'interno della propria struttura operativa, il personale dipendente autorizzato per l'espletamento di tutte le operazioni di trattamento dei dati.

2. La designazione è fatta con atto scritto nel quale sono specificati i compiti affidati agli autorizzati e le prescrizioni per il corretto, lecito, pertinente e sicuro trattamento dei dati.

3. Gli Autorizzati effettuano tutte le operazioni di trattamento dei dati nel rispetto delle istruzioni e direttive impartite dal proprio Dirigente che prevedono di:

a) accedere solo ai dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti assegnati;

b) trattare i dati personali di cui si viene a conoscenza per l'espletamento delle proprie funzioni, in modo lecito e corretto, nel rispetto delle norme di legge, dello Statuto e dei Regolamenti che disciplinano le attività del Comune;
c) verificare costantemente i dati, il loro aggiornamento, la loro completezza e pertinenza;
d) custodire con cura atti e documenti contenenti dati personali ricevuti in consegna per adempiere ai compiti assegnati e restituirli al termine delle operazioni affidate;
e) comunicare i dati personali trattati solo previa autorizzazione;
f) osservare scrupolosamente le misure di sicurezza predisposte;
g) osservare, anche in seguito a modifica, trasferimento e/o cessazione del rapporto di lavoro gli obblighi relativi alla riservatezza e alla comunicazione.

Art. 11
Amministratori di sistema

1. I Dirigenti, in relazione ai trattamenti di loro competenza, provvedono a designare gli amministratori di sistema tra i propri dipendenti o, se necessario, tra soggetti esterni, nei casi e con le modalità stabilite dal Provvedimento del 27.11.2008 (e successive modifiche e integrazioni) del Garante della Privacy.

2. Qualora la designazione degli amministratori di sistema riguardi soggetti esterni al Comune, la competenza è del dirigente che ha provveduto all'affidamento del contratto in base al quale viene sviluppato o gestito il software, viene strutturata o gestita la banca dati informatica o, comunque, viene effettuato il trattamento.

Art. 12
Responsabile della protezione dei dati

1. Il Responsabile della protezione dei dati ("RPD") è individuato, con decreto di nomina del Sindaco, che ne stabilisce la durata dell'incarico, fra soggetti in possesso dei requisiti previsti dal GDPR.

2. Il RPD assolve i compiti previsti dall'art. 39 del GDPR e gli eventuali altri compiti affidati alla stesso dal Sindaco.

3. Il Comune garantisce al RPD, per l'esecuzione di compiti ad esso affidati, l'autonomia e le risorse necessarie per assolverli.

4. Il RPD propone, in raccordo con la Direzione Segreteria Generale e Affari Istituzionali e la Direzione Sistemi Informativi, un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati.

5. Gli uffici formulano le proprie richieste al RPD dandone contestualmente conoscenza alla Direzione Segreteria Generale e Affari Istituzionali. Il RPD rende noti i risultati della propria attività consultiva, di norma resa entro 30 giorni, anche alla Direzione Segreteria Generale e Affari Istituzionali. Qualora la questione coinvolga più Direzioni, la Segreteria Generale e Affari Istituzionali ne dà adeguata diffusione per garantirne l'uniformità di applicazione.

6. Il RPD può convocare incontri con i dirigenti e i dipendenti per l'esecuzione dei propri compiti di informazione, consulenza, sorveglianza e consultazione e può altresì organizzare specifiche giornate di formazione.

7. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

TITOLO III
TRATTAMENTO DEI DATI PERSONALI

Art. 13
Registro delle attività di trattamento

1. Il Comune di Firenze tiene un registro Unico dei trattamenti contenente le informazioni di cui all' art. 30 del GDPR e che elenca i trattamenti delle Direzioni secondo lo schema allegato al presente regolamento.

2. In occasione dell'aggiornamento dell'elenco dei procedimenti e comunque entro il 30 giugno di ciascun anno, le Direzioni provvedono a trasmettere alla Segreteria Generale e Affari Istituzionali l'aggiornamento delle attività di trattamento con riferimento agli ambiti di competenza.

ART. 14
Consenso dell'interessato.

1. Il Comune, in quanto soggetto pubblico non deve chiedere il consenso dell'interessato al trattamento dei dati personali, purché il trattamento medesimo sia conforme ai fini istituzionali dell'Ente di cui all'art.3 del presente regolamento.

2. Nei limitati casi in cui il consenso vada richiesto questo deve essere libero, specifico, informato e inequivocabile e non è ammesso il consenso tacito o presunto.

ART. 15
Informativa

1. L'interessato deve essere preventivamente informato, oralmente o per iscritto, secondo quanto previsto dagli artt. 13 e 14 GDPR.

2.L'informativa deve avere forma concisa, trasparente, intelligibile per l'interessato e facilmente accessibile; occorre utilizzare un linguaggio chiaro e semplice.

3. Nell'informativa devono essere comunicati anche i dati di contatto del Dirigente che effettua il trattamento.

4. Ciascuna Dirigente è tenuto ad aggiornare periodicamente le informative utilizzate.

5. L'informativa può essere resa disponibile negli uffici anche mediante affissione.

ART. 16
Diritti dell'interessato

1. Per l'esercizio dei diritti di cui agli articoli da 15 a 22 GDPR l'interessato presenta richiesta al Comune ovvero al Dirigente competente al trattamento.

2. Se il trattamento è effettuato da soggetti terzi per conto del Comune, la richiesta viene presentata al dirigente che ha provveduto alla nomina del Responsabile del trattamento.

3. La richiesta può essere inoltrata anche per posta elettronica.

4. L'esercizio dei diritti dell'interessato è gratuito. Il rilascio di copie non è soggetto a rimborsi di diritti di riproduzione e di ricerca.

5. L'Ufficio competente provvede senza ritardo sulla richiesta, e comunque entro trenta giorni dal suo ricevimento. Se le operazioni necessarie per il riscontro alla richiesta sono complesse o ricorre altro giustificato motivo, il termine per il riscontro è di sessanta giorni.

6. Sono fatte salve le limitazioni di cui agli artt. 2-undecies e 2-duodecis del D.Lgs. 196/2003 e le altre limitazioni previste dalla legge.

7. Di norma si procede alla cancellazione dei dati personali in conformità alle norme sulla conservazione della documentazione amministrativa.

Art. 17
Sicurezza del trattamento

1. Ciascun Dirigente mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio e procede, secondo una pianificazione concordata con il RPD, ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati.

2. Il Comune favorisce l'adesione ai codici di condotta per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto

Art. 18
Durata del trattamento

1. Fatto salvo quanto specificamente disposto da disposizioni di settore e nelle more dell'approvazione del manuale di conservazione, la durata del trattamento dei dati personali coincide, di norma, con i tempi di conservazione indicati, in riferimento alle diverse tipologie documentali, nel Piano di conservazione dell'Ente e nel relativo Massimario di scarto. La durata dei trattamenti è indicata nel Registro Unico di cui all'art. 13.

ART. 19
Valutazione di impatto

1. Ciascun Dirigente valuta la necessità di sottoporre a valutazione di impatto i trattamenti da effettuare e/o le proprie banche dati; qualora decida di procedere a valutazione di impatto si coordina con il RPD e, in caso di trattamento con modalità informatica, con il Direttore dei Sistemi informativi per programmarne le modalità operative.

2. La valutazione di impatto dovrà essere prioritariamente effettuata sulle banche dati condivise.

Art.20
Violazione dei dati personali

1. Chiunque venga a conoscenza di una violazione dei dati personali (data breach) è tenuto a segnalarlo, anche per il tramite del proprio responsabile, al Dirigente che deve provvedere tempestivamente ai sensi del presente articolo.

2. Il responsabile del trattamento che viene a conoscenza di una violazione informa tempestivamente il Dirigente che lo ha nominato.

3. Il Dirigente ove possibile, notifica la violazione dei dati personali al Garante della protezione dei dati personali entro 72 ore dal momento in cui ne sia venuto a conoscenza, a meno che sia improbabile che la stessa violazione presenti un rischio per la tutela dei diritti e delle libertà delle persone fisiche.

4. La notifica viene effettuata, prevedendo almeno gli elementi indicati al paragrafo 3 dell'articolo 33 del GDPR. La notifica al Garante della protezione dei dati personali effettuata oltre le 72 ore, deve essere motivata.

5. Le segnalazioni e le notifiche dei casi di violazione dei dati personali sono comunicati tempestivamente dai Dirigenti alla Direzione Sistemi Informativi, alla Direzione Segreteria Generale e Affari Istituzionali e al RPD.

6. Ciascun Dirigente deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza per poter dimostrare il rispetto delle disposizioni del GDPR.

Art. 21
Formazione del personale

1. Il Comune di Firenze assicura la programmazione e l'organizzazione delle attività formative del personale per la corretta applicazione delle disposizioni in materia di trattamento dei dati personali anche sulla base delle indicazioni del RPD.

Art. 22
Trattamento dei dati personali da parte di Amministratori

1. Gli Amministratori sono legittimati al trattamento dei dati personali esclusivamente nell'esercizio delle proprie funzioni istituzionali e sono tenuti alla riservatezza; in tale esercizio devono assicurare il rispetto del GDPR.

2. I trattamenti dei dati personali effettuati negli Uffici di supporto agli organi politici devono essere svolti da personale adeguatamente informato, formato e autorizzato.

ART. 23
Comunicazione e diffusione dei dati personali comuni.

1. La comunicazione dei dati personali all'interno dell'Ente per lo svolgimento delle funzioni istituzionali non è soggetta a limitazioni, salvo quelle espressamente previste da leggi e regolamenti.

2. Il Dirigente, valutato il caso, può decidere di adottare le misure necessarie alla tutela della riservatezza degli interessati.

3. La comunicazione dei dati personali ad altri soggetti pubblici e la loro diffusione è disciplinata dall'art. 2 ter del Codice.

ART. 24
Norma finale

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni di cui al GDPR, al D.Lgs. 196/03 (Codice Privacy) e successive modifiche ed integrazioni e ai Regolamenti comunali vigenti.