COMUNE DI TRESIGNANA

Provincia di Ferrara

DELIBERAZIONE DEL COMMISSARIO PREFETTIZIO
NELL'ESERCIZIO DEI POTERI DELLA GIUNTA

Deliberazione n. 19 del 18-03-2019

OGGETTO: APPROVAZIONE DEL "MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" DEL COMUNE DI TRESIGNANA AI SENSI DEL REGOLAMENTO UE 2016/679

L'anno duemiladiciannove il giorno diciotto del mese di marzo alle ore 13:00 presso la solita sala delle adunanze.

Il Commissario Prefettizio Dott.ssa Adriana Sabato, con l'assistenza del Segretario Comunale Musco Antonino, in virtù dei poteri conferiti con Decreto del Prefetto di Ferrara Prot. 72667/2018 allo svolgimento delle funzioni del Consiglio e della Giunta.

IL COMMISSARIO PREFETTIZIO

Premesso che:

- con L.R. n. 16 del 05/12/2018 è stato istituito a decorrere dal 1.1.2019 il comune di Tresignana, nato dalla fusione fra i comuni di Tresigallo e Formignana;
- con Decreto del Prefetto della Provincia di Ferrara prot. num. 72667/2018 del 19/12/2018 è stata nominata Commissario Prefettizio la Dott.ssa Adriana Sabato per la provvisoria amministrazione del nuovo ente ai sensi dell'art. 19 del R.D. 03/03/1934, n. 383;
- con il suddetto decreto al commissario sono conferiti i poteri spettanti al sindaco, alla giunta e al consiglio comunale;

Dato atto che:

- il 24/05/2016 è entrato in vigore il Regolamento UE 2016/679 sulla protezione dei dati personali (di seguito, Regolamento UE o GDPR), che dispiega efficacia negli ordinamenti nazionali a partire dal 25/05/2018;
- le ragioni dell'adozione di una nuova disciplina europea sono illustrate nei considerando del Regolamento UE e sono riconducibili all'obsolescenza dei sistemi giuridici tradizionali, a fronte dell'evoluzione tecnologica, alla necessità di creare strumenti sovranazionali per la protezione dei dati, superando le divergenze delle legislazioni nazionali e alla necessità di creare un sistema di norme vincolanti anche per le imprese di Stati terzi, stabilite o prestatori di servizi nell'UE;
- con l'art. 13 della legge 25 ottobre 2017, n. 163, il Governo è stato delegato ad adottare uno o più provvedimenti, in fase di emanazione, rivolti a: abrogare le disposizioni del Decreto Legislativo n. 196/2003 (l'attuale Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del Regolamento, valutare l'opportunità di avvalersi dei poteri specifici del Garante per la protezione dei dati personali affinché adotti provvedimenti attuativi e integrativi; adeguare l'attuale regime sanzionatorio, a livello penale e amministrativo, al fine di garantire la corretta osservanza della nuova normativa;
- il D.Lgs. 10/08/2018 n. 101 pubblicato nella G.U. del 04/09/201/, n. 205 ha introdotto le disposizioni di adeguamento della normativa nazionale (D.Lgs. 193/2003) alle disposizioni del Regolamento UE di cui sopra;

Considerato che il Regolamento UE introduce significative innovazioni nel quadro normativo nazionale, determinando l'avvio di un percorso di adeguamento, che rappresenta un'opportunità, oltre che un adempimento, per migliorare, standardizzare e rendere maggiormente sicuri i processi, nonché per procedere ad una razionalizzazione dei flussi di dati all'interno dell'Ente, a beneficio degli utenti;

Richiamati in particolare:

- il principio di accountability" o "responsabilizzazione", che pone in capo al titolare il compito di adottare comportamenti attivi e tali da dimostrare la concreta adozione di misure "idonee" finalizzate ad assicurare l'applicazione del Regolamento;
- i principi di "privacy by design" a di "privacy by default", ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento e tutelare i diritti dell'interessato;
- l'obbligo di effettuare una "valutazione d'impatto", allorché il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche;

- l'obbligo di notifica delle "violazioni" dei dati personali dalle quali derivino rischi per i diritti e le libertà degli interessati;
- l'obbligo di tenere un "registro delle attività di trattamento", allo scopo di disporre di un quadro aggiornato dei trattamenti in essere da esibire su richiesta al Garante per la protezione dei dati personali;
- l'obbligo di designare un "Responsabile della protezione dei dati" (DPO), dotato di qualità professionali e conoscenza specialistica, da coinvolgere in tutte le questioni riguardanti il trattamento dei dati;

Atteso che, al fine di garantire una gestione efficace ed efficiente dei requisiti normativi in un'ottica di continuo miglioramento, il Comune di Tresignana intende dotarsi di un sistema strutturato per la *governance* della privacy, il cui processo di dispiegamento è articolato in tre fasi, ed in particolare:
1. fase ricognitiva: consiste nella mappatura dei trattamenti di dati, comprendente le categorie di dati ed interessati, gli attori che intervengono nel trattamento con indicazione dei ruoli e delle responsabilità, e le misure tecniche ed organizzative per la protezione dei dati;
2. fase di progettazione: consiste nella predisposizione di un "Modello organizzativo in materia di protezione dei dati personali" che, sulla scorta della ricognizione effettuata, definisca l'assetto organizzativo che il Comune di Tresignana intende implementare per governare i processi di gestione della privacy, con l'individuazione delle figure coinvolte nel trattamento dei dati (Titolare, Contitolare, DPO, Coordinatori, Incaricati, ecc..) e dei relativi ruoli e responsabilità;
3. fase di implementazione e di gestione della protezione dei dati: consiste nell'esecuzione delle attività di analisi d'impatto, di trattamento del rischio, di interazione con la nuova figura del DPO, di adeguamento delle politiche e delle procedure di protezione dei dati adottate dall'Ente e di erogazione di servizi di sicurezza dei sistemi informativi.

Dato atto che:

- con deliberazione del Commissario Prefettizio n. 12 del 28/01/2019 si è disposto il subentro nello affidamento a Lepida S.p.A. di servizi inerenti l'attuazione della nuova normativa sulla protezione dei dati personali (GDPR) di cui al Regolamento UE 2016/679 nell'ambito dei quali viene fornita una piattaforma denominata "RecordER" per la gestione e manutenzione del registro dei trattamenti a norma di Legge e proposto un modello organizzativo per la governance della privacy condiviso con le Comunità Tematiche della Regione Emilia-Romagna, per l'omogeneizzazione dei processi a livello regionale;
- con la sopra citata deliberazione è stato stabilito inoltre che il Settore Servizi Informativi e Telematici dell'Unione, opererà come unità organizzativa di coordinamento tra i Comuni e l'Unione, nei rapporti con LEPIDA, per l'adozione di sistemi di protezione dei dati automatizzati e per garantire interpretazioni ed applicazioni uniformi della normativa in tema di Tutela dei Dati Personali, nonchè per le funzioni di coordinamento e per il ruolo di interlocutore unico di LEPIDA S.P.A. per i Comuni e l'Unione, per le funzioni operative ed organizzative previste dal contratto afferente i servizi offerti da Lepida S.p.A. per l'attuazione della nuova normativa in tema di protezione dei dati personali; - il registro dei trattamenti del Comune di Tresignana è in corso di predisposizione e riversamento nella succitata piattaforma, e che, come previsto dal modello organizzativo, verrà richiesto al DPO di formulare indirizzi e pareri in ordine alla corretta realizzazione del medesimo;

Visto il “Modello organizzativo in materia di protezione dei dati personali” che si allega al presente atto e che dello stesso forma parte integrante e sostanziale, con il quale il Comune di Tresignana definisce il proprio ambito di titolarità, incarica i dirigenti ed il personale, ciascuno per il proprio ambito di competenza, per l’attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al DPO e definisce i criteri generali da rispettare nell’individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità;

Visto che l’ex Comune di Formignana con DCC n. 34 del 23.11.2012 e l’ex Comune di Tresigallo con DCC n. 37 del 19.11.2012 hanno approvato la convenzione per il trasferimento all'Unione dei Comuni Terre e fiumi delle funzioni relative al personale;

Visto che l’ex Comune di Formignana con DCC n. 39 del 20.12.2012 e l’ex Comune di Tresigallo con DCC n. 36 del 19.12.2012 hanno approvato la convenzione per il trasferimento all'Unione dei Comuni Terre e Fiumi delle funzioni, compiti ed attività relative alla gestione dei servizi informatici e telematici;

Dato atto che in conseguenza dell’approvazione del Modello organizzativo in materia di protezione dei dati personali e della nomina del DPO, nonchè del Responsabile per la transizione in modalità digitale, i soggetti incaricati daranno avvio alle necessarie attività per garantire la piena conformità al Regolamento dei processi di gestione della privacy, ciascuno nel proprio ambito di competenza, in collaborazione con il DPO;

Dato atto che sulla proposta in esame è stato espresso il parere favorevole del Responsabile del Servizio Segreteria e SS.DD. ai sensi dell’art. 49 del Tuel 267/2000 ed è stata svolta, da parte del Segretario Comunale, la funzione di assistenza giuridico-amministrativa, ai sensi dell’art. 97 comma 2 del Testo Unico delle leggi sull’ordinamento degli Enti Locali, approvato con D.Lgs. 18/08/2000 n. 267 e che lo stesso, su richiesta del Commissario Prefettizio, attraverso la sottoscrizione del presente atto, esprime parere favorevole ordine alla conformità dell’azione amministrativa alle leggi, agli statuti ed ai regolamenti;

DELIBERA

Per quanto alle premesse;

- di approvare il “Modello organizzativo in materia di protezione dei dati personali” che si allega al presente atto e che dello stesso forma parte integrante e sostanziale, con il quale il Comune di Tresignana definisce il proprio ambito di titolarità, i responsabili ed il personale, ciascuno per il proprio ambito di competenza, per l’attuazione degli adempimenti previsti dalla normativa, indica i compiti assegnati al DPO e definisce i criteri generali da rispettare nell’individuazione dei soggetti autorizzati a compiere le operazioni di trattamento, delineando il complessivo ambito delle responsabilità;

- di incaricare il responsabile del Settore Segreteria e SS.DD. di:
  - dare esecuzione al presente provvedimento;
  - trasmettere il presente atto al D.P.O. (Lepida SpA)
  - trasmettere il presente atto ai Servizi Informativi dell'Unione Terre e Fiumi per la verifica dell'esecuzione del modello organizzativo, paragrafo 2.9;

- di incaricare il Segretario Comunale di programmare la formazione del personale di concerto con l'Ufficio del Personale dell'Unione Terre e Fiumi;

- di dichiarare la presente deliberazione immediatamente eseguibile, ai sensi dell'art. 134 comma 4 del D.lgs. 267/2000, stante l'urgenza di provvedere.

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

IL COMMISSARIO	IL SEGRETARIO
Sabato Adriana	Musco Antonino

COMUNE DI TRESIGNANA

Provincia di Ferrara

Piazza Italia, 32 – 44039 –Tresignana loc. Tresigallo –
Sede distaccata: Via Vittoria, 29 – 44035 – Tresignana – loc. Formignana

Modello organizzativo in materia di protezione dei dati personali del comune di Tresignana

INDICE

1. INDIRIZZI GENERALI

1.1 - PREMESSE

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 (di seguito anche solo "Regolamento") 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.

Il D.Lgs 10.8.2018 n. 101 pubblicato nella G.U del 4.9.2018 n. 205 ha introdotto le disposizioni di adeguamento della normativa nazionale (D.Lgs. 196/2003) alle disposizioni del Regolamento UE di cui sopra.

Per dare attuazione ai suddetti obblighi ed adempimenti, occorre rivedere l'assetto delle responsabilità tenuto conto della specifica organizzazione del Comune di Tresignana

Il regolamento europeo 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;
- il responsabile 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;
- Responsabile della protezione dei dati (di seguito anche Data Protection Officer o DPO): figura prevista dagli artt. 37 e ss. del regolamento, che ne disciplinano compiti, funzioni e responsabilità;
- persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile: figura che si desume implicitamente dalla definizione di "terzo" di cui al n. 10 del comma 1 art. 4 del Regolamento.

Con il presente documento il Comune di Tresignana incarica i responsabili ed il personale, ciascuno per il proprio ambito di competenza, per l'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 di seguito riportato.

1.2. - STRUTTURA ORGANIZZATIVA

La struttura organizzativa del Comune di Tresignana si compone dei seguenti n. 4 settori:

SETTORE SEGRETERIA E SS.DD
SETTORE SERVIZI ALLA PERSONA
SETTORE FINANZIARIO
SETTORE LL.PP AMBIENTE MANUTENZIONI

Ad ogni settore è preposto un Responsabile, nominato con provvedimento del Sindaco, cui competono le funzioni previste dall'art. 107 del D.Lgs. 18/08/2000 n. 267 relativamente alle materie riferibili ai servizi compresi nel settore.

2. MODELLO ORGANIZZATIVO

2.1 - IL TITOLARE

Titolare dei trattamenti di dati personali, ai sensi dell'art. 4 n. 7 e art. 24 del Regolamento, è il **Comune di Tresignana,** nella persona del Legale Rappresentante, cui spetta l'adozione di misure tecniche e organizzative adeguate per garantire che il trattamento è effettuato conformemente al Regolamento. Spetta pertanto in particolare al Comune:

- adottare, nelle forme previste dal proprio ordinamento, gli interventi normativi necessari, anche con riferimento alle disposizioni del Codice per la protezione dei dati personali;
- 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;
- effettuare, a mezzo della struttura competente, 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;
- favorire la formazione dei soggetti autorizzati al trattamento dei dati personali.
- la notifica e la comunicazione delle violazioni dei dati personali all'autorità di controllo ai sensi degli artt. 33 e 34 del Regolamento.

2.2 - I RESPONSABILI DEL TRATTAMENTO DEI DATI

Sono designati quali soggetti attuatori degli adempimenti necessari per la conformità dei trattamenti di dati personali effettuati dall'Ente in esecuzione del regolamento i **Responsabili di settore** ciascuno per il proprio ambito di competenza. I Responsabili di settore sono designati quali responsabili del trattamento dei datii afferenti il Settore di competenza.

Relativamente ai trattamenti di dati personali trasversali a più strutture si applica il criterio della prevalenza.
Di seguito, sono indicati i compiti affidati ai Responsabili del Trattamento dei dati, designati soggetti attuatori:

A. verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di riferimento;
B. disporre, in conseguenza alla verifica di cui alla lett. 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;

F. individuare i soggetti autorizzati a compiere operazioni di trattamento (di seguito anche “incaricati”) fornendo agli stessi istruzioni per il corretto trattamento dei dati, sovrintendendo e vigilando sull’attuazione delle istruzioni impartite; tale individuazione deve essere effettuata in aderenza alle indicazioni contenute nel presente documento ed, in particolare, facendo espresso richiamo alle policy in materia di sicurezza informatica e protezione dei dati personali;
G. predisporre ogni adempimento organizzativo necessario per garantire agli interessati l’esercizio dei diritti previsti dalla normativa;
H. provvedere, anche tramite gli incaricati, a dare riscontro alle istanze degli interessati inerenti l’esercizio dei diritti previsti dalla normativa;
I. disporre l’adozione dei provvedimenti imposti dal Garante;
J. collaborare con il DPO al fine di consentire allo stesso l’esecuzione dei compiti e delle funzioni assegnate;
K. adottare, se necessario, specifici Disciplinari tecnici di settore, anche congiuntamente con altri con altri Soggetti delegati all’attuazione, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla propria area di competenza;
L. individuare, negli atti di costituzione di gruppi di lavoro comportanti il trattamento di dati personali, i soggetti che effettuano tali trattamenti quali incaricati, specificando, nello stesso atto di costituzione, anche le relative istruzioni;
M. garantire 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;
N. designare gli amministratori di sistema in aderenza alle norme vigenti in materia;
O. effettuare 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;
P. consultare il Garante, in aderenza all’art. 36 del Regolamento e nelle modalità previste dal par. 3.1 lett b), 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;
Q. richiamare obbligatoriamente nei contratti di sviluppo di software e piattaforme, la policy in materia di sviluppo delle applicazioni, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l’Ente di risoluzione del contratto;
R. dare comunicazione al Titolare delle violazioni dei dati personali oggetto di notifica.

Nell’attuazione dei compiti sopraindicati i soggetti designati possono acquisire il parere del DPO nei casi e con le modalità specificate nel seguito.

Fermo restando che la responsabilità delle attività sopraindicate rimane in ogni caso in capo al soggetto designato attuatore, in ragione del fatto che non sono ascrivibili a funzioni di direzione, coordinamento generale e controllo, sono eventualmente demandabili ai responsabili del procedimento i compiti di cui alle lettere c), d), e), g), h), j), m).

Sono inoltre 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 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 all'interno di contratti o convenzioni e, in ogni caso, in costanza di formazione del rapporto contrattuale, in aderenza ai fac-simili messi a disposizione dalla struttura competente in materia di privacy.

2.3 - GLI INCARICATI

Sono autorizzati al compimento alle operazioni di trattamento dei dati i soggetti designati attuatori di cui al precedente paragrafo ed il personale da essi designato ai sensi della presente disciplina, che conformano i loro trattamenti alle policy dell'Ente in materia di protezione dei dati personali e alle istruzioni di seguito riportate:

- sono trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento;
- sono verificati legittimità e correttezza dei trattamenti, verificando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

Sono, altresì, autorizzati tutti i soggetti che effettuino operazioni di trattamento, dipendenti e collaboratori a qualsiasi titolo e che operano sotto la diretta autorità del Titolare o dei soggetti designati. Tali soggetti devono essere da questi formalmente autorizzati.

Gli incaricati sono quindi designati:

- tramite individuazione nominativa (nome e cognome) delle persone fisiche. In questo caso occorre specificare, per ciascun nominativo, i trattamenti che lo stesso è autorizzato ad effettuare;
- tramite assegnazione funzionale della persona fisica alla unità organizzativa di minori dimensioni, qualora la persona fisica effettui tutti i trattamenti individuati puntualmente per tale unità.

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 alle policy del Comune in materia di sicurezza informatica e protezione dei dati personali.

2.4 - 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).

Specificatamente, sono di seguito indicati i compiti del DPO in aderenza agli 37 e ss del suddetto regolamento, conformati alla precipua organizzazione del Comune:

- informa e fornisce 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;
- sorveglia l'osservanza della normativa in materia di protezione dei dati personali nonché 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 connesse attività di controllo;
- coopera con il Garante per la protezione dei dati personali;
- funge da punto di contatto per l'Autorità Garante per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettua, se del caso, consultazioni relativamente a qualunque altra questione;
- partecipa allo svolgimento delle verifiche di sicurezza svolte dai Responsabili di servizio competenti o ne richiede di specifiche;
- promuove la formazione di tutto il personale dell'Ente in materia di protezione dei dati personali e sicurezza informatica;;
- partecipa alla gestione degli incidenti di sicurezza nelle modalità previste da specifica policy dell'Ente;
- formula gli indirizzi per realizzazione del Registro delle attività di trattamento di cui all'art. 30 del Regolamento.
- fornisce i pareri obbligatori e facoltativi richiesti dalle strutture secondo quanto specificato di seguito.

Il Responsabile della protezione dei dati (Data Protection Officer, di seguito DPO) è Lepida SpA

2.5 - 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 della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di 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 poste a mitigazione del rischio delle criticità emerse dall'analisi dei rischi, che abbiano un significativo impatto sulla protezione dei dati personali;
- incidenti sicurezza.

Pareri facoltativi

Possono essere inoltre richiesti, se ritenuti utili, pareri in ordine a:
- progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy by design e by default;

- valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento 2016/679;
- 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 ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016;
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti.

Le richieste di parere devono essere inviate a mezzo di posta elettronica nelle modalità che saranno stabilite dall'Ente.

Possono presentare le richieste di parere i soggetti designati attuatori.

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 dell'Ente in materia di protezione dei dati personali.

Nei casi in cui il DPO esprima pareri "NC" e "OS" il soggetto designato attuatore deve 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.

2.6 - IL GRUPPO DEI REFERENTI PRIVACY

Costituisce attuazione dei principi di informazione e sensibilizzazione del Regolamento europeo n. 679/2016 la costituzione all'interno dell'ente di un gruppo permanente di referenti privacy, composto dai responsabili di servizio preposti alle strutture di massima dimensione dell'ente, che assicuri un presidio per le strutture dell'Ente per quel che concernono gli adempimenti continuativi, lo studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti anche delle nuove disposizioni normative.

Il Gruppo di referenti ha i seguenti compiti:
- attuare, per le strutture di appartenenza, le misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo come individuate dall'Ente, anche a seguito di analisi ed approfondimenti in seno al Gruppo dei referenti privacy;
- coordinare il puntuale aggiornamento delle designazioni degli amministratori di sistema all'interno delle Direzioni/strutture di appartenenza e la costante verifica dei privilegi assegnati agli amministratori già designati;

- effettuare la ricognizione costante, a mezzo del Registro, dei trattamenti di dati personali effettuati dalle strutture di appartenenza, servendosi di risorse e competenze messe all'uopo a disposizione dal soggetto delegato attuatore o dal dirigente dallo stesso delegato;
- fornire supporto alle verifiche di sicurezza svolte dal DPO;
- provvedere alla revisione e all'aggiornamento dei Disciplinari Tecnici;
- coordinare le richieste di parere al DPO dei soggetti designati attuatori di propria afferenza nei casi e con le modalità previsti dal presente documento.

2.7 - 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'art. 5, c. 5, 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 ad 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 controinteressati e comunque per tutti gli aspetti relativi alla protezione dei dati personali inerenti le richieste di accesso civico generalizzato.
Il DPO funge altresì da supporto al R.P.C.T. nei casi di riesame di 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 ordine alla valutazione dell'eventuale pregiudizio che l'accesso potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016.

Il DPO, su richiesta delle strutture, formula il proprio parere, entro tre giorni, in ordine all'opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti 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 l'interesse alla protezione dei dati personali e la rilevanza dell'interesse conoscitivo della collettività che la richiesta di accesso mira a soddisfare, che deve essere finalizzato essenzialmente al controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche.

2.8 - RESPONSABILE PER LA TRANSIZIONE ALLA MODALITÀ DIGITALE

Al Responsabile per la transizione alla modalità digitale 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, con il supporto del servizio informatico.
Il Responsabile è il Segretario Comunale.

2.9 - IL SERVIZIO INFORMATICO/CED DELL'UNIONE TERRE E FIUMI

Il servizio informatico svolge un ruolo di supporto al DPO in tema di risorse strumentali e di competenze. Al fine di adeguare le funzioni assegnate con la designazione della nuova figura del DPO è necessario prevedere per il servizio i seguenti compiti:

- 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 obbligatorio del DPO, come ad esempio per la redazione delle linee guida in materia di sicurezza delle informazioni e protezione dei dati personali e per la redazione ed aggiornamento dei disciplinari tecnici trasversali;
- condivide 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;
- provvede, ogni qualvolta venga avvertito un problema di sicurezza a attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza, assicurando la partecipazione del DPO;
- individua misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere obbligatorio del DPO;
- segnalare al Titolare le violazioni dei dati personali ai fini della notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali;
- supporta il Responsabile per la transizione alla modalità digitale nell'esecuzione delle verifiche sulla puntuale osservanza della normativa e delle policy dell'Ente 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;
- promuove la formazione di tutto il personale dell'Ente in materia di sicurezza informatica, anche attraverso un piano di comunicazione e divulgazione, coordinandosi con le azioni promosse dal DPO.