Valutazione di impatto sulla protezione dei dati personali ex art. 35 GDPR

1. DATI DEL TITOLARE E DEI RESPONSABILI DEL TRATTAMENTO

Titolare del trattamento	
Nome	Comune di Fiesso d'Artico
Indirizzo	Piazza Marconi, n. 16, 30032 Fiesso d'Artico (VE)
E-mail	protocollo@comune.fiessodartico.ve.it
PEC	comunefiessodartico.ve@legalmail.it
Responsabile del trattamento	
Nome	Maggioli S.p.A.
Indirizzo	Via del Carpino, n. 8, 47822 Santarcangelo di Romagna (RN)
E-mail	maggiolispa@maggioli.it
PEC	segreteria@maggioli.legalmail.it
Parte del trattamento gestita	Implementazione delle varie sezioni del sito, caricamento di contenuti, manutenzione e aggiornamento, fornitura di server
Data di completamento della Valutazione di impatto	
12 dicembre 2023	

2. NECESSITÀ DI UNA VALUTAZIONE DI IMPATTO EX ART. 35 GDPR

In seguito alla realizzazione di una preliminare valutazione del rischio, è emerso che i trattamenti effettuati dal Comune tramite il proprio sito internet istituzionale (nel prosieguo, il "Sito"), che include lo Sportello telematico polifunzionale, presentano in alcuni casi un rischio elevato per i diritti e le libertà delle persone fisiche, considerando l'impatto che la perdita di riservatezza, integrità e disponibilità dei dati stessi avrebbe per gli interessati, e la probabilità che le minacce si verifichino.

Inoltre, la valutazione di impatto è ritenuta necessaria, ai sensi di quanto indicato nelle Linee guida sulla DPIA dell'EDPB e nell'Allegato al provvedimento "Elenco delle tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto" del Garante Privacy italiano, in quanto, mediante le pubblicazioni e le comunicazioni effettuate attraverso il Sito o lo Sportello telematico:

- avviene un trattamento, su larga scala, di dati aventi carattere estremamente personale. Con tale espressione, il Garante privacy italiano ha inteso fare riferimento, fra gli altri, "ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti)";

- il Comune pone in atto "trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati", in riferimento alle modalità di utilizzo dei servizi messi a disposizione online;

- il Comune pone in atto trattamenti non occasionali di dati relativi a soggetti vulnerabili (come minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo);

- il Comune può altresì trattare categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

In generale, i trattamenti di dati personali realizzati dal Comune possono comportare anche lo scambio tra diversi Titolari di dati su larga scala con modalità telematiche.

3. INTRODUZIONE NORMATIVA

La valutazione di impatto ("DPIA") viene definita nel dettaglio dal Comitato Europeo per la protezione dei dati[1] (CEPD o EDPB, ex WP29), che la identifica come "*un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità*".

Ai sensi dell'art. 35 del Regolamento UE 2016/679 ("GDPR"), la valutazione di impatto deve contenere almeno:

"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione."

L'art. 35 del GDPR stabilisce che, quando un tipo di trattamento, allorché prevede 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, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Inoltre, il medesimo articolo stabilisce che la valutazione di impatto è obbligatoria qualora avvenga:

"a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico."

Tuttavia, è bene specificare che il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che i Titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

Invero, i trattamenti elencati dall'art. 35 GDPR paragrafo 3, che comportano obbligatoriamente l'adozione di una valutazione di impatto, rappresentano un'elencazione non esaustiva di tutti i trattamenti necessitanti di detta valutazione.

---

[1] Il comitato europeo per la protezione dei dati è un organo europeo indipendente, che contribuisce all'applicazione coerente delle norme sulla protezione dei dati in tutta l'Unione europea e promuove la cooperazione tra le autorità competenti per la protezione dei dati dell'UE.
Il Comitato europeo per la protezione dei dati è composto da rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (GEPD). Ne fanno altresì parte le autorità di controllo degli Stati EFTA/SEE per quanto riguarda le questioni connesse al regolamento generale sulla protezione dei dati (GDPR).

Vi possono infatti essere operazioni che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto "elevati" e che devono quindi essere sottoposti ad una valutazione d'impatto.

Nel 2017 l'EDPB ha adottato delle Linee guida sulla DPIA in cui ha ulteriormente specificato alcune ipotesi in cui la stessa è ritenuta necessaria. Ne è infatti consigliata l'adozione qualora sussistano almeno due delle ipotesi indicate. Su questo modello, anche il Garante italiano, con proprio provvedimento dell'11 ottobre 2018, ha poi predisposto un elenco - comunque non esaustivo - delle tipologie di trattamento ai sensi dell'art. 35, par. 4 che devono essere necessariamente sottoposte a valutazione d'impatto.

È bene evidenziare infine che la consultazione dell'Autorità Garante in via preventiva rispetto al trattamento è necessaria, ai sensi dell'interpretazione più diffusa dell'articolo 36 GDPR, solo qualora la valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati.

La responsabilità per l'implementazione e l'adozione della DPIA è in capo al Titolare del trattamento, a cui spetta garantire l'effettuazione della stessa, sebbene la conduzione materiale possa essere affidata ad un altro soggetto, interno o esterno all'organizzazione aziendale. Qualora risulti che il trattamento sia svolto in tutto o in parte da un Responsabile del trattamento, quest'ultimo deve assistere il Titolare nella conduzione della DPIA, fornendo ogni informazione necessaria.

4. STRUTTURA DELLA VALUTAZIONE DI IMPATTO

La valutazione di impatto si compone di due documenti:

1. la presente valutazione, che contiene indicazioni in ordine alla normativa di riferimento e la descrizione del trattamento, dei rischi connessi e delle categorie di misure di sicurezza adottate;
2. un documento in Excel, denominato "DPIA Sito e Sportello telematico", che contiene invece la descrizione dettagliata dei rischi individuati e delle misure di sicurezza adottate dal Titolare del trattamento, al fine di contrastare i rischi connessi ai trattamenti.

5. DESCRIZIONE DEL TRATTAMENTO

5.1 DATI TRATTATI E FINALITÀ DEL TRATTAMENTO

Il Comune di Fiesso d'Artico è un comune italiano di 8.433 abitanti circa, della città metropolitana di Venezia, in Veneto, situato nel cuore della riviera del Brenta. Il Comune ha una superfice di 6,31 kmq.

Il Comune è dotato di due Organi di governo, la Giunta comunale e il Consiglio comunale, e prevede quattro settori, rappresentanti le diverse aree amministrative, oltre all'Ufficio di staff del Sindaco. Ciascun settore ricomprende diversi Uffici al proprio interno.

I settori, così come descritti nella sezione "Amministrazione trasparente" del Sito (Amministrazione trasparente), sono i seguenti: economico-amministrativo; lavori pubblici, patrimonio, manutenzioni, ecologia, protezione civile; edilizia privata, urbanistica, ambiente; socio-culturale.

Il Sito è reperibile al link www.comune.fiessodartico.ve.it e contiene le sezioni e le funzionalità di seguito descritte.

Il Sito istituzionale Municipium, l'Albo Pretorio e l'Amministrazione Trasparente sono stati realizzati dalla società Maggioli S.p.A., con la quale il Comune ha stipulato anche un contratto di assistenza e manutenzione triennale. Maggioli è titolare di diritti esclusivi per quanto riguarda il Sito Municipium.

Per ogni sezione o funzionalità, viene di seguito indicato se la stessa comporti un trattamento di dati personali ulteriori rispetto ai dati di navigazione. Questi ultimi ricomprendono, in particolare, indirizzo IP, URI (Uniform Resource Identifier) delle risorse richieste, l'orario e la data dell'interazione con il Sito, la tipologia di sistema operativo, il browser utilizzato, la risoluzione dello schermo ed altre informazioni tecniche sul dispositivo utilizzato. Si tratta di dati personali la cui

trasmissione è implicita nell'uso dei protocolli di comunicazione di internet e, quindi, di dati che non sono raccolti per essere associati a te, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare l'utente.

La struttura del Sito è reperibile al seguente link: https://www.comune.fiessodartico.ve.it/it/sitemap consultato da ultimo in data 18 ottobre 2023.

Il Sito è stato aggiornato in conformità alle "Linee Guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione", emanate in attuazione dell'art. 53, co. 1ter del Codice dell'Amministrazione Digitale.

Homepage

L'Homepage del Sito contiene i collegamenti alle sezioni più rilevanti per gli interessi dei cittadini. L'header permette l'accesso all'area personale, alla funzione "cerca" e alle sezioni "amministrazione", "novità", "servizi" e "vivere il Comune". È poi presente un footer con link a diverse sezioni raccolte nelle seguenti macrocategorie: amministrazione, categorie di servizio, novità, vivere il Comune, contatti. È presente altresì un link all'account Twitter X del Comune.

"Contatta il Comune"

In calce a diverse sezioni è presente un riquadro "Contatta il Comune" attraverso il quale è possibile usufruire delle funzioni: "richiedi assistenza", "chiama il Comune", "prenota un appuntamento", "segnala un disservizio".

Nel form "richiedi assistenza", l'utente può identificarsi tramite SPID o CIE, oppure indicando nome, cognome ed e-mail.

L'accesso tramite SPID o CIE comporta la condivisione dei seguenti dati personali con il fornitore dei servizi:

- Codice identificativo
- Nome
- Cognome
- Luogo di nascita
- Data di nascita
- Sesso
- Codice fiscale
- Provincia di nascita
- Numero di telefono mobile
- Indirizzo di posta elettronica.

L'assistenza viene prestata in relazione a tutti i servizi offerti dagli Uffici comunali e l'utente può quindi scrivere i dettagli della propria richiesta. In calce al form è presente un link all'informativa privacy generale del Sito.

"Chiama il Comune" permette di aprire app per la gestione di telefonate.

Il form "prenotazione appuntamento" comporta il trattamento dei seguenti dati personali: nome, cognome, e-mail, eventuali dettagli (facoltativi) relativi alla motivazione di richiesta dell'appuntamento. In calce al form è presente un link all'informativa privacy generale del Sito. Questo form è dedicato alla richiesta di appuntamenti con gli Amministratori Comunali e gli Uffici Comunali.

La funzione "segnala disservizio" permette invece di accedere direttamente alla sezione "Segnalazioni" del Sito e di inviare quindi una segnalazione relativa a accessibilità, ambiente, CIE, guasti illuminazione pubblica, richieste di appuntamento con sindaco e assessori, rifiuti abbandonati, verde pubblico e arredo urbano, viabilità e segnaletica, o altro. I dati personali trattati attraverso il form sono i seguenti: nome, cognome, telefono, e-mail, oltre ad eventuali dati contenuti nel testo della segnalazione o nelle immagini allegate. In calce al form, è presente un'informativa privacy breve con link all'informativa estesa relativa ai "servizi offerti previa iscrizione da apposito modulo".

Verifica del gradimento

Il Sito contiene una sezione per la verifica del gradimento da parte del cittadino, predisposta in conformità alle "Linee Guida per i Soggetti Attuatori individuati tramite avvisi pubblici a lump sum" emanate dalla Presidenza del Consiglio dei Ministri, come da ultimo aggiornate nel mese di ottobre 2023.

In calce ad ogni pagina del Sito è infatti presente un riquadro riportante la domanda "Quanto sono chiare le informazioni su questa pagina?" e cinque stelle. Se l'utente seleziona le stelle da uno a tre, gli viene chiesto dove abbia incontrato le maggiori difficoltà. È possibile selezionare una delle risposte proposte o indicare "altro".

Se l'utente seleziona la quarta o la quinta stella, invece, gli viene chiesto quali siano stati gli aspetti che ha preferito. La risposta può essere data con le stesse modalità sopra indicate.

"Amministrazione"

Le sottosezioni "Organi di governo, "Aree amministrative", "Uffici", "Enti e fondazioni", "Politici", "Personale amministrativo", "Documenti e dati" non comportano il trattamento di dati personali dell'utente.

La sottosezione "Organi di governo" (suddivisa in "giunta comunale" e "consiglio comunale") e quella denominata "Politici" prevedono la pubblicazione di nome, cognome e incarichi dei soggetti che compongono gli organi di governo e di indirizzo politico del Comune.

Le sottosezioni "Aree amministrative" e "Enti e fondazioni" riportano il link alla sezione "Amministrazione trasparente", che sarà analizzata nel prosieguo.

Nella sottosezione "Uffici" sono presenti i link alle sezioni dedicate a ciascun ufficio e sono indicati nome, cognome e incarichi delle persone che compongono ciascuna struttura (interni o esterni al Comune). Gli stessi dati (nome, cognome e incarichi) sono indicati in riferimento a tutto il personale amministrativo nella sottosezione "Personale amministrativo".

La sottosezione "Documenti e dati" è suddivisa in "accordo fra enti", "atto normativo", "dataset", "documento tecnico di supporto", "documento albo pretorio", "documento attività politica", "documento di programmazione e rendicontazione", "documento funzionamento interno", "istanza", "modulistica".

Alcune sottosezioni sono dedicate alla pubblicazione dei documenti indicati nella relativa denominazione e potrebbero quindi contenere e divulgare dati personali di eventuali soggetti citati all'interno dei documenti stessi.

Altre sottosezioni ("Documento Albo pretorio", "Documento attività politica", "Documento di programmazione e rendicontazione", "Documento funzionamento interno") contengono i link, rispettivamente, alle sezioni Albo pretorio e Amministrazione trasparente.

Per quanto riguarda la sottosezione "Dataset", si dà atto del fatto che attualmente il Comune non rende disponibile online alcuna banca dati.

"Novità"

Questa sezione, e le relative sottosezioni "Notizie", "Comunicati" e "Avvisi" non comportano un trattamento di dati personali ulteriori.

"Servizi"

Questa sezione presenta tutti i servizi offerti dal Comune alla propria utenza. I servizi sono elencati sia singolarmente, sia raggruppati per "categorie di servizio", che sono le seguenti: anagrafe e stato civile; cultura e tempo libero; vita lavorativa; imprese e commercio; appalti pubblici; catasto e urbanistica; turismo; mobilità e trasporti; educazione e formazione; giustizia e sicurezza pubblica; tributi, finanze e contravvenzioni; ambiente; salute, benessere e assistenza; autorizzazioni; agricoltura e pesca.

Entrando in ciascun specifico servizio, è quasi sempre presente un link alla sezione dedicata all'Ufficio che gestisce il servizio. Ciascun Ufficio mette quindi a disposizione tramite il Sito alcune informazioni di base in merito alle proprie competenze, ai servizi offerti, alla modulistica e alle delibere utili, oltre ai dati di contatto e agli orari di apertura.

La sezione di ciascun Ufficio contiene altresì un link allo Sportello telematico polifunzionale per la presentazione di istanza online.

In alternativa, all'interno del singolo servizio sono resi disponibili i link ad altre sezioni del Sito in cui si possono reperire ulteriori informazioni.

La sezione "Servizi" non comporta quindi di per sé il trattamento di dati personali ulteriori rispetto a quelli di navigazione.

"Vivere il Comune"

Questa sezione presenta tutti gli eventi, le iniziative e i luoghi d'interesse del territorio comunale. Questa sezione non comporta un trattamento di ulteriori dati personali. Nella sottosezione "luoghi" è caricata una mappa realizzata mediante OpenStreetMap.

"Accedi all'area personale"

Questa funzione permette a qualsiasi cittadino di identificarsi tramite SPID o CIE per accedere ad alcuni servizi offerti dal Comune tramite il Sito.

L'accesso comporta la condivisione dei seguenti dati personali con il fornitore dei servizi:

- Codice identificativo
- Nome
- Cognome
- Luogo di nascita
- Data di nascita
- Sesso
- Codice fiscale
- Provincia di nascita
- Numero di telefono mobile
- Indirizzo di posta elettronica

All'interno dell'Area personale, l'utente può visualizzare eventuali "Messaggi" e vedere il proprio "Profilo" e quindi l'anagrafica registrata.

Nell'anagrafica, per ogni riferimento di contatto (cellulare, telefono o e-mail) c'è un selettore di "Consenso". L'utente può così esprimere il proprio consenso a essere contattato anche per messaggi diversi da quelli inerenti alle attività di Protezione Civile, come comunicazioni che riguardano la vita cittadina, le scadenze amministrative, le manifestazioni o altri avvisi.

L'utente può altresì monitorare le proprie Pratiche e seguirne lo Stato di avanzamento.

Funzione "Cerca"

A seguito dell'unificazione del Sito comunale, dell'Albo Pretorio online e della sezione Amministrazione Trasparente in un unico sito, l'utente ha la possibilità di effettuare una ricerca complessiva delle informazioni e della documentazione contemporaneamente in tutte le sezioni, in attuazione degli obiettivi previsti nell'ambito dell'esperienza del cittadino nei servizi pubblici "Cittadino informato".

"Amministrazione trasparente"

Mediante questa sezione del Sito, il Comune adempie ai propri obblighi di pubblicazione di dati e documenti per finalità di "trasparenza", intesa come accessibilità totale allo scopo di promuovere la partecipazione degli interessati all'attività amministrativa e di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche (ai sensi del D. Lgs. n. 33/2013). I documenti pubblicati hanno ad oggetto incarichi di consulenti e collaboratori, bandi di concorso e relativi esiti e graduatorie, informazioni sugli enti controllati, provvedimenti, bandi di gara e contratti, ecc.

Mediante la sezione "Amministrazione trasparente" il Comune divulga dati personali di soggetti sia interni sia esterni all'ente. Tali dati personali possono essere sia comuni sia, più raramente, appartenenti a particolari categorie.

Il rispetto dei principi di minimizzazione e liceità del trattamento dei dati personali è garantito dal rispetto degli obblighi di legge, delle Linee guida del Garante per la protezione dei dati personali italiano "in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati" (provvedimento del 15 maggio 2014) e della Circolare del Comune riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni.

"Albo pretorio"

Mediante questa sezione del Sito, il Comune adempie ai propri obblighi di pubblicazione di dati, informazioni e documenti contenuti in specifiche disposizioni di settore, non riconducibili a finalità di trasparenza, come quelli volti a far conoscere l'azione amministrativa in relazione al rispetto dei principi di legittimità e correttezza, o quelli atti a garantire la pubblicità legale degli atti amministrativi (pubblicità integrativa dell'efficacia), quali a titolo meramente esemplificativo, le pubblicazioni di Deliberazioni, Ordinanze e Determinazioni, le pubblicazioni matrimoniali, ecc.

Nell'Albo pretorio sono quindi pubblicati i documenti previsti dall'ordinamento, da provvedimenti dell'autorità giudiziaria e quelli dai quali possono nascere diritti, doveri, aspettative o interessi legittimi di terzi e dalla cui diffusione nei confronti di una indistinta pluralità di soggetti potenzialmente interessati dipende la loro efficacia.

I contenuti della sezione "Albo pretorio" non sono indicizzati per i motori di ricerca.

Questa sezione comporta la divulgazione di dati personali comuni.

Funzioni aggiuntive

La funzione "Accesso redazione" contiene un link per accedere a cloud.minucipiumapp.it e quindi ad un'area riservata, con accesso possibile mediante username e password.

Il Sito interagisce altresì con l'app Municipium, creata sempre da Maggioli. L'app riproduce quasi tutti i contenuti presenti sul Sito. "Notizie" ed "eventi" vengono pubblicati in automatico. In alcune sezioni, invece, l'app contiene link alla corrispondente sezione del Sito che presenta il contenuto integrale. L'app permette l'invio di notifiche push nel momento dell'aggiunta di nuovi contenuti.

"Sportello telematico polifunzionale"

Con deliberazione di Giunta Comunale n. 7 del 25/02/2021, il Comune ha approvato la "realizzazione dello sportello telematico polifunzionale del Comune di Fiesso d'Artico, il quale, in particolare, comprende:
- la presentazione di istanze online da parte dei cittadini;
- la gestione dei procedimenti amministrativi in modalità automatizzata tramite il software gestionale;
- l'interscambio di informazioni e documentazione tra Comune e cittadini;
- la comunicazione delle informazioni relative alla gestione delle istanze dello sportello telematico polifunzionale anche tramite l'App-Io".

Più specificamente, l'implementazione dello Sportello telematico comporta:

a) il completamento della parte di back office dello sportello telematico polifunzionale anche per i procedimenti amministrativi che non appartengono allo Sportello Unico Edilizia – SUE, per la gestione dei procedimenti

amministrativi in modalità automatica e la possibilità di visionare istanze presentate o in fase di presentazione, per la verifica di eventuali criticità di completamento della modulistica;

b) l'attivazione della possibilità di inviare documentazione al cittadino tramite la scrivania virtuale dello Sportello telematico polifunzionale, con possibilità per il cittadino di gestire e tenere monitorati i propri procedimenti amministrativi e i tempi procedimentali;
c) la possibilità del collegamento diretto dello Sportello telematico polifunzionale con il sito PagoPa-My Pay della Regione Veneto, per l'effettuazione dei versamenti di diritti di segreteria, imposte e tributi, dovuti per la presentazione delle istanze, con allegazione automatica delle ricevute di corretto versamento alle istanze presentate dal cittadino;
d) la redazione e messa a disposizione di schede procedimento e istanze create secondo le indicazioni date dagli Uffici Comunali e in conformità alle modifiche normative da applicare.

Con determinazione del Settore Economico-Amministrativo n. 152 del 18/03/2021 è stato affidato a Maggioli l'incarico della realizzazione della prima parte del progetto di realizzazione dello sportello telematico polifunzionale, comprensivo della costituzione dello sportello telematico polifunzionale, per la presentazione delle istanze, con accesso tramite identità digitale Spid, carta d'identità elettronica Cie o Carta Nazionale dei Servizi CNS.
Inoltre, all'interno dello Sportello telematico polifunzionale, è stato realizzato lo Sportello Unico Edilizia – SUE, per la presentazione delle istanze in materia di edilizia e urbanistica. Il SUE, insieme allo Sportello telematico, consente al cittadino di avere un unico Sito dove ottenere le informazioni relative a servizi e procedimenti amministrativi relativi al Settore Edilizia Privata-Urbanistica-Ambiente, per poter presentare le conseguenti istanze, segnalazioni, dichiarazioni, osservazioni e comunicazioni generiche.
Come da incarico conferito dal Comune a Maggioli, lo Sportello telematico è stato quindi adeguato alle "Linee Guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione", pubblicate dall'Agenzia per l'Italia Digitale – Agid in data 27 luglio 2022.
Si rileva quindi che, attraverso lo Sportello telematico, accessibile mediante il link sportellotelematico.comune.fiessodartico.ve.it, il Comune effettua trattamenti delle seguenti categorie di dati personali:
- dati contenuti nelle istanze online presentate dai cittadini;
- dati del personale dell'ente e dei cittadini necessari per la gestione dei procedimenti amministrativi tramite il software gestionale;
- dati contenuti nelle comunicazioni scambiate con i cittadini;
- dati dei cittadini raccolti mediante l'interazione con servizi di fornitori terzi (SPID e altri sistemi di autenticazione; PagoPa-MyPa; App IO).

Ciascun trattamento viene eseguito dal Comune per le finalità e in conformità alle basi giuridiche indicate nel Registro dei trattamenti per i corrispondenti trattamenti off-line.
Le sezioni dello Sportello telematico che consentono una comunicazione di dati personali da parte degli utenti, diversi dai dati di navigazione, contengono un link all'informativa privacy generale dello Sportello telematico (https://sportellotelematico.comune.fiessodartico.ve.it/action%3As_italia%3Aprivacy.policy ; data di ultima consultazione: 30 ottobre 2023).

Soggetti interessati	**Dati trattati**
Cittadini (inclusi minori e disabili)	Dati comunicati mediante moduli e istanze inviati mediante il Sito: nome, cognome, dati per l'autenticazione tramite SPID o CIE, indirizzo e-mail, numero di telefono, dati appartenenti a categorie particolari, dati contenuti in messaggi. Si veda il Registro dei trattamenti del Titolare per l'elenco dettagliato
Personale amministrativo del Comune	Nome, cognome, e-mail istituzionale, incarichi ricoperti

Utenti del Sito	Dati di navigazione, dati comunicati tramite i moduli presenti sul Sito
Componenti degli Organi di governo (Giunta comunale e Consiglio comunale)	Nome, cognome, e-mail istituzionale, incarichi ricoperti
Fornitori e loro rappresentanti e/o referenti; candidati per posizioni lavorative; membri di organi e commissioni; dipendenti di altri enti pubblici	Dati identificativi, dati finanziari, curriculum vitae ed eventuali altri dati la cui pubblicazione nelle sezioni "Amministrazione trasparente" o "Albo pretorio" risulta obbligatoria

5.2 BASI GIURIDICHE DEI TRATTAMENTI

Le basi giuridiche che legittimano i trattamenti sopra descritti da parte del Titolare sono specificamente mappate e identificate all'interno del Registro dei trattamenti del Comune e nelle informative privacy appositamente predisposte per le specifiche sezioni del Sito.

5.3 IMPATTO SUGLI INTERESSATI

I trattamenti operati tramite il Sito portano benefici a tutte le diverse categorie di interessati, perché si tratta di un servizio che consente a cittadini di accedere più facilmente e celermente a informazioni di loro interesse; di usufruire di procedure più celeri, efficienti e interamente online; quindi, in ultima analisi, di esercitare più facilmente i propri diritti. Si ritiene altresì che, in considerazione delle misure di sicurezza tecniche e organizzative implementate, il trattamento di dati prospettato non comporti né l'esposizione degli interessati a rischi maggiori rispetto a quelli che derivano dai trattamenti di dati svolti dal Titolare del trattamento per altre finalità, né la raccolta di dati eccessivi o sproporzionati.

5.4 CONSERVAZIONE DEI DATI

I dati degli interessati raccolti tramite il Sito sono conservati per i periodi indicati nel Registro dei trattamenti del Titolare.

I tempi di conservazione, nel caso di richieste di cittadini inoltrate online, sono gli stessi previsti per le procedure gestite in via analogica.

Per quanto riguarda i dati personali relativi al personale amministrativo del Comune e ai membri degli Organi di governo, gli stessi resteranno pubblicati sul Sito per la durata del rapporto di lavoro o dell'incarico.

I dati personali riportati all'interno di documenti pubblicati sul Sito in ottemperanza ad un obbligo di legge, resteranno pubblicati per i periodi previsti dalla normativa applicabile. Al termine, tali dati saranno trattati dal Comune per il periodo previsto in base alle finalità per cui sono stati raccolti.

6. PROCESSO DI CONSULTAZIONE

L'art. 35.9 GDPR prevede che il Titolare del trattamento debba valutare l'opportunità di raccogliere "le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti."

A tale riguardo, si specifica che la consultazione degli interessati al momento non è stata ritenuta necessaria in quanto il Titolare del trattamento agisce in esecuzione e in conformità a obblighi e indirizzi previsti da norme nazionali ed europee. Pertanto, si ritiene che gli interessati siano già sufficientemente informati e le loro opinioni rappresentate.

7. PRINCIPI FONDAMENTALI

Il GDPR indica quali sono i principi fondamentali che devono in ogni caso essere seguiti nello svolgimento delle attività e dei trattamenti dei dati personali raccolti.

a. Principio di liceità: i trattamenti di dati personali devono necessariamente avere una base giuridica ed essere conformi alle norme dell'ordinamento giuridico.
b. Principio di correttezza: i dati personali devono essere trattati secondo buona fede.
c. Principio di trasparenza: devono essere facilmente accessibili e comprensibili le informazioni e le comunicazioni relative le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati i dati personali e deve essere utilizzato un linguaggio semplice e chiaro.
d. Principio di limitazione delle finalità: i dati devono essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente trattati in modo che non sia incompatibile con tali finalità.
e. Principio di esattezza dei dati: i dati devono essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
f. Principio di limitazione della conservazione: i dati devono essere conservati in una forma che consenta l'identificazione degli interessati per il tempo strettamente necessario al conseguimento delle finalità per le quali sono trattati.
g. Principio di integrità e riservatezza: i dati devono essere trattati mediante l'adozione delle misure tecniche e organizzative idonee ad assicurarne la sicurezza rispetto a trattamenti non autorizzati o illeciti e alla perdita, distruzione o danno accidentali.
h. Principio di minimizzazione: i dati trattati devono essere solamente quelli indispensabili, quindi pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
i. Principio di responsabilizzazione: compete al Titolare del trattamento l'identificazione di adeguate garanzie per tutelare i diritti e le libertà degli interessati e la documentazione dell'avvenuta adozione delle stesse.

I principi fondamentali qui menzionati devono guidare il Titolare del trattamento nello sviluppo e nell'implementazione del Sito e devono fungere da linee guida per l'individuazione delle misure di sicurezza più adatte a garantire un'adeguata protezione dei dati trattati e dei diritti e libertà degli interessati.

Nel caso dei trattamenti qui descritti, come si vedrà nei paragrafi a seguire, il Comune ha pienamente rispettato questi principi sia in fase di progettazione che nella fase di individuazione delle misure di sicurezza più idonee a consentire la limitazione dei rischi connessi a detti trattamenti.

8. NECESSITÀ E PROPORZIONALITÀ DEL TRATTAMENTO (ART. 35.7, LETT. B))

8.1 VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ

I trattamenti oggetto della presente valutazione di impatto possono incidere sui diritti e le libertà degli interessati, a cominciare dal diritto alla riservatezza della vita privata, che potrebbe essere leso da un trattamento illegittimo per la sua configurazione o modalità di attuazione.

Il trattamento di dati personali effettuato dal Comune, tuttavia, risulta necessario per il perseguimento delle finalità del trattamento, poiché è un trattamento necessario per adempiere a obblighi di legge ed eseguito mediante modalità che garantiscono la sicurezza e la riservatezza previste dalla stessa normativa.

In secondo luogo, il trattamento dei dati personali risulta proporzionato rispetto alle finalità perseguite. Il Comune, infatti, tratta solo i dati necessari e rilevanti per le finalità prestabilite, in conformità all'art. 5 GDPR. Inoltre, il Comune ha valutato che non esistano mezzi che comportino minori rischi e un minore impatto sui diritti e le libertà degli interessati e che al contempo permettano di conseguire gli stessi benefici per gli interessati stessi.

Infine, la qualità e l'integrità dei dati, oltre alla loro minimizzazione, viene garantita dal Comune per mezzo dell'adozione delle misure di sicurezza di cui si darà atto nei paragrafi seguenti.

8.2 MISURE DI PROTEZIONE DEI DIRITTI DEGLI INTERESSATI

In particolare, al fine di limitare l'impatto sui diritti e le libertà degli interessati, prima di iniziare i trattamenti qui descritti, il Comune intende adottare le seguenti misure:

i. adozione di specifiche informative privacy per ciascuna categoria di interessati, visualizzabili prima che avvenga l'effettiva comunicazione dei dati;
ii. adozione di procedure interne, per garantire che il trattamento di dati personali avvenga in sicurezza in ogni sua fase;
iii. formazione rivolta ai dipendenti;
iv. specifici atti di nomina ad autorizzato del trattamento ex art. 29 GDPR, riportanti le istruzioni impartite dal Titolare del trattamento;
v. assenza di trasferimenti di dati personali verso Paesi terzi;
vi. adozione di contratti di nomina specifici e dettagliati con tutti i Responsabili del trattamento coinvolti. Il Comune si avvale esclusivamente di soggetti nominati Responsabili del trattamento, adeguatamente selezionati e nominati ai sensi dell'art. 28 GDPR. Il Comune conserva e aggiorna costantemente un elenco di tutti i Responsabili del trattamento;
vii. acquisizione del consenso degli interessati che, ove richiesto, viene prestato in modo specifico, esplicito, libero e previa consegna di adeguata informativa;
viii. garanzia dell'esercizio dei diritti degli interessati previsti dagli artt. 15-22 GDPR.

È quindi possibile affermare che il trattamento risulta necessario e proporzionato e non incide sul contenuto essenziale dei diritti degli interessati.

9. SISTEMI DI VALUTAZIONE DEL RISCHIO E RISCHI CONNESSI AL TRATTAMENTO (ART. 35.7, LETT. C))

Il trattamento dei dati personali effettuato dal Titolare del trattamento presenta alcuni rischi, che devono essere previamente valutati.

Per quanto concerne la metodologia utilizzata ai fini dell'identificazione e valutazione delle minacce e dei rischi afferenti ai trattamenti di dati personali oggetto della presente DPIA, si dà atto che la valutazione del rischio è stata condotta secondo un approccio basato sulla metodologia proposta da ENISA, in particolare nei documenti "Handbook on security of personal data processing" del dicembre 2017 e "Reinforcing trust and security in the area of electronic communications and online services" del dicembre 2018. Si è inoltre tenuto presente il documento "NIST Special Publication 800-30", pubblicato nel settembre 2012 dal National Institute of Standards and Technology degli Stati Uniti per regolamentare la sicurezza delle informazioni di sistemi di enti pubblici.

Il livello di rischio del trattamento è determinato dall'impatto sui diritti degli interessati della possibile perdita di riservatezza, integrità e disponibilità dei dati e dalla probabilità che l'evento dannoso si verifichi.

Sono definiti quattro livelli di impatto in relazione al realizzarsi di una possibile minaccia:

a) molto alto – Gli interessati possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).
b) alto – Gli interessati possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
c) medio – Gli interessati possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
d) basso - Gli interessati possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).

La valutazione dell'impatto rappresenta il risultato di un processo di analisi qualitativa che prende in considerazioni molteplici fattori, tra cui:

- il tipo di dati trattati,

- le criticità delle operazioni di trattamento,

- il quantitativo di dati,

- eventuali specifiche caratteristiche del Titolare del trattamento, e

- eventuali categorie particolari di interessati.

Il livello di impatto è calcolato sulla base dell'esperienza e della conoscenza dei servizi descritti e del relativo ambito di attuazione. L'impatto è altresì calcolato avendo riguardo alle possibili conseguenze per gli interessati, in particolare:

- perdita del controllo dei dati personali,
- privazione o limitazione dei diritti o libertà,
- discriminazione,
- furto o usurpazione di identità,
- frodi,
- perdite finanziarie o altre conseguenze economiche negative,
- decifratura non autorizzata della pseudonimizzazione,
- pregiudizio alla reputazione,
- perdita di riservatezza dei dati personali coperti da segreto professionale,
- conoscenza da parte di terzi non autorizzati,
- qualsiasi altro danno economico o sociale significativo,
- violazione delle misure di sicurezza che comporti distruzione, perdita, modifica, divulgazione non autorizzata, accesso illegale ai dati trasmessi, conservati e/o trattati.

È poi necessario considerare le diverse fonti di rischio per verificare le probabilità che dalle stesse derivi un danno o una minaccia ai diritti degli interessati. Le principali fonti di rischio possono di fatto essere raggruppate in due macrocategorie: fattori di rischio umani e fattori non umani.

I fattori di rischio umani si concretizzano in accadimenti che discendono dalla condotta dolosa o colposa di un soggetto; a titolo meramente esemplificativo, un soggetto incaricato del trattamento potrebbe erroneamente manomettere, o modificare alcuni dati, senza averne la reale consapevolezza né l'intenzione, danneggiando dunque l'integrità dei dati stessi. Parimenti, potrebbe accadere che un esperto informatico riesca ad abbattere o eludere, illegalmente, le misure di sicurezza adottate per la protezione dei dati, giungendo così a conoscere informazioni strettamente riservate e/o personali.

Si considerano, invece, fattori non umani tutte quelle fonti di rischio che traggono origine da eventi non connessi alla condotta di un soggetto, ma piuttosto discendenti da fattori imprevedibili, quali ad esempio disastri ambientali, incendi, terremoti, ecc., ovvero errori o bug di sistema.

Anche il processo di analisi delle probabilità è di tipo qualitativo, perché è strettamente condizionato dallo specifico contesto in cui avviene il trattamento di dati personali. Alla probabilità del verificarsi delle minacce deve essere attribuito un livello basso, medio o alto. Seguendo il modello di ENISA, sono state considerate quattro aree di valutazione della probabilità del verificarsi di minacce ai diritti degli interessati, e cioè:

- risorse tecniche e di rete (hardware e software),

- processi e procedure relativi al trattamento di dati personali,

- diverse parti e soggetti coinvolti nelle operazioni di trattamento,

- settore di operatività e scala del trattamento.

La stima della probabilità di accadimento è effettuata sulla base del livello di esposizione alla minaccia e del livello di vulnerabilità, che risulta essere inversamente proporzionale rispetto al livello di applicazione delle misure di sicurezza che servono a mitigare le minacce.

ENISA suggerisce di calcolare il livello di probabilità secondo i parametri riportati nella tabella sottostante (fonte: ENISA):

Somma globale della probabilità di occorrenza di una minaccia	LIVELLO DI PROBABILITÀ DELLE MINACCE
4 - 5	Basso
6 - 8	Medio
9 -12	Alto

La valutazione finale del rischio di un trattamento viene ottenuta incrociando il livello di impatto calcolato e la relativa probabilità di occorrenza delle minacce.

Il Titolare del trattamento prende quindi in considerazione le misure di sicurezza tecniche e organizzative adottate per verificare che siano adeguate a ridurre il rischio rilevato ad un livello accettabile.

9.1 VALUTAZIONE DELL'IMPATTO

Nel presente paragrafo si riportano i risultati delle analisi e delle valutazioni svolte nell'allegato file Excel "DPIA Sito e Sportello telematico", Fogli "Rischi".

Il Titolare del trattamento ha infatti valutato l'impatto sui diritti fondamentali e le libertà degli interessati che risulterebbe da un evento (accidentale o intenzionale) che comporti la perdita delle caratteristiche di riservatezza, integrità e disponibilità dei dati personali trattati.

Di seguito si riportano i livelli di impatto calcolati per i diversi trattamenti di dati personali attuati dal Comune mediante il Sito e lo Sportello telematico:

Titolo	**Dati comuni comunicati dal cittadino/utente (nome, cognome, indirizzo e-mail, numero di telefono, dati contenuti nei messaggi inviati)**	**Dati comuni pubblicati dal Comune (nome, cognome, incarichi)**	**Altri dati per accesso tramite SPID o CIE (luogo e data di nascita, sesso, codice fiscale)**	**Dati appartenenti a categorie particolari**	**Dati di minori o disabili**	**Livello di impatto**
1.Form "Richiedi assistenza"	Sì	No	sì	no	sì	**Molto alto**
2.Area personale; istanze presentate tramite lo Sportello telematico	sì	no	sì	sì	sì	**Molto alto**
3.Form "Prenotazione appuntamento"; Segnalazioni;	sì	No	No	no	no	**Alto**

Verifica del gradimento						
4.Organi di governo; Politici; Uffici; Personale amministrativo; Accordo fra enti; Atto normativo; Documento tecnico di supporto; Albo pretorio	no	sì	no	no	no	**Basso**
5.Amministrazione trasparente	no	Sì	no	sì	sì	**Medio**

9.2 VALUTAZIONE DELLA PROBABILITÀ E LIVELLO DI RISCHIO INERENTE

Nel presente paragrafo verranno delineati i principali fattori di rischio che emergono dall'analisi del contesto in cui vengono effettuati i trattamenti di dati personali e le relative probabilità di accadimento, riportando i risultati delle valutazioni documentate nell'allegato file Excel "DPIA Sito e Sportello telematico", Fogli "Rischi".

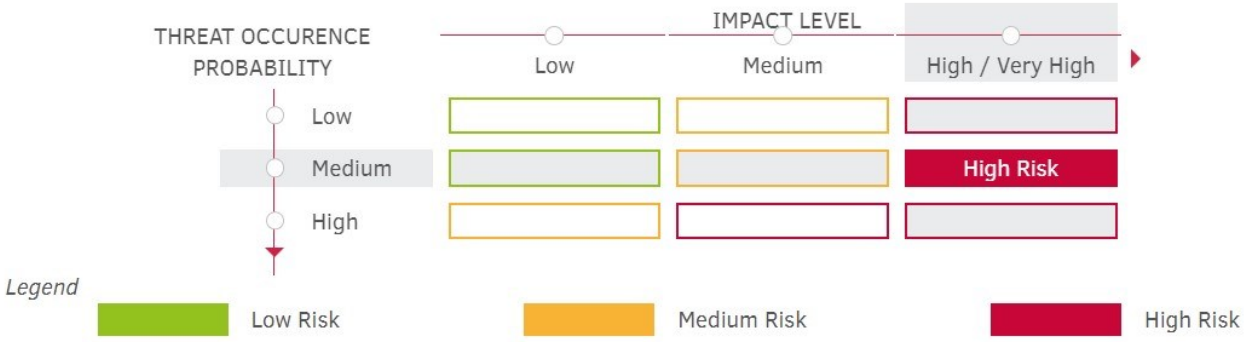
Si rileva che il Sito rappresenta un sistema informatico unitario, pertanto tutti i trattamenti di dati personali che avvengono per il suo tramite presentano le stesse vulnerabilità. Per quanto riguarda invece le minacce, emerge che quelle rappresentate da azioni umane intenzionali malevole esterne potrebbero con maggiore probabilità colpire: 1) trattamenti che coinvolgono dati particolari degli interessati; 2) trattamenti che comportano un'interconnessione e uno scambio di dati con sistemi informatici esterni. Si è ritenuto, tuttavia, che anche ove attaccanti esterni prendessero di mira uno specifico trattamento di dati o una sua parte, questo comporterebbe un elevato rischio che si verifichi una minaccia anche in riferimento ai dati coinvolti in altri trattamenti. Di conseguenza, si è ritenuto ragionevole applicare lo stesso livello di probabilità di accadimento di minacce in riferimento a tutti i trattamenti delineati nei paragrafi precedenti.

Il livello complessivo di probabilità è risultato medio (fonte immagine: ENISA):

Impact assessment

ASSESSMENT AREA	PROBABILITY	
Network and Technical Resources	High	3
Processes/Procedures related to the processing of personal data	Low	1
Parties/People involved in the processing of personal data	Low	1
Business sector and scale of processing	Medium	2
Overall Threat Occurrence Probability	Medium (7)	

La valutazione del rischio è effettuata combinando i due fattori principali, "impatto" e "probabilità", come illustrato negli schemi sottostanti (fonte immagine: ENISA):



I livelli di rischio sono riportati di seguito:

Titolo	**Impatto**	**Probabilità**	**Livello di rischio inerente**	**Livello di rischio applicato**
1.Form "Richiedi assistenza"	Molto alto	Medio	**Alto**	**Alto / Molto alto**
2.Area personale; istanze presentate tramite lo Sportello telematico	Molto alto	Medio	**Alto**	**Alto / Molto alto**
3.Form "Prenotazione appuntamento"; Segnalazioni; Verifica del gradimento	Alto	Medio	**Alto**	**Alto / Molto alto**
4.Organi di governo; Politici; Uffici; Personale amministrativo; Accordo fra enti; Atto normativo; Documento tecnico di supporto; Albo pretorio	Basso	Medio	**Basso**	**Alto / Molto alto**
5.Amministrazione trasparente	Medio	Medio	**Medio**	**Alto / Molto alto**

Il valore della probabilità di accadimento precedente all'implementazione delle contromisure necessarie a mitigare il rischio di attuazione delle minacce è definito come rischio inerente. Il livello di rischio applicato rappresenta, invece, il livello considerato per individuare le misure di sicurezza che si ritengono necessarie. Dato che i trattamenti vengono operati tramite un unico sistema informatico, si è ritenuto più prudente applicare a tutti i trattamenti un livello di rischio alto/molto alto, al fine di individuare misure di sicurezza adeguate anche per i trattamenti più delicati. Sulla base delle misure di sicurezza proprie dell'ambiente in esame e delle funzionalità di sicurezza che sono state implementate, di cui si darà atto nel paragrafo seguente, viene calcolato invece il valore di rischio residuo.

10. MISURE DI SICUREZZA

Dopo aver analizzato i rischi connessi ai trattamenti di dati personali, è essenziale indicare quali sono le misure di sicurezza adottate per eliminare o ridurre suddetti rischi, al fine di garantire la conformità ai principi del GDPR.

Si precisa che le misure di sicurezza sono state adottate nel rispetto dell'art. 32 GDPR, ovverosia "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche".

Le misure ritenute adeguate sono state individuate in base al livello di rischio determinato e al contesto generale del trattamento dei dati personali.

Con riferimento all'individuazione e descrizione specifica delle misure di sicurezza implementate dal Comune, si rinvia al file Excel allegato "DPIA Sito e Sportello telematico".

Per l'elenco delle misure di sicurezza, è stato seguito l'"Handbook on security of personal data processing" di ENISA del dicembre 2017.

Mediante la mappatura delle misure di sicurezza tecniche e organizzative implementate dal Titolare del trattamento, si è dato atto del rispetto dei principi della privacy *by design* e *by default* ai sensi dell'art. 25 GDPR. In particolare, si è dimostrato il rispetto di otto "strategie" che consentono di:

a) Minimizzare: è necessario che i server ove risiedono database e applicazioni trattino solo i dati personali che sono effettivamente necessari per il perseguimento delle finalità di volta in volta considerate (art. 5 GDPR). È quindi essenziale dimostrare che i dati trattati sono necessari per il perseguimento delle finalità descritte.
b) Nascondere: i dati personali, e le loro relazioni, debbano essere celati, se non viene riscontrata alcuna necessità di esposizione. In questo modo, il rischio di abusi di vario genere è ridotto al minimo. Risulta, in particolare, essenziale anonimizzare o pseudonimizzare i dati che devono essere nascosti.
c) Separare: i dati personali devono essere trattati in modalità distribuita, in compartimenti separati laddove sia possibile. La separazione evita che si possano costruire profili completi senza accedere a tutti i compartimenti.
d) Garantire il controllo: gli interessati devono poter controllare il processo di trattamento dei propri dati personali. Deve dunque essere garantito l'esercizio dei diritti di accesso, aggiornamento e oblio. Questa strategia è essenziale perché permette di mantenere i database aggiornati, migliorando la qualità degli stessi.
e) Aggregare: i dati devono essere trattati al più alto livello di aggregazione possibile con il minor dettaglio possibile che sia (ancora) utile.
f) Informare: gli interessati devono essere adeguatamente informati sul trattamento dei loro dati personali.
g) Controllare: gli interessati devono poter controllare il processo di trattamento dei propri dati.
h) Applicare: le disposizioni del GDPR devono essere concretamente applicate e conosciute.
i) Dimostrare: tutti i trattamenti e le scelte ad essi collegate debbano essere giustificati e dimostrati, nel tempo. Va dunque dimostrato come la politica di protezione dei dati sia effettivamente implementata all'interno del sistema IT del Titolare del trattamento.

Si rileva altresì che Maggioli S.p.A., che si occupa della creazione, aggiornamento e manutenzione del Sito e dello Sportello telematico e dei relativi server, ha conseguito alcune certificazioni relative alle parti di trattamento di dati personali alla stessa affidate, e in particolare:

- la Certificazione ISO 27001:2017 (Tecnologie informatiche, Tecniche di sicurezza, Sistemi di gestione della sicurezza) (per la progettazione, sviluppo, installazione, manutenzione, formazione e assistenza di applicativi software anche in modalità SaaS (Software as a Service));

- la Certificazione ISO 9001:2015 (Sistemi di gestione per la qualità) (relativa alla progettazione, sviluppo, installazione, manutenzione, formazione e assistenza di applicativi software anche in modalità SaaS (Software as a Service));

- la Certificazione ISO 14001:2015 (Sistemi di gestione ambientale).

11. CONCLUSIONI

La presente valutazione di impatto ha consentito di determinare livelli iniziali di rischio dei trattamenti che talvolta sono risultati anche alti o molto alti. I trattamenti, infatti, possono avere un impatto rilevante sulla sfera personale e sui diritti dei cittadini interessati.

Dall'analisi delle misure di sicurezza organizzative e tecniche implementate dal Titolare del trattamento, tuttavia, è risultato che il rischio residuo è stato ridotto ad un livello accettabile per tutti i trattamenti considerati e per tale ragione non si è ritenuto necessario procedere alla consultazione preventiva del Garante Privacy, altrimenti prevista dall'art. 36 del GDPR.

Questa valutazione è stata compiuta anche considerando che il Comune è una Pubblica amministrazione che, nella definizione degli specifici trattamenti considerati nel presente documento, è strettamente vincolato da norme nazionali ed europee, che stabiliscono quali dati personali è necessario trattare, per quali finalità e con quali modalità. Nell'ambito ed entro i limiti della propria discrezionalità, il Comune ha adottato misure di sicurezza adeguate a garantire il rispetto dei diritti e delle libertà degli interessati.

Il Responsabile del trattamento Maggioli ha altresì dichiarato che il progetto relativo al nuovo Sito del Comune e allo Sportello telematico polifunzionale è conforme a tutta la normativa nazionale ed europea applicabile e, in particolare, alla normativa in materia di trattamento dati personali, alle Linee Guida di design per i siti internet e i servizi digitali della Pubblica Amministrazione del 27/09/2022, alla normativa in materia di accessibilità e alla normativa che disciplina il diritto al lavoro dei disabili, ai sensi dell'articolo 17 della L. 12 marzo 1999 n. 68.

Le certificazioni di cui dispone Maggioli permettono altresì di attestare il possesso di gran parte delle misure di sicurezza tecniche e organizzative ritenute adeguate per minimizzare il rischio dei trattamenti di dati personali.

Si dà comunque atto, in conclusione, che il Comune si impegna a revisionare almeno con cadenza annuale la presente valutazione di impatto al fine di attestare l'implementazione di ulteriori misure di sicurezza, adeguate e aggiornate rispetto allo stato della tecnica, e di dare atto delle modifiche introdotte nel trattamento qui descritto, per scelta del Comune o per la necessità di adempiere a nuove previsioni normative.

La valutazione di impatto fa riferimento allo stato di implementazione del Sito e dello Sportello telematico polifunzionale alla data del 18 ottobre 2023 ed è basata sulle informazioni a disposizione del Titolare del trattamento alla stessa data. Le misure di sicurezza di cui il Responsabile del trattamento Maggioli S.p.A. non ha confermato la presenza sono indicate come "in approfondimento" e sono state considerate come non implementate al momento della redazione del presente documento.

Per ridurre ulteriormente il livello di rischio residuo, il Titolare del trattamento si impegna a provvedere agli adempimenti di seguito descritti:

- aggiornare il Registro dei trattamenti in conformità a quanto attestato dalla presente valutazione di impatto;

- aggiornare le informative privacy relative ai trattamenti di dati effettuati mediante il Sito e lo Sportello telematico polifunzionale;

- adottare una policy di sicurezza delle informazioni.