CITTA' DI SANTARCANGELO DI ROMAGNA
Provincia di Rimini

DECRETO N. 2/SG Santarcangelo di Romagna, 21.09.2018

OGGETTO: ISTITUZIONE GRUPPO DI COORDINAMENTO PRIVACY, TRASPARENZA E ACCESSO, COORDINATO DAL SEGRETARIO GENERALE E INCARDINATO RIGUARDO ALLA FUNZIONE GESTIONALE NEI SERVIZI AMMINISTRATIVI

IL SEGRETARIO GENERALE

Premesso che:

- Il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)» (di seguito RGPD), in vigore dal 24 maggio 2016, è applicabile dal 25 maggio 2018;

- uno degli elementi di novità introdotti dal Regolamento è rappresentato dal principio della responsabilizzazione (accountability – art.24), secondo il quale spetterà al titolare del trattamento, e, dunque all'Ente Comune, con onere di prova, dimostrare di aver predisposto tutte le misure tecniche ed organizzative utili a soddisfare i dettami del legislatore ed a ridurre in tal modo il rischio di violazioni in materia di protezione dei dati personali;

- che il legislatore ha introdotto una figura obbligatoria per tutte le pubbliche amministrazioni, qualificandola come Responsabile della protezione dei dati personali (RPD)(art.37), dotato di comprovate competenze giuridiche, con particolare riferimento alla normativa in tema di privacy e significative esperienze lavorative nel settore del data protection, cui può essere affiancato un ufficio di supporto, che funga da tramite fra il responsabile della protezione dei dati e la struttura;

- che, dunque, le novità introdotte dal Regolamento Europeo disegnano una fase di implementazione organizzativa di un vero e proprio team funzionale;

Considerato altresì che stato pubblicato il D.Lgs. 10.08.2018 n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)";

Visto il decreto sindacale di nomina di Lepida S.p.A. a responsabile dei dati personali (DPO) con atto n. 19 del 25/05/2018;

Ricordato che al segretario comunale del Comune è anche responsabile per la prevenzione della Corruzione e della Trasparenza, destinatario delle istanze di accesso civico semplice e del riesame delle istanze di accesso civico generalizzato, e deve occuparsi anche degli aspetti di privacy in raccordo alle procedure di tutela della trasparenza, alle procedure di accesso civico, alle procedure anticorruzione;

Valutata, quale misura di buon andamento ed efficienza dell'azione ammniistrativa, di istituire un gruppo di coordinamento Privacy, Trasparenza e Accesso, coordinato dal Segretario comunale e incardinato riguardo alla funzione gestionale nei Servizi Amministrativi, che funga anche da supporto agli altri uffici e servizi nella gestione delle istanze che coinvolgano gli ambiti sopra riportati, secondo il modello organizzativo privacy predisposto per dare attuazione agli obblighi e adempimenti a carico dei soggetti che trattano dati personali, allegato sub "A" al presente atto;

Vista, poi, la delibera di Giunta n. 15 del 06.02.2018 "Costituzione dell' ufficio della transizione al digitale ex art. 17 del d.lgs. 82/2005, aggiornato con le modifiche e integrazioni introdotte dal d.lgs. 217/2017, e nomina del responsabile", che prevede l'inserimento dell'ufficio in Staff al Sindaco, in osservanza alle disposizioni di cui al comma 1 ter dell'art.17 del CAD (aggiornato con le modifiche e integrazioni introdotte dal Decreto Legislativo n. 217 del 13 dicembre 2017);

Vista anche la delibera di Giunta n. 37 del 16.03.2018, esecutiva ai sensi di legge, con la quale è stato approvato il Piano Esecutivo di Gestione per l'anno 2018, in cui, nell'ambito delle assegnazioni di personale, la Giunta ha espresso la volontà di dare impulso prioritario alle attività legate allo sviluppo della promozione turistica, nonché al rafforzamento della struttura di pianificazione urbanistica, particolarmente impegnata nei prossimi mesi per l'esecuzione e il completamento dei piani approvati dal Consiglio comunale, stabilendo pertanto di dover dar seguito ai predetti indirizzi, istituendo una nuova unità operativa denominata "Ambiente e Turismo";

Vista infine la determinazione AMM/136 del 07.05.2018 di definizione dei servizi e degli uffici del Comune di Santarcangelo di Romagna per l'anno 2018, in cui viene istituita l'unità operativa denominata "Ambiente e Turismo" come servizio in staff al dirigente del settore Territorio;

DECRETA

1. di richiamare e confermare quanto sin qui espresso;

2. di istituire gruppo di coordinamento Privacy, Trasparenza e Accesso, coordinato dal Segretario comunale e incardinato riguardo alla funzione gestionale nei Servizi Amministrativi;

3. di precisare che tale ufficio sarà a supporto del Responsabile per la protezione dei dati, per quanto riguarda la privacy, oltre che a supporto anche del resto della struttura riguardo alle procedure di tutela della trasparenza, alle procedure di accesso civico, alle procedure anticorruzione e alla protezione dei dati;

4. approvare il modello organizzativo privacy, allegato sub "A" al presente atto;

5. approvare l'organigramma, allegato sub "B" al presente atto, aggiornato con l'istituzione del gruppo di coordinamento Privacy, Trasparenza e Accesso, dell'Ufficio per la Transizione al Digitale e dell'ufficio Ambiente e Turismo;

6. di trasmettere il presente atto al Sindaco, alla Giunta, all'Ufficio Unico del Personale dell'Unione di Comuni Valmarecchia e alle P.O. del Comune di Santarcangelo di Romagna.

7. di pubblicare il presente atto nel sito web istituzionale dell'Ente, sia nell'Albo Pretorio online, sia nella sezione Amministrazione trasparente

IL SEGRETARIO GENERALE
Dr.ssa Lia Piraccini
(documento firmato digitalmente)

Allegato A

MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Sommario

Indirizzi generali

Il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (di seguito "Regolamento"), abroga la direttiva 95/46/CE e detta una complessa disciplina di carattere generale in materia di protezione dei dati personali, prevedendo molteplici obblighi e adempimenti a carico dei soggetti che trattano dati personali, comprese le pubbliche amministrazioni.

Con D.Lgs. 10.08.2018 n. 101 ad oggetto "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione del dati)" sono state emanate le disposizioni di adeguamento della normativa nazionale (D.Lgs. 196/2003) alle disposizioni del Regolamento stesso.

Per dare attuazione a questi obblighi, occorre rivedere l'assetto delle responsabilità tenendo conto della specifica organizzazione del Comune di Santarcangelo.
Il Regolamento individua diversi attori che intervengono nei trattamenti di dati personali effettuati dalle organizzazioni, ciascuno con funzioni e compiti differenti:

- il 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 (Comune di Santarcangelo – organi politico - amministrativi);
- il contitolare del trattamento: due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento (Unione di Comuni Valmarecchia)
- il responsabile esterno del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento (ad es. i fornitori);
- il Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO):

figura prevista dall' articolo 37 e successivi del Regolamento, che ne disciplinano compiti, funzioni e responsabilità;

- le persone autorizzate (o incaricati) al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figure che si desumono implicitamente dalla definizione di "terzo" presente al punto 10 dell'articolo 4, comma 1 del Regolamento (dipendenti comunali);
- il designato: figura introdotta dal D.Lgs. 101/2018 sopra citato: una persona fisica designata espressamente dal Titolare o dal Responsabile del trattamento, operante sotto la sua volontà, per specifici compiti e funzioni connessi al trattamento di dati personali nell'ambito dell'assetto organizzativo dell'Ente

Con il presente documento l'Ente definisce il proprio ambito di titolarità, individua i soggetti competenti all'attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al DPO designato 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 riportato di seguito.

Il titolare (Comune di Santarcangelo di Romagna – organi politico-amministrativi)

Titolare del trattamento dei dati personali, in base agli articoli 4, punto 7 e 24 del Regolamento è l'Ente cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che il trattamento è

effettuato conformemente al Regolamento stesso. Spetta pertanto all' Ente, nelle rispettive attribuzioni del Sindaco, del Consiglio Comunale e della Giunta Comunale :

● adottare gli interventi normativi necessari, nelle forme previste dal proprio ordinamento, anche con riferimento alle disposizioni del D.Lgs. 101/2018;
● designare il Responsabile della protezione dei dati (decreto di nomina da parte del Sindaco);
● individuare i soggetti competenti all'attuazione degli adempimenti previsti dalla normativa in materia di trattamento di dati personali;
● effettuare, a mezzo della struttura competente individuata (Gruppo Coordinamento privacy, trasparenza e accesso), apposite verifiche sull'osservanza delle disposizioni vigenti in materia di trattamento, compresi i profili relativi alla sicurezza informatica, in collaborazione con il DPO designato;
● istruire i soggetti autorizzati (o incaricati) al trattamento dei dati personali.

I contitolari (Unione di Comuni Valmarecchia)

In base a quanto previsto dal Regolamento, la protezione dei diritti e delle libertà degli interessati esige una chiara ripartizione delle responsabilità, compresi i casi in cui un titolare del trattamento stabilisca le finalità e i mezzi del trattamento congiuntamente con altri titolari del trattamento stesso.
I contitolari del trattamento determinano in modo trasparente**,** mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato e le rispettive funzioni di comunicazione delle informazioni previste agli articoli 13 e 14 del Regolamento.
L'accordo citato riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati; il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Persone autorizzate (o incaricati)

Sono tutti i soggetti autorizzati ad effettuare operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo che operano sotto la diretta autorità del Titolare.
Gli incaricati sono designati tramite individuazione nominativa (nome e cognome) delle persone fisiche. Occorre specificare per ciascun nominativo i trattamenti che lo stesso è autorizzato ad effettuare; la designazione scritta deve inoltre contenere le istruzioni impartite agli incaricati del trattamento.
Tali istruzioni, oltre a riguardare eventuali aspetti di dettaglio da diversificare in relazione alle specificità dei singoli trattamenti, devono quanto meno contenere un espresso richiamo alla policy dell'Ente in materia di sicurezza informatica e protezione dei dati personali.

I responsabili esterni del trattamento (ad es. i fornitori)

Sono designati responsabili del trattamento di dati personali i soggetti esterni all'amministrazione 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 comportante anche il trattamento di dati personali, la scelta del soggetto dev'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 disposizioni vigenti in materia di trattamento, compreso quanto previsto sotto il profilo della sicurezza.
Attesa la natura negoziale delle designazioni dei responsabili del trattamento, questa deve essere effettuata all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale.

Servizio competente in materia di sistemi informativi (Unione di Comuni Valmarecchia)

Al servizio competente in materia di sistemi informativi (ICT), compresa la sicurezza informatica, spetta:
- l'adozione di policy in materia di privacy e sicurezza informatica, con particolare riferimento all'utilizzo, alla sicurezza delle risorse informatiche e allo sviluppo delle applicazioni informatiche, da aggiornare periodicamente, ogni qualvolta l'evoluzione tecnica o normativa lo renda necessario;
- la sottoscrizione degli atti di notifica e di consultazione preventiva al Garante;
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo prevista agli articoli 33 e 34 del Regolamento.

Il Servizio competente in materia di sistemi informativi, compresa la sicurezza informatica, svolge un ruolo di supporto al DPO in tema di risorse strumentali e competenze.
Al fine di coordinare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il Servizio i compiti di seguito meglio specificati:
- individuare le misure più adeguate ed efficaci per la tutela e riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente; tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali, come ad esempio le linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e i disciplinari tecnici trasversali, sono sottoposte a parere preventivo obbligatorio del DPO;

● condividere le evidenze dell'analisi dei rischi con il DPO, il quale fornisce parere obbligatorio sulle misure poste a mitigazione del rischio che abbiano un significativo impatto sulla protezione dei dati personali;
● provvedere, 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;
  – individuare misure idonee al miglioramento della sicurezza del trattamento dei dati personali, previo parere obbligatorio del DPO;
  – segnalare al Responsabile in materia di sistemi informativi le violazioni dei dati personali ai fini della notifica al Garante per la protezione dei dati personali, prevista all'articolo 33 del Regolamento;
● svolgere verifiche sulla puntuale osservanza della normativa e della policy dell'Ente in materia di sicurezza delle informazioni e di trattamento dei dati personali prevedendo la partecipazione del DPO, nonchè realizzare le verifiche specifiche richieste dello stesso;
● promuovere la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione interna, coordinandosi con le azioni promosse dal DPO.

Il Responsabile della Protezione dei dati (DPO)

Il Regolamento prevede l'obbligo per gli Enti pubblici di designare il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO).
Di seguito sono indicati i compiti attribuiti al DPO in aderenza all'articolo 37 e successivi del Regolamento, conformati alla specifica organizzazione dell'Ente:
● informare e fornire consulenza all'Ente in merito agli obblighi derivanti dalla normativa in materia di protezione dei dati personali, con il supporto del gruppo dei referenti designati dalle singole strutture;
● sorvegliare l'osservanza della normativa e delle politiche dell'Ente in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle attività di controllo connesse;
● cooperare con il Garante per la protezione dei dati personali;
● fungere da punto di contatto con l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva prevista all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relative a qualunque altra questione;
● partecipare allo svolgimento delle verifiche di sicurezza svolte dal Responsabile del servizio ICT competente o richiederne di specifiche;

● promuovere la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;
● partecipare alla gestione degli incidenti di sicurezza nelle modalità previste dalla specifica policy dell'Ente;
● formulare gli indirizzi per realizzazione del Registro delle attività di trattamento previsto all'articolo 30 del Regolamento;
● fornire i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

Pareri del DPO

Il DPO fornisce il proprio parere in ordine alla legittimità e alla correttezza dei trattamenti di dati personali sulle istanze che le strutture dell'Ente presentano nei casi di seguito indicati.

Pareri obbligatori

Devono essere obbligatoriamente richiesti pareri in ordine a:
● individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela di riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche in seguito a incidenti di sicurezza o analisi dei rischi;
● adozione di policy e disciplinari in materia di protezione dei dati personali e sicurezza delle informazioni, redazione e aggiornamento dei disciplinari tecnici con impatto sulla sicurezza delle informazioni;
● individuazione di misure per la mitigazione delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
● incidenti di sicurezza.

Pareri facoltativi

Possono inoltre essere richiesti, se ritenuti utili, pareri in ordine a:
● progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza ai principi della *privacy by design e by default*;
● valutazione d'impatto sulla protezione dei dati in base all'articolo 35 del Regolamento;
● valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali come previsto dal comma 2 dell'articolo 5-bis e, in via generale, dal Regolamento;

● opposizione formulata dai controinteressati nella misura in cui questa sia riferibile alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.
Le richieste di parere devono essere inviate all'indirizzo di posta elettronica DPO-TEAM@LEPIDA.IT, nelle modalità stabilite dall'Ente.
I pareri sono espressi nel rispetto delle seguenti codifiche:
● NC: acronimo di "non conformità", nei casi in cui siano rilevati elementi di non conformità alla normativa e alle policy in materia di protezione dei dati personali;
● OS: acronimo di "osservazione", nei casi in cui vi siano elementi di miglioramento che garantiscono una maggiore aderenza alla normativa e alle policy in materia di protezione dei dati personali, non costituendo vincolo di attuazione;
● PO: acronimo di "positivo", nei casi in cui siano prospettati elementi valutati come conformi alla normativa e alle policy in materia di protezione dei dati personali.
Nei casi in cui il DPO esprima pareri "NC" e "OS" i soggetti competenti (nei vari casi, gli incaricati o i responsabili esterni o i designati) devono formalizzare nelle medesime forme utilizzate dal DPO per l'espressione del parere, le motivazioni che giustificano l'esecuzione dell'attività o l'implementazione della soluzione tecnologica in contrasto alle indicazioni fornite dal DPO.
I pareri espressi dal DPO sono conservati agli atti.

Il Gruppo di Coordinamento privacy, trasparenza e accesso

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento la costituzione di un gruppo permanente di referenti privacy che assicuri un presidio per le strutture dell'Ente in relazione agli adempimenti continuativi, allo studio e all'approfondimento degli aspetti normativi, organizzativi e procedurali derivanti anche dalle nuove disposizioni normative.
Il Gruppo di Coordinamento ha i seguenti compiti:
● collaborare all'elaborazione della modulistica interna di applicazione della normativa privacy, nonché supportare gli uffici dell'Ente nelle tematiche relative a trasparenza e accesso;
● effettuare la ricognizione costante dei trattamenti di dati personali effettuati, a mezzo del registro dei trattamenti;
● fornire supporto alle verifiche di sicurezza svolte dal Servizio competente in materia di sistemi informativi e/o dal DPO;
● collaborare alla revisione e all'aggiornamento dei disciplinari tecnici;
● coordinare le richieste di parere al DPO nei casi e con le modalità previsti dal presente documento.

Accesso civico generalizzato e ruolo DPO

Con specifico riferimento alla normativa in materia di trasparenza, si ritiene opportuno disciplinare la necessaria interazione tra il DPO, le strutture dell'Ente e il Responsabile per la prevenzione della corruzione e trasparenza (R.P.C.T.).

Il D.L. 97/2016, di modifica del D.lgs. 33/2013 ha introdotto l'istituto dell'accesso civico "generalizzato", che attribuisce a "chiunque" il diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione.

L'esercizio di tale diritto soggiace ai limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis" del D.Lgs. n. 33/2013.

L'articolo 5, comma 5 del D.Lgs. n. 33/2013 prevede che, per ciascuna domanda di accesso generalizzato, l'amministrazione debba verificare l'eventuale esistenza di controinteressati, eccetto i casi in cui la richiesta di accesso civico abbia a oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria.

Il DPO funge da supporto alle strutture competenti sulle singole richieste di accesso nella fase di individuazione dei soggetti da ritenersi contro interessati, e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.

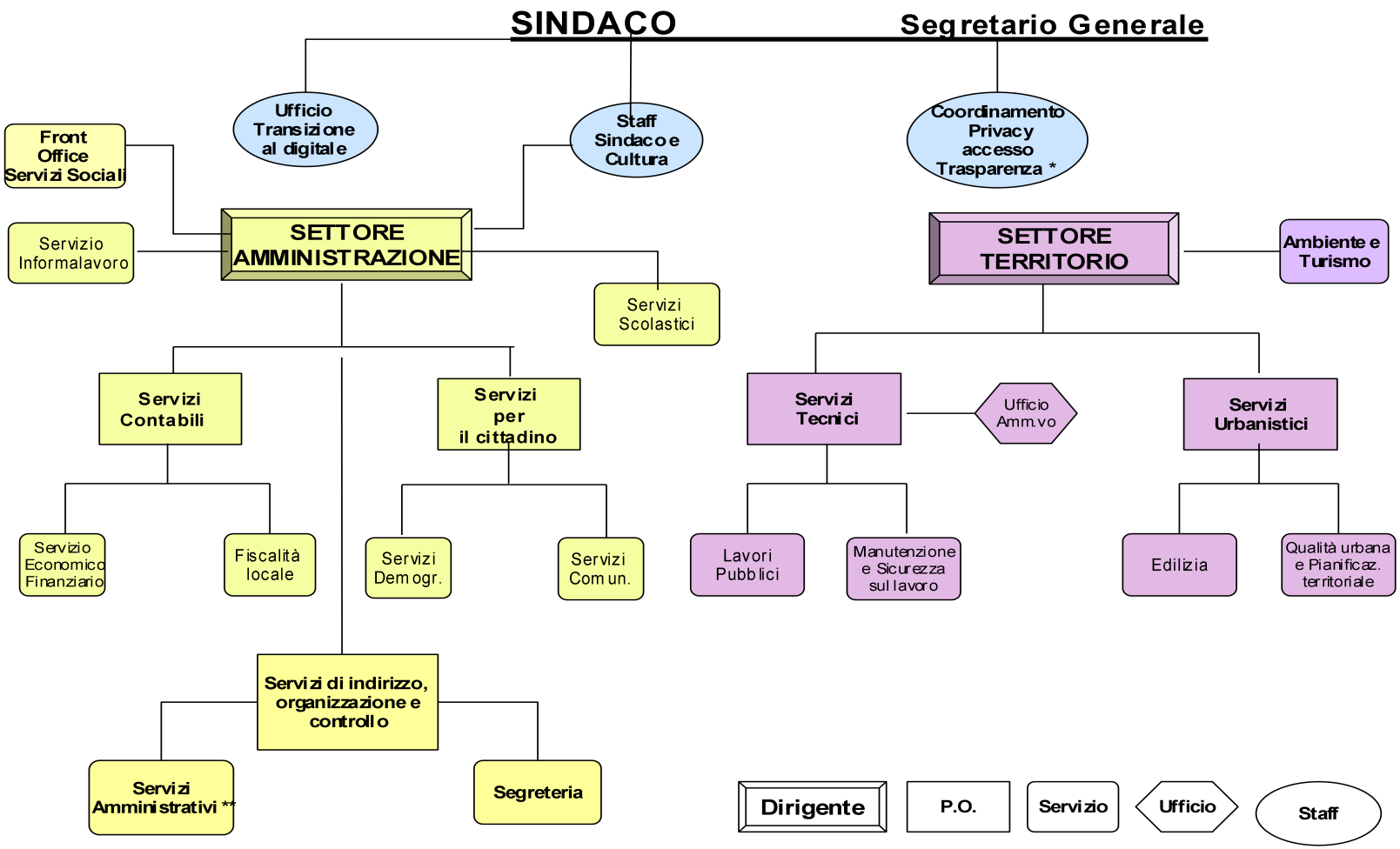
Il DPO funge anche da supporto al R.P.C.T. nei casi di riesame delle istanze di accesso negato o differito a tutela dell'interesse alla protezione dei dati personali.

Il DPO, inoltre, su richiesta delle strutture esprime proprio parere in merito all'eventuale pregiudizio che l'accesso potrebbe comportare ai controinteressati, nella misura in cui questo riguardi la tutela dei loro dati personali in base a quanto previsto dall'articolo 5-bis, comma 2 e, in generale, del Regolamento.

Su richiesta delle strutture, sempre il DPO formula entro tre giorni il proprio parere in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Sulla scorta di tale parere le strutture competenti sulle singole richieste di accesso effettueranno il bilanciamento tra gli interessi presumibilmente lesi e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare

Allegato B



* La funzione gestionale di Privacy – accesso - trasparenza è incardinata nei Servizi Amministrativi

** Per la parte di Privacy – accesso – trasparenza il coordinamento è del Segretario Generale