COMUNE DI AREZZO

SEGRETERIA GENERALE

RACCOLTA DEGLI STATUTI E REGOLAMENTI IN VIGORE NEL COMUNE DI AREZZO

REGOLAMENTO DEL MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

definito "Modello organizzativo GDPR"

Approvato con delibera di Giunta Comunale
n. 326 del 4 luglio 2023

(integra il Regolamento sull'ordinamento degli uffici e dei servizi del Comune di Arezzo)

1. INQUADRAMENTO E INDIRIZZI GENERALI

Il Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (denominato General Data Protection Regulation, di seguito definito "Regolamento" o "GDPR"), detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi ed adempimenti a carico dei soggetti che trattano dati personali, ivi comprese le pubbliche amministrazioni.

In Italia l'interesse prevalente, nell'ambito della pubblica amministrazione, era stato rivolto alla trasparenza, anche nell'ottica della prevenzione della corruzione. La normativa fondamentale in materia è il D. Lgs. 33/2013, che viene modificato dal D. Lgs. n. 97/2016.

In materia di privacy, il D. Lgs. 196/2003 (Codice in materia di protezione dei dati personali) viene modificato dal D. Lgs. 101/2018, per l'adeguamento al Reg. UE 679/2016.

L'operatività del GDPR richiede una maggiore attenzione, da parte delle pubbliche amministrazioni, all'applicazione del principio della trasparenza amministrativa, sia per le altissime sanzioni previste in caso di violazione della "privacy", sia per la sempre maggiore digitalizzazione della società. Nella nuova ottica, si può parlare non di antagonismo fra trasparenza e privacy, bensì di complementarietà.

Il GDPR introduce un concetto di più ampio rispetto alla "privacy", quello della protezione dei dati personali e del relativo trattamento.

L'Art. 5 del GDPR enuncia i principi applicabili al trattamento di dati personali: liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione.

Al fine di garantire in modo efficace ed efficiente l'attuazione di quanto previsto dal GDPR e dal D. Lgs. 196/2003 e s.m.i., occorre puntualizzare l'assetto delle responsabilità, tenuto conto della specifica organizzazione del Comune di Arezzo (nel seguito definito anche "Ente"), definendo quindi il presente "modello organizzativo GDPR".

Il regolamento europeo, nonché le ulteriori disposizioni normative vigenti ed i provvedimenti dell'Autorità Garante, individuano diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

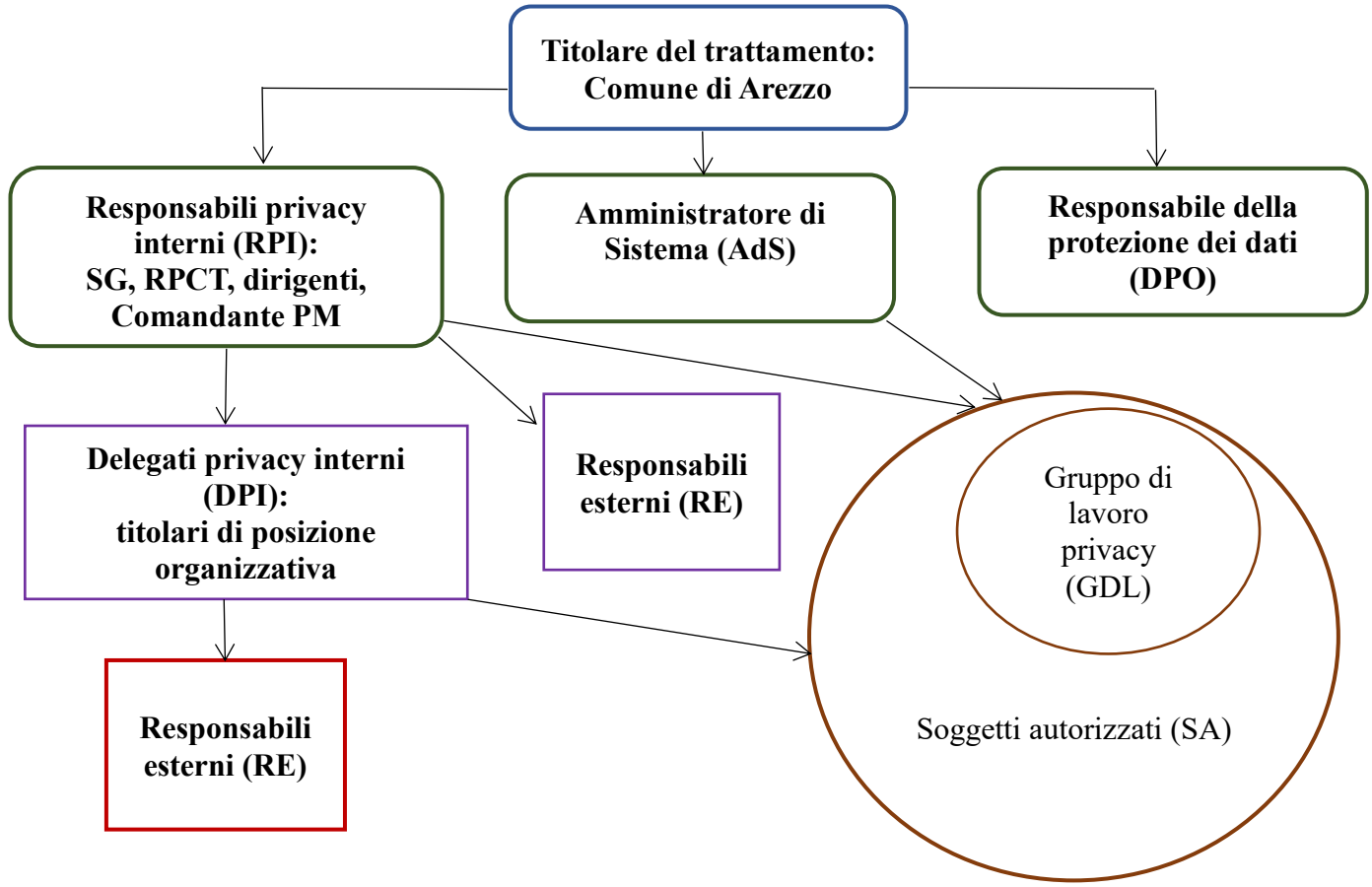
- il **titolare del trattamento** (vedasi capo IV del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;
- il **responsabile del trattamento** (vedasi capo IV del GDPR): la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (soggetto esterno all'organizzazione);
- il **responsabile della protezione dei dati** (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del GDPR, che ne disciplinano compiti, funzioni e responsabilità;
- le **persone autorizzate al trattamento dei dati personali** sotto l'autorità diretta del titolare o del responsabile del trattamento ex art. 29 del Regolamento UE 679/2016. figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del GDPR.
- l'**amministratore di sistema**, introdotto dal provvedimento del Garante per la Protezione dei Dati Personali (nel seguito definito "GPDP" o "Garante") del 27/11/2008 e modificato il 25/6/2009 (G.U. n. 149 del 30/6/2009), nel caso di trattamenti effettuati con strumenti elettronici: figure professionali dotate di specifici privilegi, finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, amministratori di basi di dati, amministratori di reti e di apparati di sicurezza e amministratori di sistemi software complessi.

Con il presente documento il Comune di AREZZO definisce il proprio ambito di titolarità, individua i soggetti a cui delegare, ciascuno per il proprio ambito di competenza, l'attuazione degli adempimenti previsti dalla normativa, indica in via generale i compiti assegnati al DPO designato (per la disciplina puntale si rinvia agli artt. 37-39 del GDPR, nonché allo specifico affidamento del servizio) e definisce i criteri generali da rispettare nell'individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità, come sintetizzato nello schema di seguito riportato.

Il Comune di AREZZO intende, inoltre, creare e promuovere un sistema di accountability nell'ambito della tutela dei dati personali, avvalendosi della collaborazione di tutte le figure coinvolte ai vari livelli. A tale scopo si avvale delle modalità operative ritenute più opportune, anche in relazione allo stato della tecnica (ad esempio fascicolazione sul protocollo, cartelle condivise, cloud, etc.).

Al fine di una chiara distinzione dei ruoli e delle figure, è stabilita nel proseguo una specifica e univoca terminologia per individuare gli attori che intervengono nel trattamento dei dati.

RUOLI NELL'AMBITO DEL MODELLO ORGANIZZATIVO GDPR



Nb: le frecce indicano i soggetti che designano altri soggetti.

2. TITOLARE DEL TRATTAMENTO

Il titolare del trattamento, ai sensi dell'art. 4 n. 7 e dell'art. 24 del Regolamento è il Comune di Arezzo, che agisce tramite gli organi competenti secondo le disposizioni di legge e regolamento.

Spetta al titolare l'adozione di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente alla normativa vigente.

Spetta in particolare al Sindaco, in qualità di legale rappresentante del titolare del trattamento:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi regolativi e dispositivi necessari, con riferimento alla normativa vigente;
- designare il Responsabile della protezione dei dati;
- designare i soggetti delegati all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali e precisamente i responsabili privacy;
- effettuare, a mezzo della struttura organizzativa definita nel presente modello, apposite verifiche sulla osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
- istruire i soggetti autorizzati al trattamento dei dati personali.

3. "RESPONSABILI PRIVACY" e "DELEGATI PRIVACY" INTERNI

In considerazione degli adempimenti rilevanti in tema di trattamento dei dati personali nell'ambito dei compiti e delle funzioni dell'Ente, difficilmente perseguibili direttamente e personalmente dal Titolare, con l'approvazione del presente modello organizzativo, il titolare del trattamento individua e designa i soggetti, cui, all'interno del proprio assetto organizzativo, vengono attribuiti specifici compiti e funzioni connessi al trattamento dei dati, i cd. "Responsabili privacy" e "Delegati privacy".

Detti soggetti dovranno seguire le indicazioni e istruzioni contenute nel presente documento, nonché nell'atto di nomina o nelle relative integrazioni. Per tutto quanto non espressamente previsto nel presente atto, si rinvia alle disposizioni vigenti in materia di protezione dei dati personali.

3.1 RESPONSABILI PRIVACY INTERNI (RPI)

Il Segretario Generale, il Responsabile della Prevenzione della Corruzione e per la Trasparenza (RPCT), i titolari di incarico dirigenziale quali responsabili delle strutture apicali dell'Ente, il Comandante della Polizia Municipale quale Responsabile del Corpo di Polizia Municipale, sono individuati come **"RESPONSABILI PRIVACY INTERNI" (nel seguito definiti RPI)**, in virtù della professionalità posseduta, dell'ambito di attribuzioni, funzioni e competenze conferite, e dato atto che sono in possesso dei requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

Ogni RPI è responsabile del trattamento dei dati effettuato anche con strumenti elettronici o, comunque, automatizzati e/o con strumenti diversi, per l'ambito di attribuzioni, funzioni, competenze attinenti alla propria unità organizzativa (comprese tutte le eventuali sedi e distaccamenti), indicate negli atti organizzativi (funzionigramma) e di nomina (decreto di nomina), per le finalità ivi previste.

Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza.

L'autorizzazione al trattamento e la designazione in qualità di RPI ai soggetti sopra individuati discendono dall'atto di nomina, come previsto dal regolamento sull'ordinamento degli uffici e dei servizi, e dalle disposizioni del presente modello organizzativo.

Il Segretario Generale, e il RPCT se diverso, si intende designato in qualità di RPI per tutta la durata del suo incarico, per le attività di diretta competenza.

Fermo restando il rinvio alla normativa vigente e alle indicazioni/istruzioni specifiche, si evidenzia che ai RPI sono affidati i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
b) disporre, in conseguenza alla verifica di cui alla lettera a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) adottare soluzioni di privacy by design e by default;
d) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
e) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento, renderle conoscibili con i modi e i mezzi ritenuti più opportuni, e assicurarsi che le stesse confluiscano nella "Raccolta comunale delle informative GDPR" istituita con il presente documento;
f) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
g) provvedere, anche tramite i soggetti DELEGATI o AUTORIZZATI, a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
h) disporre l'adozione dei provvedimenti imposti dal Garante, d'intesa con il DPO;
i) adottare, se necessario, specifici disciplinari tecnici di settore, anche congiuntamente con altri soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi al proprio ambito di competenza;
j) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
k) garantire all'Amministratore di sistema e ai suoi collaboratori (vedasi par. 5), al Responsabile dell'unità organizzativa competente in materia di sistemi informativi e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
l) effettuare preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, d'intesa con il DPO, nei casi in cui un trattamento, allorché preveda in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
m) consultare il Garante, d'intesa con il DPO, secondo quanto previsto dall'art. 36 del Regolamento, nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
n) richiamare obbligatoriamente nei contratti di acquisto, utilizzo, sviluppo di software e piattaforme, la disciplina in materia di trattamento dei dati personali e i relativi obblighi e adempimenti;
o) designare i RESPONSABILI ESTERNI del trattamento;
p) designare i DELEGATI PRIVACY INTERNI;
q) individuare e designare i soggetti AUTORIZZATI;
r) segnalare tempestivamente al DPO e all'AdS eventuali violazioni dei dati personali, in modo da consentire al Titolare di procedere agli adempimenti di competenza, di concerto con il DPO e specificatamente alla notifica della violazione al Garante entro 72 ore, a norma dell'art. 33 del GDPR e alla comunicazione agli interessati ex art. 34 del GDPR.
s) in generale, operare nell'ottica e al fine dell'accountability in materia di protezione dei dati.

3.2 DELEGATI PRIVACY INTERNI (DPI)

I/le titolari di posizione organizzativa sono individuati quali **DELEGATI PRIVACY INTERNI (nel seguito definiti DPI)**, limitatamente alle funzioni delegabili ai sensi del vigente regolamento sull'ordinamento degli uffici e dei servizi, in virtù della professionalità posseduta e dell'ambito di attribuzioni, funzioni e competenze conferite, in quanto sono anch'essi in possesso dei requisiti di esperienza, capacità ed affidabilità idonei a garantire il pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati, ivi compreso il profilo relativo alla sicurezza.

I titolari di posizione organizzativa individuati come DPI sono designati dal dirigente gerarchicamente sovraordinato in attuazione delle disposizioni del presente modello organizzativo; la designazione è effettuata all'atto del conferimento della posizione organizzativa, ovvero, se non contestuale, con il medesimo tipo di atto previsto dal Regolamento sull'ordinamento degli uffici e dei servizi.

Ogni DPI è responsabile del trattamento dei dati effettuato anche con strumenti elettronici o, comunque, automatizzati e/o con strumenti diversi, relativamente alle attribuzioni, funzioni, competenze e processi attinenti alla propria unità organizzativa (comprese tutte le eventuali sedi e distaccamenti), come indicate negli atti organizzativi (micro organizzazione) e di nomina (istituzione e conferimento), per le finalità ivi previste.

Fermo restando il rinvio alla normativa vigente e alle indicazioni/istruzioni specifiche, si evidenzia che ai DPI sono affidati i seguenti compiti:

a) verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento e collaborare con il "responsabile privacy" al fine di garantire il corretto trattamento dei dati;
b) disporre, in conseguenza alla verifica di cui alla lettera a), le modifiche necessarie al trattamento perché lo stesso sia conforme alla normativa vigente ovvero disporre la cessazione di qualsiasi trattamento effettuato in violazione alla stessa;
c) adottare soluzioni di privacy by design e by default;
d) tenere costantemente aggiornato il registro delle attività di trattamento per la struttura di competenza;
e) predisporre le informative relative al trattamento dei dati personali nel rispetto dell'art. 13 del Regolamento, renderle conoscibili con i modi e i mezzi ritenuti più opportuni, e assicurarsi che le stesse confluiscano nella "Raccolta comunale delle informative GDPR" istituita con il presente documento;
f) predisporre ogni adempimento organizzativo necessario per garantire agli interessati l'esercizio dei diritti previsti dalla normativa;
g) provvedere a dare riscontro alle istanze degli interessati inerenti l'esercizio dei diritti previsti dalla normativa;
h) disporre, d'intesa con il dirigente e con il DPO, l'adozione dei provvedimenti imposti dal Garante;
i) adottare, se necessario, d'intesa con il dirigente e con il DPO, specifici disciplinari tecnici di settore, anche congiuntamente con altri soggetti delegati all'attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi al proprio ambito di competenza;
j) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate;
k) garantire all'Amministratore di sistema e ai suoi collaboratori (vedasi par. 5), al Responsabile dell'unità organizzativa e al DPO i necessari permessi di accesso ai dati ed ai sistemi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza;
l) effettuare, d'intesa con il dirigente e con il DPO, preventiva valutazione d'impatto ai sensi dell'art. 35 del Regolamento, nei casi in cui un trattamento, allorché preveda in particolare

l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

m) consultare, d'intesa con il dirigente e con il DPO, il Garante, secondo quanto previsto dall'art. 36 del Regolamento, nei casi in cui la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenta un rischio residuale elevato;
n) richiamare obbligatoriamente nei contratti di acquisto, utilizzo, sviluppo di software e piattaforme, la disciplina in materia di trattamento dei dati personali e i relativi obblighi e adempimenti;
o) designare, d'intesa con il dirigente, i RESPONSABILI ESTERNI del trattamento;
p) individuare e designare i soggetti AUTORIZZATI nell'ambito della propria struttura;
q) segnalare tempestivamente al Dirigente, al DPO e all'AdS eventuali violazioni dei dati personali, in modo da consentire al Titolare la notifica della violazione al Garante entro 72 ore, a norma dell'art. 33 del GDPR;
r) in generale, operare nell'ottica e al fine dell'accountability in materia di protezione dei dati.

4. SOGGETTI AUTORIZZATI (SA)

Sono autorizzati al compimento delle operazioni di trattamento dei dati i soggetti di cui al precedente paragrafo 3 ed i soggetti da loro nominati ai sensi del presente paragrafo, definiti AUTORIZZATI.

In particolare, i Responsabili Privacy Interni e i Delegati Privacy Interni individuano e designano formalmente i soggetti AUTORIZZATI al trattamento dei dati ex art. 29 e 32 del GDPR, fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite.

Ogni dipendente del Comune di Arezzo, con l'assegnazione all'unità organizzativa, è da considerarsi AUTORIZZATO ai trattamenti relativi alle attività e ai procedimenti che risultano in capo all'unità organizzativa di assegnazione, come risultanti dal funzionigramma e dal piano di micro organizzazione, dagli atti di organizzazione e dal registro dei trattamenti.

Sono, altresì, AUTORIZZATI tutti i soggetti che effettuino operazioni di trattamento, collaboratori in senso lato e a qualsiasi titolo, che operano sotto la diretta autorità del Titolare o degli RPI/DPI, previa nomina, in sede di stipula del contratto/convenzione/etc. con l'Ente o quale addendum al medesimo.

I Responsabili Privacy Interni individuano negli atti di costituzione di aggregazioni organizzative non previste nell'organigramma e nel funzionigramma (ad esempio team di processo, gruppi di progetto, etc.) comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali AUTORIZZATI, specificando, nello stesso atto di costituzione, anche le relative istruzioni.

I soggetti AUTORIZZATI si impegnano a:

- trattare, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento e solo ai fini dello svolgimento della propria prestazione lavorativa;
- verificare legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere;
- verificare che i dati personali oggetto di trattamento siano adeguati, pertinenti e limitati a quanto necessario per le finalità trattamento stesso;
- informare il proprio Responsabile in tutti i casi in cui si ravvisi la sussistenza di dati eccedenti la finalità perseguita;
- conformare i trattamenti di loro competenza alle policy in materia di protezione dei dati personali e sicurezza informatica adottate dal Titolare del trattamento;
- non trasferire i dati personali trattati a soggetti terzi, se non nei limiti e nel rispetto delle condizioni di liceità assolte dal Titolare del trattamento. Specificatamente, si rappresenta che

le operazioni di comunicazioni e/o diffusione di dati personali sono lecite se previste da norma di legge o regolamento;

- trattare i dati sottoposti a pseudonimizzazione da parte del Titolare con le medesime cautele e accorgimenti previsti per i dati personali;
- prestare particolare attenzione ed attenersi precipuamente alle istruzioni ricevute quando si effettuano trattamenti di dati personali suscettibili di cagionare danni, ovverosia nei casi in cui il trattamento comporta rischi di discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione; se sono trattati dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati;
- fornire al Titolare tutte le informazioni allo stesso utili per determinare il rischio del trattamento effettuato nell'esercizio delle mansioni assegnate;
- modificare o cancellare i dati personali trattati nell'espletamento delle mansioni assegnate solo su specifica istruzione e autorizzazione del Titolare ed evitare operazioni di cancellazione e distruzione dei dati autonomamente determinate;
- avvisare immediatamente, nel caso di istanze che coinvolgano dati personali effettuate anche solo verbalmente dagli interessati, il proprio Responsabile e fornire allo stesso tutte le informazioni che consentano al Titolare di adempiere prontamente alle prescrizioni di legge;
- evitare di richiedere o rintracciare ulteriori dati rispetto a quelli che il Titolare mette a disposizione e che non consentono l'identificazione di una persona fisica. Tuttavia il soggetto AUTORIZZATO non rifiuta le ulteriori informazioni fornite dall'interessato al fine di sostenere l'esercizio dei suoi diritti;
- agevolare, per quanto di propria competenza, il Titolare nell'evasione delle richieste promananti delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica, e la libera circolazione di tali dati;
- conformarsi alle disposizioni di legge e regolamentari, alle circolari e alle indicazioni del Comune di Arezzo in merito all'accesso e all'utilizzo di apparati e servizi informatici;
- adottare, in relazione ai dati trattati, opportuni accorgimenti e idonee misure preventive e di sicurezza in modo da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, accesso non autorizzato, trattamento non consentito o non conforme alle finalità di raccolta:
- collaborare con il proprio responsabile nell'ottica e al fine dell'accountability in materia di protezione dei dati.

5. AMMINISTRATORE DI SISTEMA (AdS)

Il Comune di Arezzo individua l'**Amministratore di sistema (nel seguito AdS)** nel dirigente del Servizio competente in materia di sistemi informativi, ovvero di sicurezza informatica.

L'Amministratore di sistema individua (in base alle indicazioni del GPDP) e coordina le figure preposte alla gestione e alla manutenzione di impianti di elaborazione o di sue componenti, gli amministratori di base di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi, etc.

In relazione a quanto sopra, l'AdS, con propria determinazione organizzativa, individua le seguenti figure e i relativi nominativi (ove del caso d'intesa con i/le Responsabili delle unità organizzative alle quali sono assegnate):

- **Sub-Amministratore di sistema**, che coadiuva l'AdS nello svolgimento dei relativi compiti e funzioni, e lo sostituisce in caso di assenza o impedimento;

- **Operatori AUTORIZZATI**, recando l´elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Stante che l´attività dell'AdS e delle figure summenzionate riguarda anche servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale di lavoratori/lavoratrici, la determinazione organizzativa suddetta è pubblicata sulla sezione intranet del Comune di Arezzo.

L'AdS:

a) individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente. Tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali sono sottoposte a parere preventivo del DPO;

b) condivide le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;

c) supporta la struttura organizzativa, i responsabili privacy, i delegati e autorizzati al trattamento, il DPO, al fine di prevenire incidenti di sicurezza e presta assistenza ogni qualvolta si rende necessario;

d) provvede, ogni qualvolta venga avvertito un problema di sicurezza:

   - ad attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;

   - a segnalare al Responsabile competente in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica, d'intesa con il DPO, ai sensi dell'art. 33 del Regolamento, al GPDP;

   - a individuare misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere del DPO;

e) svolge verifiche sulla puntuale osservanza della normativa e delle policy regionali in materia di sicurezza delle informazioni e di trattamento di dati personali, prevedendo la partecipazione del DPO e realizza le verifiche specifiche richieste dello stesso;

f) promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso azioni comunicative e divulgative all'interno dell'Ente, coordinandosi con le azioni promosse dal DPO.

6. IL GRUPPO DI LAVORO PRIVACY (GDL)

Al fine di garantire correttezza, esattezza e trasparenza del trattamento dei dati, rispetto delle finalità del trattamento e riservatezza, il "modello organizzativo GDPR" del Comune di Arezzo prevede la costituzione di un apposito gruppo di lavoro (definito nel seguito GDL), che funga sia da punto di contatto e di filtro per il DPO, sia nell'ottica dell'accountability.

Il predetto gruppo opera nell'ambito della struttura di supporto al Responsabile per la Prevenzione della Corruzione e per la Trasparenza (RPCT) del Comune di Arezzo, così delineata: il RPCT si avvale della "Segreteria generale" e della rete dei referenti anticorruzione e privacy, costituita dai dirigenti e titolari di posizione organizzativa, nonché dai componenti di apposito "Gruppo di lavoro" (individuati da dirigenti e titolari di p.o. nell'ambito di ciascuna unità organizzativa).

I/le componenti del GDL svolgono un'importante attività informativa e propositiva nei confronti del RPCT, affinché questi possa ricevere dalla struttura organizzativa elementi di conoscenza e riscontri per la formazione e il monitoraggio della strategia.

Nell'ambito del GDL suddetto sono organizzati incontri di confronto e formazione. I/le componenti del GDL svolgono funzioni divulgative di informazioni e documenti nei confronti dei/delle colleghi/e delle relative unità organizzative.

I/le componenti del GDL alimentano la Raccolta comunale delle informative GDPR, acquisendo tempestivamente le informative prodotte nell'ambito del proprio Servizio/Progetto e trasmettendole alla Segreteria generale, che le colleziona e le pubblica in apposita pagina del sito web istituzionale.

I componenti del GDL sono autorizzati a trattare i dati personali nell'ambito dell'unità organizzativa dirigenziale cui afferiscono, per le finalità definite dal presente regolamento e nell'atto di nomina.

Nell'ambito della struttura di supporto al RPCT, questi individua le modalità più opportune per istruire e autorizzare al trattamento dei dati personali le persone coinvolte in ambiti ove la riservatezza assume particolare rilievo, quali il whistleblowing ovvero l'antiriciclaggio. Per la gestione di tali ambiti si rinvia alle specifiche disposizioni normative in materia, al Piano Integrato di Attività e Organizzazione (PIAO) del Comune di Arezzo, e ad altri atti comunali che ne disciplinino gli aspetti (regolamenti, disciplinari, circolari, etc.).

7. IL RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO)

Il "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016" prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).

Il DPO del Comune di Arezzo è preferibilmente esterno all'organizzazione, e individuato per almeno un triennio, eventualmente rinnovabile sino ad un massimo di ulteriori tre anni.

I compiti del DPO, in aderenza agli articoli 37 e seguenti del suddetto regolamento, sono conformati alla precipua organizzazione del Comune di Arezzo in sede di affidamento del relativo servizio.

Il DPO è designato con provvedimento del Titolare.

Possono presentare richieste di pareri e/o di valutazioni di impatto privacy (DPIA) al DPO i Responsabili privacy e i delegati privacy, nonché i soggetti autorizzati per il tramite dei primi ed anche per il tramite dei relativi componenti del GDL di cui al paragrafo 6) e l'Amministratore di sistema (anche per tramite del Sub-Amministratore).

Le predette richieste devono essere inviate dai soggetti sopra definiti ad apposito indirizzo di posta elettronica del Comune di Arezzo che inoltra le email verso uno o più indirizzi di posta elettronica forniti dal DPO, e inviate per conoscenza ad apposito indirizzo di posta elettronica del Comune di Arezzo ad uso interno nell'ambito del presente modello organizzativo).

Il DPO potrà richiedere integrazioni e informazioni alle unità organizzative richiedenti, al fine di fornire un tempestivo riscontro alle richieste di pareri o di DPIA. Il parere del DPO è rilasciato entro il termine massimo di 5 giorni, salvo i casi di richieste urgenti (da evadersi entro 24 ore dal ricevimento), ovvero i casi in cui sarà necessario, preliminarmente, interloquire con il Garante.

Le richieste ed i pareri espressi dal DPO sono conservati agli atti dell'Ente tramite acquisizione al protocollo informatico.

8. RESPONSABILI DEL TRATTAMENTO ESTERNI (RE)

Sono designati RESPONSABILI ESTERNI del trattamento di dati personali i soggetti esterni all'amministrazione (persone fisiche o giuridiche) che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare.

Pertanto, qualora occorra affidare un incarico o servizio comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata nell'ambito della stipula di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

La designazione dei responsabili esterni è di competenza del Dirigente preposto all'unità organizzativa, ovvero del Delegato Privacy Interno se delegato.