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
Responsabili 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	Migrazione di tutti i servizi comunali, eccetto quello oggetto di incarico a Euganea Innovazione; implementazione della suite SicrawebEVO
Nome	Euganea Innovazione S.r.l.
Indirizzo	Via Trento Trieste, n. 27/A, 35043 Monselice (PD)
E-mail	info@euganeainnovazione.it
PEC	info@pec.euganeainnovazione.it
Parte del trattamento gestita	Migrazione del servizio denominato "Produttività individuale"
Nome	Criticalcase S.r.l.
Indirizzo	Via Chambery n. 93/107 Torino (TO)
E-mail	marketing@criticalcase.com
PEC	criticalcase@pecmails.it
Parte del trattamento gestita	Servizio di hosting per il servizio denominato "Produttività individuale"

Data di completamento della Valutazione di impatto
15 novembre 2023
Numero versione e data ultima revisione
Versione 01 – 15 gennaio 2024

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 l'utilizzo del cloud istituzionale presentano 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:

- sussistono "trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati";

- sussistono "trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)";

- sono trattati "dati sensibili o di natura 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)";

- sussistono "trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni";

- sussistono "trattamenti di 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";

- il trattamento avviene su larga scala.

3. INTRODUZIONE NORMATIVA

3.1 LA VALUTAZIONE DI IMPATTO

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".

[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).

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. 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 del 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 Cloud", 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. CONTESTO DEL TRATTAMENTO: LA MIGRAZIONE ALL'AMBIENTE CLOUD DA PARTE DELLA PUBBLICA AMMINISTRAZIONE

Il Piano Triennale per l'informatica nella Pubblica Amministrazione (di seguito, il "Piano Triennale") promuove la trasformazione digitale della Pubblica Amministrazione attraverso la declinazione della strategia in materia di digitalizzazione in indicazioni operative, quali obiettivi e risultati attesi.

La prima edizione del Piano Triennale (2017-2019) mirava soprattutto all'introduzione del modello strategico dell'informatica e la seconda edizione (2019-2021) si proponeva di dettagliare l'implementazione del modello; infine il Piano Triennale 2020-2022 e il suo aggiornamento 2021-2023 sono stati maggiormente focalizzati sulla componente implementativa, ossia sull'attenzione alle azioni previste e sul monitoraggio dei risultati.

Da ultimo, l'aggiornamento 2022 – 2024 costituisce l'evoluzione delle due precedenti edizioni, ma attribuisce uno spazio più rilevante al Piano Nazionale di Ripresa e Resilienza (di seguito, "PNRR"), oltre a fornire un quadro organico dei vari ambiti di cui si compone, tramite la collaborazione con i soggetti che esercitano competenze istituzionali e responsabilità sull'implementazione.

L'aggiornamento 2022 – 2024 ha confermato il cd. principio *cloud first* (cloud come prima opzione), secondo il quale le Pubbliche Amministrazioni, in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi, adottano primariamente il cloud, tenendo conto della necessità di prevenire il rischio di lock-in.

Due finanziamenti previsti nel PNRR mirano all'applicazione del principio *cloud first* da parte della Pubblica Amministrazione, cioè l'"Investimento 1.1: Infrastrutture digitali" e l'"Investimento 1.2: Abilitazione e facilitazione migrazione al cloud". Come meglio si preciserà nel prossimo paragrafo, il Comune ha presentato richiesta di finanziamento per la migrazione verso ambienti cloud in forza dell'Investimento 1.2.

All'interno di tale contesto, in relazione alla migrazione verso ambienti cloud da parte della Pubblica Amministrazione, rilevano altresì le determinazioni dell'Agenzia per l'Italia Digitale (di seguito, "AgID") e dell'Agenzia per la Cybersicurezza Nazionale (di seguito, "ACN"). Infatti, tali soggetti hanno individuato caratteristiche inerenti agli aspetti di sicurezza che deve presentare l'ambiente cloud in relazione ai dati in generale, quindi non solamente quelli personali, sulla base di un rischio basato sulle conseguenze per la comunità se un determinato dato venisse violato nella sua riservatezza, integrità o disponibilità.

Ai sensi dell'art. 33-septies, co. 4, D.L. 179/2019, convertito con modificazioni dalla L. 221/2012, AgID ha approvato in data 15/12/2021, con determinazione n. 638/2021, il regolamento recante i livelli minimi di sicurezza, capacità elaborativa, risparmio energetico e affidabilità delle infrastrutture digitali per la PA e le caratteristiche di qualità, sicurezza, performance e scalabilità, portabilità dei servizi cloud per la pubblica amministrazione, le modalità di migrazione nonché le modalità di qualificazione dei servizi cloud per la pubblica amministrazione, modificato dalla Determina dell'ACN 307 del 18/1/2022 (di seguito, il "Regolamento AgID").

Ai sensi dell'art. 3 del Regolamento AgID, i dati e i servizi digitali delle amministrazioni sono classificati, sulla base della loro caratterizzazione, nelle seguenti tre classi:

a. strategici, se la loro compromissione può determinare un pregiudizio alla sicurezza nazionale;

b. critici, se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese;

c. ordinari, qualora la loro compromissione non determini i pregiudizi di cui alle lettere a) e b).

Nell'allegato B del Regolamento AgID sono previste le caratteristiche di base di qualità, di sicurezza, di performance e di scalabilità, di interoperabilità e di portabilità che i servizi di cloud per la PA devono possedere. Tali caratteristiche variano sulla base della classificazione dei dati e dei servizi: per i dati strategici sono previste caratteristiche di gestione e sicurezza più stringenti di quelle previste rispettivamente per i dati critici e i dati ordinari.

Ai sensi dell'art. 11 del Regolamento AgID, l'ACN, d'intesa con il Dipartimento per la Trasformazione Digitale, ha definito i criteri per la qualificazione dei servizi cloud per la pubblica amministrazione per le seguenti quattro tipologie:

a. qualificazione cloud di livello 1 (QC1);

b. qualificazione cloud di livello 2 (QC2);

c. qualificazione cloud di livello 3 (QC3);

d. qualificazione cloud di livello 4 (QC4).

Tali criteri sono stati elaborati in relazione al rischio e all'evoluzione della minaccia tecnica di natura cibernetica, tenuto conto della normativa e degli standard nazionali, europei e internazionali e tenendo in considerazione gli schemi di certificazione europei progressivamente adottati ai sensi del Regolamento (UE) 2019/881 (cd. Regolamento CSA o sulla cybersicurezza).

Nello specifico, sempre ai sensi dell'art. 11 del Regolamento AgID, i dati e i servizi digitali classificati come ordinari possono essere erogati tramite servizi cloud qualificati di livello 1 o 2; quelli classificati come critici possono essere erogati tramite servizi cloud di livello 2, 3 o 4; quelli classificati come strategici possono essere erogati tramite servizi cloud di livello 3 o 4.

6. DESCRIZIONE DEL TRATTAMENTO

Il Comune di Fiesso d'Artico (nel prosieguo il "Comune") 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 internet del Comune, sono i seguenti: economico-amministrativo; lavori pubblici, patrimonio, manutenzioni, ecologia, protezione civile; edilizia privata, urbanistica, ambiente; socio-culturale.

Il Comune tratta numerosi dati personali, compresi dati di categorie particolari ai sensi dell'art. 9 GDPR e dati personali relativi a condanne penali e reati ai sensi dell'art. 10 GDPR, soprattutto al fine di svolgere i propri compiti di interesse pubblico e pubblici poteri di cui è investito.

Il Comune intende procedere alla migrazione verso ambienti cloud dei database e delle applicazioni e servizi beneficiando dei fondi appositamente previsti nel PNRR. In data 26/04/2022 è stato pubblicato, nell'ambito del PNRR, l'Avviso Misura 1.2 "Abilitazione al Cloud per le P.A. locali Aprile 2022 – Comuni", con scadenza presentazione istanze in data 22/07/2022, con il quale le Pubbliche Amministrazioni possono presentare richieste di finanziamento, per la migrazione verso ambienti cloud delle basi dati e delle applicazioni e servizi dell'Amministrazione, comprensivo delle attività di assessment (valutazione), pianificazione della migrazione, esecuzione e completamento della migrazione e formazione del personale, relativamente ai Centri Elaborazione Dati.

In data 26/05/2022 il Comune ha presentato la propria candidatura al suddetto Avviso, protocollo n. 6642 del 27/05/2022. In tale occasione, il Comune ha contestualmente dichiarato che tutti i dati e i servizi digitali sono classificabili come ordinari. Ne consegue che essi possono essere erogati tramite servizi cloud di livello 1 (QC1) ai sensi dell'art. 11 del Regolamento AgID.

In data 21/06/2022, con provvedimento protocollo n. 7771 del 21/06/2022, il Dipartimento per la trasformazione digitale ha comunicato l'ammissione della candidatura n. 13250 del Comune.

Con determinazione n. 80 del 08/02/2023, il Comune ha affidato alla società Maggioli S.p.A. l'incarico per il passaggio in cloud dei servizi comunali mediante la migrazione e l'aggiornamento evolutivo e funzionale del software gestionale attualmente in dotazione al Comune, con l'aggiornamento in sicurezza di applicazioni in cloud, mediante l'utilizzo della modalità Software as a Service (Saas). Infatti, il Comune attualmente adopera Sicraweb ed intende migrare all'applicativo Sicraweb EVO, che è stato qualificato da ACN come cloud di livello 1 (QC1) in data 19/01/2023, con data di scadenza al 18/01/2024, ID scheda n. SA-2412 (All. 1).

Maggioli S.p.A. gestirà quindi la migrazione dei seguenti servizi, più specificamente descritti nel prosieguo del presente paragrafo:

1. Demografici – Anagrafe;
2. Demografici – Stato Civile;
3. Demografici – Cimiteri;
4. Demografici – Elettorale;
5. Protocollo;
6. Albo Pretorio;
7. Contabilità e Ragioneria;
8. Economato;
9. Gestione Economica;
10. Trasparenza;
11. Organi Istituzionali;
12. Contratti;
13. Ordinanze.

In relazione alla migrazione del servizio di "Produttività individuale", cioè la migrazione dei documenti in cloud, essa avverrà mediante la modalità di trasferimento in sicurezza dell'infrastruttura Information Technology. Con determina n. 145 del 09/03/2023 il Comune ha affidato il relativo incarico alla società Euganea Innovazione S.r.l.

Infine, con determinazione n. 215 del 21/04/2023, è stato affidato l'incarico del servizio di hosting del passaggio al cloud dei dati e delle basi di dati comunali per il triennio 2023-2026 alla società Criticalcase S.r.l., la quale è accreditata presso ACN dello svolgimento del servizio di Cloud Service Provider. Tale servizio di hosting sfrutterà altresì applicativi offerti da Google.

Più precisamente, Criticalcase fornirà l'hosting per il servizio denominato "Produttività individuale", che sarà oggetto di migrazione ad opera di Euganea Innovazione.

Il Comune finora si è servito di due server in locale, uno dedicato ai domini, quindi alle utenze, ai privilegi e autorizzazioni di ciascun utente, mentre il secondo è dedicato ai documenti informatici che il Comune produce ed elabora durante la sua attività quotidiana. Il contenuto di tali due server costituisce il servizio "Produttività individuale" sopra citato. A migrazione ultimata, i due server locali non saranno più utilizzati e dismessi.

Come anticipato, il Comune intende avvalersi altresì di Sicraweb EVO, una suite strutturata per la gestione delle attività delle Amministrazioni Locali. Tale suite è offerta da Maggioli S.p.A. ed è una soluzione Software as a Service ("SaaS") che favorisce la migrazione degli enti locali al cloud e si appoggia a Google Cloud. Tale suite verrà utilizzata per tutti i documenti ufficiali del Comune (in via esemplificativa, provvedimenti del Sindaco, delibere della Giunta comunale, atti inerenti procedimenti amministrativi, ecc.) e i messaggi di posta elettronica certificata, costituendo uno strumento di lavoro parallelo rispetto al cloud dedicato al servizio di "Produttività individuale", dove invece vengono elaborati ed archiviati tutti i documenti prodotti dal Comune, senza esclusione alcuna.

La suite integra le informazioni tra i vari uffici del Comune, tra il Comune e soggetti privati, e infine con i servizi di gestione documentale, favorendo la realizzazione di sistemi di archiviazione e di ricerca documentale.

Sicraweb EVO è composta da una serie di verticali modulari, realizzate sulle esigenze di ogni singolo ufficio del Comune: tutte le informazioni (anagrafiche, tributarie, catastali, ecc.) sono condivise dalle applicazioni verticali, favorendo una condivisione del dato tra uffici diversi.

Uno degli obiettivi della suite è quindi quello di creare una repository documentale comune e di permettere la ricerca di dati all'interno del database. A tal fine vengono impiegate tecniche di data-mining.

Sicraweb EVO gestisce altresì lo storico di tutti i dati che possono subire variazioni nel tempo, permettendo di recuperare i dati registrati in una determinata data. La suite consente quindi la completa ricostruzione storica e registra automaticamente in archivi di log i principali interventi di aggiornamento e stampa.

Entrando nel dettaglio, Sicraweb EVO è una suite che offre la possibilità di implementare i seguenti sistemi informativi:

1) Iride EVO (Sistema informativo per la gestione dei flussi documentali e dei procedimenti amministrativi)
   Software applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, per la gestione delle informazioni, dei documenti, dei processi e dei procedimenti amministrativi; realizza il tracciamento e l'esecuzione automatica dei flussi di lavoro (Work-Flow) e di Gestione Documentale.
   Tale piattaforma è composta da un'ampia gamma di moduli applicativi immediatamente fruibili a supporto dei processi del Comune: protocollo informatico, atti monocratici e collegiali, messi notificatori, contratti, gestione prenotazioni appuntamenti e risorse.
   Tutte le informazioni sono convalidabili con l'apposizione della Firma Digitale e sono protette da accessi non autorizzati (Access Control List). Il sistema informativo è dotato di un nucleo base a cui si possono aggiungere una serie di componenti applicative ed una serie di componenti di integrazione.

2) Serfin EVO (Sistema informativo per la gestione dei servizi finanziari)
   Software gestionale applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, e consente una gestione integrata, coerente ed unificata delle problematiche relative alla contabilità finanziaria.

Il sistema contabile finanziario Serfin EVO è la componente di base che coordina e governa tutte le restanti componenti del sistema: la contabilità economica-patrimoniale, derivata dalla contabilità finanziaria attraverso il Piano dei Conti Integrato, la contabilità fiscale, la gestione delle fatture elettroniche, e che nel loro complesso costituiscono un Sistema Informativo Contabile Integrato.
Il Sistema Contabile Integrato Serfin EVO è organizzato in moduli funzionali ciascuno dei quali è incaricato di gestire aspetti specifici e funzionalità di competenza dei vari Servizi e Uffici dell'Area economico finanziaria:

- Contabilità Finanziaria;
- Contabilità economico-patrimoniale;
- Contabilità Fiscale (IVA, Split Payment, Ritenute fiscali);
- Fattura Elettronica;
- Mutui;
- Cassa Economale e Agenti Contabili;
- Magazzino Economale e Ordini;
- Inventario;
- Collegamento telematico con Tesoreria (ordinativo informatico)/Siope+;
- Esportazione dati BDAP.

3) Smart EVO (Sistema informativo per il controllo di gestione e la valutazione delle performance)
Software gestionale applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, creato per l'implementazione e l'informatizzazione del sistema di Controllo di Gestione (cd. "Governance Interna") e di valutazione della performance attraverso la gestione di un piano dettagliato degli obiettivi.
Smart EVO ha un elevato grado di personalizzazione e flessibilità. Prevede una procedura basata sul metodo degli Indicatori diretta a verificare l'efficacia, l'efficienza e l'economicità ottenuti nella realizzazione degli obiettivi programmati.
Attraverso questa procedura viene previsto un iter metodologico che parte dalla predisposizione di un piano dettagliato di obiettivi, alla rilevazione dei costi e dei proventi dei risultati ottenuti, fino alla valutazione dei risultati in relazione al piano strategico pianificato.
Il sistema consente la gestione coordinata e coerente dell'intero ciclo della programmazione, partendo dalla pianificazione strategica fino alla programmazione operativa.
Tale gestionale applicativo opera condividendo e integrandosi con il sistema economico-contabile Serfin EVO, con il quale condivide la stessa base dati. In una logica di integrazione del ciclo di programmazione gestionale con la programmazione economico-finanziaria, Smart EVO consente il collegamento dell'obiettivo/attività gestionale alle movimentazioni di contabilità finanziaria.

4) Trib EVO (Sistema informativo per la gestione delle entrate locali e dei servizi a domanda individuale)
Software gestionale applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, per la gestione completa dei servizi Ici/Imu, Tarsu/Tia, Tares, Icp, Dpa, Tosap e a domanda individuale. L'integrazione nella Suite consente di condividere il motore di calcolo, la gestione dei pagamenti, l'interfacciamento con PagoPA, il workflow, il repository documentale e l'integrazione con la conservazione documentale.
Trib EVO è parte integrante della suite Sicraweb EVO con cui condivide nativamente: l'indice generale dei soggetti, la gestione del territorio, il motore di calcolo, la gestione dei pagamenti e l'interfacciamento con PagoPA, il workflow, il repository documentale e l'integrazione con la conservazione documentale, il monitoraggio dei debiti e dei pagamenti, la gestione della sicurezza e della privacy by design.
L'essere parte integrante di Sicraweb EVO consente a Trib EVO di automatizzare nativamente processi come:

- protocollazione e firma digitale massiva (Iride EVO):
- movimentazione TARI da una variazione demografica (Demos EVO);
- movimentazione degli oggetti a canone da un iter di rilascio (Aut EVO);
- disponibilità di un accesso all'atto della creazione nel territorio e visualizzazione cartografica (Ter EVO).

La tecnologia di Trib EVO consente la massima apertura verso componenti di terze parti permettendo l'interfacciamento con:

- il sistema di pagamento digitale degli F24;

- il sistema di produzione di video comunicativi (video bolletta Tari) nel pieno adempimento della delibera 444/2019 di Arera;
- il sistema ini-pec di Infocamere per l'aggiornamento delle PEC;
- il sistema della camera di commercio per l'acquisizione dei codici ateco;
- i servizi posti a disposizione dall'Agenzia delle Entrate e utili alla gestione delle entrate locali;
- il sistema di gestione della firma grafometrica;
- i sistemi di raccolta e tracciatura dei rifiuti per consentire il calcolo puntuale della Tari;
- i servizi posti a disposizione da piattaforme a riuso in aderenza con quanto richiesto da AGID.

5) Demos EVO (Sistema informativo per la gestione dei servizi demografici)
Software gestionale applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, per la gestione completa dei servizi Anagrafe, ANPR, Elettorale, Stato Civile, Leva, Statistica, Carta d'Identità Elettronica (CIE), giudici popolari.
L'integrazione è specializzata al fine di agevolare l'operatore in tutte le attività interconnesse con i vari uffici grazie ad automatismi nella compilazione di schede ed elenchi:
   - Integrazione con altri Uffici del Comune: Demos EVO condivide gli archivi e mette a disposizione dell'Ente le informazioni sotto forma di schede, elenchi e dati statistici;
   - Integrazione con altri Enti e/o Privati: Demos EVO consente di dialogare con cittadini, imprese, liberi professionisti e altri Enti che hanno l'esigenza di usufruire di servizi specializzati grazie a procedure telematiche e tradizionali; l'interfaccia dell'applicativo d'anagrafe con il CNSD (Centro Nazionale Servizi Demografici) garantisce il rapporto diretto così come previsto dalle normative verso la banca dati dell'INA e il sistema di emissione della CIE;
   - Integrazione con il sistema di protocollo informatico: Demos EVO collega automaticamente, attraverso il Protocollo Informatico, le attività di stampa alle funzioni che generano i numeri di protocollo;
   - Integrazione con i servizi di Gestione Elettronica Documentale: servizi per archiviare e gestire elettronicamente i documenti e il patrimonio informativo del cliente per rendere efficienti attività dispendiose come consultazione, distribuzione, archiviazione e ricerca.

6) Cim EVO (Sistema informativo per la gestione dei servizi cimiteriali)
Software applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, per la gestione dei servizi cimiteriali; contiene schedario dei defunti, struttura ed elementi dei cimiteri, area concessioni, registri delle operazioni o dei trasferimenti, elenco di aventi diritto, gestione lampade votive e gestione grafica delle strutture cimiteriali.
L'anagrafica unica fornisce una piena integrazione tra lampade votive e concessioni cimiteriali oltre che con le altre applicazioni di Sicraweb EVO.
La definizione della struttura dei cimiteri consente di modellare l'articolazione del cimitero rispettando le convenzioni e le abitudini locali. Lo schedario consente di inserire i dati anagrafici completi, le cause della morte, la fotografia del defunto, lo stato fisico delle spoglie (salma, resti, ceneri) e la storia delle movimentazioni.
Sono disponibili servizi a supporto dell'ufficio cimiteriale: digitalizzazione delle concessioni e delle mappe cimiteriali, rilievi fisici, popolamento e analisi delle banche dati.

7) Pers EVO (Sistema informativo per la gestione delle risorse umane)
Software applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, per semplificare gli adempimenti e le necessità di una moderna Gestione del Personale; realizzata utilizzando le due piattaforme applicative SicraWeb EVO e VAADIN portal free e open source.

8) Pe EVO (Sistema informativo per la gestione delle pratiche edilizie)
Software applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, dedicato alla gestione delle pratiche edilizie (permessi di costruire, CILA/SCIA, valutazioni preventive, autorizzazioni ambientali ecc.) in conformità alle normative nazionale, regionale, provinciale e ai regolamenti comunali.

PE EVO può essere attivato in modalità standard, fornendo il sistema preconfigurato sulla base dei procedimenti edilizi previsti dalla normativa, oppure in modalità custom sfruttando la possibilità di configurare nuovi e diversi procedimenti e di consentire la gestione attraverso motore di work-flow.
Per ogni pratica vengono gestiti:

- tutti i dati della domanda, dei richiedenti, dei professionisti e delle imprese;
- gli adempimenti e relative scadenze per ciascuna tipologia di pratica;
- la tipologia di intervento;
- i dati urbanistici ed eventuali vincoli;
- l'istruttoria amministrativa e tecnica;
- la gestione di pareri e prescrizioni;
- la gestione e rilascio della pratica e delle licenze ad essa collegate;
- il fascicolo della pratica mediante il sistema di Gestione Documentale.

Il sistema consente inoltre:

- la gestione storica di ogni intervento eseguito su un'opera (intesa come edificio o porzione di terreno) in un determinato momento storico;
- il calcolo degli oneri;
- la consultazione della commissione edilizia e della conferenza dei servizi;
- la visione degli scadenzari e degli adempimenti relativi;
- la presa visione delle denunce delle opere strutturali;
- la consultazione dell'anagrafe tributaria;
- l'automazione di documenti e report.

9) <u>Aut EVO (Sistema informativo per la gestione delle pratiche autorizzatorie)</u>

Acronimo di J-Autorizzazioni, è il software gestionale applicativo della suite Sicraweb EVO, realizzato in tecnologia Java e Web, dedicato alla gestione delle pratiche di Autorizzazione di occupazione di spazi e aree pubbliche, imposta della pubblicità, pubbliche affissioni, e si compone della componente amministrativa (pratiche) e della componente tributaria (tributi).
Aut EVO è l'applicativo della suite Sicraweb EVO dedicato alla gestione delle pratiche di autorizzazione di:

- Occupazione di spazi e aree pubbliche;
- Imposta della pubblicità;
- Pubbliche Affissioni.

Aut EVO si integra con le altre soluzioni della suite Sicraweb per le tematiche di:

- Anagrafe: condivisione delle banche dati dell'anagrafe demografica gestite in Demos EVO e dell'anagrafe generale dei soggetti Sicraweb EVO;
- Stradario: condivisione generale dell'archivio delle strade per la localizzazione dell'occupazione richiesta;
- Protocollo: collegamento con le funzionalità informatiche dei documenti di Iride EVO, in entrata ed in uscita;
- Gestione documentale: gestione dei procedimenti e dei relativi documenti, fascicolazione, gestione della PEC, conservazione sostitutiva;
- Finanziaria: integrazione Serfin EVO per la gestione delle previsioni e dei pagamenti;
- Presentazione online della pratica: portale per la presentazione ed il monitoraggio delle pratiche;
- Pagamenti: integrazione con il sistema PagoPA;
- Cartografia: integrazione con il Ter EVO per la visualizzazione cartografica.

Per ogni pratica di autorizzazione vengono gestiti:

- i dati relativi alla domanda, ai richiedenti, ai soggetti;
- il tipo di richiesta in funzione se si sta chiedendo una pubblicità o un'occupazione;
- l'istruttoria amministrativa e tecnica (documenti, pareri interni ed esterni all'Ente, nullaosta e quant'altro richiesto) e le sospensioni;
- la gestione ed il rilascio della autorizzazione comprensivo della produzione automatica dei documenti necessari, come configurato per la tipologia di pratica o come definito dall'iter associato mediante il motore di workflow.

10) Ter EVO (Sistema informativo per la gestione della cartografia)

Ter EVO introduce, come "funzione" della suite Sicraweb EVO, uno strumento in grado di rappresentare dati cartografici gestiti internamente alla suite o provenienti da servizi cartografici WMS resi disponibili da fonti esterne; in un'unica banca dati sono presenti e correlate tutte le informazioni gestionali e di localizzazione cartografica.

Ter EVO consente:

- produzione di mappe tematiche: la rappresentazione cartografica diventa la semplice estensione delle funzionalità di ricerca ed estrazione dati;
- analisi del territorio, la ricerca e l'identificazione dell'oggetto o degli oggetti di interesse per il recupero automatico, in base ai privilegio di accesso ai dati assegnati all'utente;
- generazione automatica delle mappe catastali direttamente dall'importazione dei dati forniti dell'Agenzia delle Entrate e la loro visualizzazione;
- misurazione delle planimetrie catastali fornite dall'Agenzia delle Entrate e recupero automatico delle misure dei vani effettuate nella scheda dell'immobile;
- acquisizione e visualizzazione dei dati cartografici provenienti da fonti esterne o interne attraverso servizi standard WMS.

Ter EVO consente di acquisire e rappresentare le informazioni cartografiche dell'Ente, come ad esempio:

- lo strumento urbanistico: servizio personalizzato per il recupero delle informazioni urbanistiche dell'Ufficio Tributi e dell'Ufficio Tecnico, per attività di consultazione e di recupero automatico delle norme attuative o per la produzione automatica del Certificato di Destinazione Urbanistica;
- lo stradario e la numerazione civica: servizio personalizzato per il recupero dati dell'Ente con rappresentazione cartografica dello stradario e degli accessi del territorio, per metterli in relazione con le informazioni già presenti nell'archivio di Sicraweb EVO ed utilizzati da tutti i moduli gestionali;

Consente inoltre di collegarsi a:

- servizi cartografici basati su dati open source (*OpenStreetMap*), per la visualizzazione della mappa e per la navigazione nelle informazioni relative a stradario e numerazione civica;
- l'accesso alle immagini panoramiche di *Street View* di *Google Maps* per la rappresentazione virtuale e l'esplorazione dei luoghi di interesse.

11) Com EVO (Sistema informativo per la gestione delle attività economiche)

Modulo software della Suite Sicraweb EVO che gestisce l'archivio delle attività economiche presenti sul territorio comunale: una soluzione integrata con la piattaforma di gestione delle pratiche Suap che consente di inserire, modificare e storicizzare tutta l'attività.

Il sistema consente di effettuare l'istruttoria della pratica, la verifica della documentazione ricevuta e la possibilità di produrre documenti da trasmettere, la richiesta parere ad enti Terzi o interni. Il flusso si conclude poi con la generazione di un provvedimento autorizzativo finale, laddove necessario, con la possibilità di avere registri specifici per ogni tipologia di Autorizzazione.

Com EVO consente la gestione precisa e puntuale di tutti i mercati, con i relativi posteggi e con la possibilità di avere la profondità storica del:

- concessionario del posteggio;
- gestione delle presenze e assenze per ogni giornata di mercato;
- gestione della bollettazione delle tariffe per ogni singolo concessionario;
- gestione degli spuntisti con relative presenze per ogni giornata di mercato.

È prevista anche la visualizzazione grafica della situazione dei posteggi per ogni singolo mercato, fiera, manifestazione, con l'evidenza dei posteggi liberi e occupati. È prevista altresì la visualizzazione dei calendari di ogni singolo mercato, con l'indicazione se la giornata è stata svolta, se sono state elaborate le presenze dei concessionari e se la giornata di mercato è stata chiusa. Elenco dei concessionari abilitati a svolgere la giornata di mercato, con indicazione della presenza o assenza nella giornata che si sta elaborando.

Dopo aver elaborato i concessionari, si abilita in automatico la gestione degli spuntisti, anche in questo caso sarà possibile indicare la sola presenza al mercato e la presenza effettiva nel caso di assegnazione di un posteggio libero.

Ogni graduatoria è specifica per categoria (spuntisti o concessionari). In fase di creazione si configurano:

- requisiti per l'ammissione;
- quesiti per l'attribuzione dei punteggi da attribuire ad ogni soggetto;
- allegati che devono essere presentati per l'ammissione;
- liste che devono essere prodotte dopo la chiusura della graduatoria;
- lista di attesa che deve essere prodotta nel caso di una graduatoria con posti limitati, per i soggetti aventi diritto e che risultano in una posizione eccedente il numero massimo di posti.

Ogni graduatoria può essere popolata manualmente o attraverso la funzione di popolamento massivo.
Per ogni domanda presente nella graduatoria è possibile verificare l'esito dei requisiti/quesiti.

12) Suap EVO (Sistema informativo per la gestione delle attività produttive)

Suap EVO informatizza lo scambio elettronico dei documenti dalla presentazione della richiesta da parte delle imprese, fino alla conclusione dell'iter istruttorio. Tutto il flusso informativo da e verso il Comune viene scadenzato e monitorato attraverso processi gestiti attraverso un motore di workflow.
Il SUAP si occupa di interfacciarsi con gli uffici comunali coinvolti nel procedimento, nonché con gli Enti esterni al Comune, fornendo la documentazione necessaria affinché gli stessi possano provvedere al rilascio dell'eventuale parere e/o nulla osta di competenza.
Sarà inoltre necessario prevedere l'informatizzazione del fascicolo documentale per permettere la corretta gestione della domanda unica, dei documenti allegati e, allo stesso modo, predisporre i modelli di output per l'inoltro dei pareri agli Enti Terzi.

13) Concilia (Software gestionale che governa le attività dei Comandi di Polizia Locale)

Sistema informativo per la gestione delle violazioni al Codice della Strada ed extra-Codice della Strada realizzata per la gestione delle attività dei Comandi di Polizia Locale, con un parco installato di oltre 2000 unità tra Comuni, Associazioni di Comuni, Consorzi, Unioni e Province.
Concilia è il software per la Polizia Municipale e Locale e contiene l'intero iter procedurale che l'operatore usa abitualmente durante il lavoro ordinario nel proprio ufficio.
Prevede una serie di moduli, tra cui la Verbalizzazione: infatti è il software di gestione verbali di violazione al Codice della Strada, sanzioni extra-Codice della Strada (leggi di polizia amministrativa o sul commercio, regolamenti comunali, leggi sul commercio), stampa in più lingue dei verbali (Concilia Stranieri) e Concilia Road, su notebook, ideale per la contestazione verbali su strada.
Concilia Software insieme a Concilia Service Plus (il servizio in outsourcing per la gestione completa delle violazioni al Codice della Strada ed extra Codice della Strada) e Autoscan (la piattaforma per la gestione dei dispositivi per la lettura delle targhe dei veicoli e del rilevamento delle violazioni al Codice della Strada) compongono Concilia, l'ecosistema per la sicurezza stradale e il monitoraggio territorio.
Il software per la Polizia Municipale Concilia è accreditato AgID come Cloud Service Provider (CSP) per servizi SaaS e l'offerta disponibile sul Marketplace della PA.

14) Appalti Contratti EProcurement (Piattaforma web integrata per la gestione di contratti pubblici)

La piattaforma web integrata per supportare l'Ente Pubblico nella gestione dell'intero ciclo di vita di un contratto pubblico, dalla nascita dell'esigenza di affidamento fino al collaudo e accettazione, passando attraverso le fasi di affidamento in senso stretto (e-procurement) e fornendo il necessario supporto in tutte le fasi di monitoraggio e rendicontazione post aggiudicazione.
È una piattaforma composta da applicazioni integrate, in grado di supportare l'Ente Pubblico nella gestione dell'intero ciclo di vita di un contratto pubblico, dalla nascita dell'esigenza di affidamento fino al collaudo/accettazione, passando attraverso le fasi di affidamento in senso stretto (e-procurement) e garantendo il necessario supporto in tutte le fasi di monitoraggio e rendicontazione post aggiudicazione.
La piattaforma dispone di diversi moduli applicativi ognuno dei quali risponde alle esigenze operative e di rendicontazione di una determinata fase del ciclo di vita di un contratto pubblico. Tutti i moduli sono nativamente integrati tra loro in modo per evitare la duplicazione di inserimento di informazioni per fini diversi.

15) Icaro EVO (Software gestionale per Servizi Socio Assistenziali e Socio Sanitari)

ICARO EVO è il sistema informativo web nativo realizzato per supportare gli Enti Locali ed Aziende Sanitarie nella gestione integrata dei Servizi Socio-Assistenziali e Socio-Sanitari.
Supporta tutti i processi organizzativi legati all'attività di assistenza a persone o a famiglie che si trovano in uno stato di bisogno o che devono essere assistite a domicilio.
È una applicazione software per il governo della rete degli interventi e dei servizi alla persona e affronta tutte le problematiche della gestione operativa, del monitoraggio, della programmazione e della rendicontazione dei Servizi Sociali.
Il software Icaro EVO è conforme alla normativa vigente in tema di servizi socio assistenziali e in particolare alla legge 8 novembre 2000, n. 328 "Legge quadro per la realizzazione del sistema integrato di interventi e servizi sociali", al decreto direttoriale n. 103 del 15 Settembre 2016 "Casellario Assistenza" e al D.L. n. 147 del 15 settembre 2017 "Disposizioni per l'introduzione di una misura nazionale di contrasto alla povertà".

16) Auxilium (Software gestionale per l'assistenza Integrativa)
Il software permette la gestione del magazzino aziendale, la gestione delle pratiche di concessione e della consegna di protesi, di presidi ed ausili a varie tipologie di individui residenti nel territorio di competenza dell'Azienda Sanitaria Locale, quali invalidi, minori e persone in attesa di completamento della pratica di invalidità.
È il software per il governo dei processi di Assistenza Integrativa di competenza dell'Azienda Sanitaria Locale e gestiti in collaborazione con il territorio.
Il sistema provvede, nel rispetto della normativa di legge vigente, alla gestione delle pratiche di concessione e della consegna di protesi, di presidi ed ausili a varie tipologie di individui residenti nel territorio di competenza della Azienda Sanitaria Locale, e segnatamente a invalidi, minori e persone in attesa di completamento della pratica di invalidità.
Il sistema viene integrato con la Base Informativa Anagrafica Aziendale in modo da poter ricevere in tempo reale gli aggiornamenti delle informazioni anagrafico sanitarie dei soggetti di competenza e di poterle mettere a disposizione per il trattamento dei dati relativi, direttamente dall'interno dell'applicazione.

Allo stato, il Comune ha programmato di servirsi dei seguenti sistemi informativi in cloud: Iride EVO, Serfin EVO, Trib EVO, Demos EVO, Cim EVO, Pe EVO.

6.1 FLUSSI DI DATI

I dati saranno oggetto di migrazione ad opera delle due società incaricate Maggioli S.p.A. ed Euganea Innovazione S.r.l. La prima ha presentato un piano di migrazione, a cui si rinvia (All. 2).

Euganea Innovazione non ha ancora potuto redigere un piano di migrazione: questo sarà implementato dopo che la società Maggioli S.p.A. avrà terminato la propria attività di migrazione per questioni operative e organizzative.

Una volta completata la migrazione da parte di entrambi i soggetti, i dati saranno trattati totalmente in cloud.

I dati verranno allora inseriti nel cloud o direttamente dagli interessati o da dipendenti ovvero collaboratori di persone giuridiche, enti o associazioni in via telematica, tramite l'invio di comunicazioni dirette al Comune. Inoltre, potranno essere inseriti da soggetti appositamente incaricati ed autorizzati, cioè dai dipendenti del Comune stesso.

6.2 DATI TRATTATI E CATEGORIE DI INTERESSATI

Il Comune tratta i dati personali dei cittadini residenti nel territorio comunale, di soggetti beneficiari di servizi, anche se non residenti nel territorio, del personale del Comune ovvero di ulteriori soggetti i cui dati sono trattati per rispondere ad un obbligo di legge o di regolamento o per fornire loro servizi di interesse pubblico.

Tra gli interessati sono ricompresi anche soggetti particolarmente vulnerabili, come minori, soggetti diversamente abili e soggetti in difficoltà economica.

I titolari vengono di volta in volta resi edotti delle modalità del trattamento dei loro dati e dei soggetti autorizzati ad accedervi mediante le informative appositamente predisposte dal Comune.

I dati personali trattati sono numerosi e di diverse categorie e vengono selezionati sulla base del servizio erogato e/o del compito o interesse pubblico che il Comune è chiamato a svolgere ed esercitare di volta in volta. Tra essi sono ricompresi

anche categorie particolari di dati ai sensi dell'art. 9 GDPR oppure di dati relativi a condanne penali e a reati di cui all'art. 10 GDPR.

In relazione ai pacchetti di SicrawebEvo che il Comune ha programmato di implementare, si ritiene che vengano trattati i seguenti dati personali:

Iride EVO	DATI COMUNI Nomi e cognomi, codici fiscali, luogo e data di nascita, dati di contatto, residenza, domicilio, ruoli istituzionali, numeri e codici identificativi, curriculum vitae, informazioni relative alle proprietà mobiliari registrate e immobiliari, informazioni relative a procedimenti sanzionatori, dati bancari, dati finanziari, economici e patrimoniali, professione, stato di disoccupazione, dati relativi alla vita privata, stato coniugale, stato di convivenza, nazionalità, permessi di soggiorno, capacità di elettorato passivo e attivo, stato servizio militare, stato di famiglia, iscrizione ad associazioni o altri enti, titolarità di documenti, licenze o autorizzazioni, qualsiasi altro dato personale che possa essere contenuto in un documento del Comune. DATI APPARTENENTI A CATEGORIE PARTICOLARI E GIUDIZIARI Origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza.
Serfin EVO	DATI COMUNI Nomi e cognomi, codici fiscali, dati di contatto, residenza, domicilio, dati finanziari, economici e patrimoniali, dati bancari.
Trib EVO	DATI COMUNI Nomi e cognomi, codici fiscali, dati di contatto, residenza, domicilio, dati finanziari, economici e patrimoniali, dati bancari.
Demos EVO	DATI COMUNI Nomi e cognomi, codici fiscali, luogo e data di nascita, dati di contatto, residenza, domicilio, ruoli istituzionali, numeri e codici identificativi, curriculum vitae, informazioni relative alle proprietà mobiliari registrate e immobiliari, informazioni relative a procedimenti sanzionatori, dati bancari, dati finanziari, economici e patrimoniali, professione, stato di disoccupazione, dati relativi alla vita privata, stato coniugale, stato di convivenza, nazionalità, permessi di soggiorno, capacità di elettorato passivo e attivo, stato servizio militare, stato di famiglia, iscrizione ad associazioni o altri enti, titolarità di documenti, licenze o autorizzazioni, qualsiasi altro dato personale che possa essere contenuto in un documento del Comune. DATI APPARTENENTI A CATEGORIE PARTICOLARI E GIUDIZIARI Origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, appartenenza sindacale, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza.
Cim EVO	DATI COMUNI Nomi e cognomi, codici fiscali, dati di contatto, residenza, domicilio, dati bancari. DATI APPARTENENTI A CATEGORIE PARTICOLARI convinzioni religiose o filosofiche.
Pe EVO	DATI COMUNI

	Nomi e cognomi, codici fiscali, luogo e data di nascita, dati di contatto, residenza, domicilio, ruoli istituzionali, informazioni relative alle proprietà immobiliari, informazioni relative a procedimenti sanzionatori, qualsiasi altro dato personale eventualmente contenuto nei documenti necessari per i procedimenti edilizi.

Per una descrizione più dettagliata e precisa delle categorie di interessati e dei dati personali trattati dal Comune, si rinvia al Registro dei trattamenti del Comune stesso.

6.3 FINALITÀ DEL TRATTAMENTO

Attraverso Sicraweb EVO, il Comune intende migrare la gestione dei dati relativi all'attività istituzionale del Comune su cloud, all'interno del quale poter gestire le proprie attività e quindi i trattamenti dei dati personali, nonché creare una repository documentale, anch'essa totalmente in cloud.

Le finalità del trattamento dei dati personali perseguite da parte del Comune (o di soggetti nominati Responsabili al trattamento) sono rappresentate da quelle riportate al paragrafo 6, in relazione ai sistemi informativi Iride EVO, Serfin EVO, Trib EVO, Demos EVO, Cim EVO, Pe EO, e da quanto previsto nel Registro dei trattamenti del Comune, a cui si rinvia.

Attraverso la migrazione del servizio "Produttività individuale", il Comune intende migrare la gestione su cloud di tutti i dati trattati dal Comune, creando anche la relativa repository documentale, totalmente in cloud.

6.4 BASI GIURIDICHE DEI TRATTAMENTI

Il Comune effettua diversi trattamenti, sempre previa individuazione di una corretta base giuridica. Le basi giuridiche dei trattamenti operati dall'ente sono quindi:

1) necessarietà per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art. 6, par. 1, lett. e GDPR).
   Tale base giuridica viene individuata dal Comune recuperando altresì il diritto dell'Unione Europea o il diritto nazionale che la stabilisce. In particolare, rileva l'art. 2-ter del D. Lgs. 196/2003 (cd. "Codice Privacy") e il D. Lgs. 267/2000 (cd. "Testo Unico delle Leggi sull'ordinamento degli enti locali"), oltre alle specifiche normative che regolamentano i singoli servizi che il Comune ha il diritto-dovere di erogare.

2) necessità per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (art. 6, par. 1, lett. c GDPR).
   Tale base giuridica viene individuata dal Comune recuperando altresì il diritto dell'Unione Europea o il diritto nazionale che la stabilisce. In particolare, rileva l'art. 2-ter del D. Lgs. 196/2003 (cd. "Codice Privacy"), oltre alle specifiche normative che regolamentano i singoli obblighi e doveri che gravano sul Comune.

3) necessarietà per l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (art. 6, par. 1, lett. b GDPR).
   Tale base giuridica rileva nelle ipotesi in cui il Comune non svolge attività istituzionale, pertanto quando non sussiste un compito o interesse pubblico. In via esemplificativa, tale base giuridica rileva nei rapporti di lavoro con i dipendenti e collaboratori esterni, in ipotesi di servizi che non rientrano nell'alveo delle attività istituzionali e per il trattamento dei dati personali in occasioni di numerosi bandi o concorsi pubblici.

4) consenso espresso dall'interessato al trattamento dei propri dati personali per una o più specifiche finalità (art. 6, par. 1, lett. a GDPR).
   Si tratta di una base giuridica residuale rispetto alle altre. Viene richiesto il consenso dell'interessato in rare ipotesi, a fronte del ruolo istituzionale ricoperto dal Comune: il consenso rappresenta la base giuridica di alcuni trattamenti di dati personali come, ad esempio, l'iscrizione a newsletter (non istituzionali) o la diffusione di immagini rappresentanti persone fisiche identificabili.

In relazione alle categorie particolari di dati personali, il Comune opera i relativi trattamenti solo qualora sussista una delle eccezioni previste al paragrafo 2 dell'art. 9 GDPR. In particolare, rilevano le seguenti eccezioni a fronte dell'attività istituzionale svolta dal Titolare:

lett. b) - il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;

lett. g) - il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri: in tale ipotesi rileva in particolare l'art. 2-sexies Codice Privacy;

lett. i) - il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale;

lett. j) - il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

Infine, il trattamento di dati personali relativi a condanne penali e reati è effettuato dal Comune solo qualora sia autorizzato dal diritto dell'Unione Europea o nazionale che preveda garanzie appropriate per i diritti e le libertà degli interessati.

In ogni caso, i trattamenti di dati personali sono sempre fondati su idonea base giuridica, come meglio dettagliato nel Registro dei trattamenti del Comune, a cui si rinvia.

6.5 IMPATTO SUGLI INTERESSATI

L'esecuzione di trattamenti di dati personali in ambiente cloud anziché presso i server comunali presenta diversi vantaggi. Consente infatti di migliorare l'efficienza operativa dei sistemi di tecnologia dell'informazione e della comunicazione, di conseguire significative riduzioni di costi, di rendere più semplice ed economico l'aggiornamento dei software, di migliorare la sicurezza e la protezione dei dati e di velocizzare l'erogazione dei servizi a cittadini e imprese.

Tali vantaggi permettono al Comune di poter erogare i propri servizi in modo più efficiente, consentendo una riallocazione delle risorse a vantaggio della comunità, nonché di velocizzare l'erogazione dei servizi stessi, avvantaggiando così l'esercizio dei diritti degli interessati.

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 tramite gli odierni mezzi, che saranno sostituiti con la migrazione al cloud, né la raccolta di dati eccessivi o sproporzionati.

6.6 CONSERVAZIONE DEI DATI

I dati personali sono conservati per un periodo di tempo idoneo al singolo trattamento a cui si riferiscono, come meglio precisato nel Registro dei trattamenti, a cui si rinvia.

I dati personali vengono conservati su cloud: i server sono ubicati presso il Datacenter TIM in Italia, che rientrerà nel futuro Polo Strategico Nazionale.

6.7 RESPONSABILI DEL TRATTAMENTO

Il Comune ha esternalizzato l'attività di migrazione ad ambiente cloud e la sua gestione a soggetti terzi. Qualora il servizio preveda il trattamento di dati personali in nome e per conto del Comune, il soggetto esterno viene nominato Responsabile del trattamento con contratto o altro atto giuridico. A tali soggetti vengono quindi consegnate idonee istruzioni in relazione

alla materia disciplinata, la durata, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del Titolare del trattamento e dello stesso Responsabile.

In occasione della migrazione all'ambiente cloud, il Comune ha aggiornato le nomine di Maggioli S.p.A. e Euganea Innovazione S.r.l. al fine di regolare il trattamento dei dati personali.

Allo stesso modo, il Comune ha nominato Criticalcase S.r.l. quale Responsabile del trattamento per il servizio di hosting, in quanto può avere accesso a dati personali.

7. PROCESSO DI CONSULTAZIONE

Ai sensi dell'art. 35, par. 9, GDPR, in alcuni casi compete al Titolare del trattamento 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.

8. PRINCIPI FONDAMENTALI

L'art. 6 GDPR indica quali sono i principi fondamentali che devono in ogni caso essere seguiti nello svolgimento delle attività e dei trattamenti dei dati personali.

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 ed 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 o al Responsabile 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 trattamento prospettato, 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, questi principi sono stati pienamente rispettati 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.

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

9.1 VALUTAZIONE DELLA NECESSITÀ E PROPORZIONALITÀ

I trattamenti di dati personali qui analizzati 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.

Tuttavia, i trattamenti effettuati dal Comune si rappresentano come necessari per poter adempiere ai propri obblighi e compiti istituzionali. Anche i trattamenti non strettamente riconducibili all'attività istituzionale sono attuati in via accessoria e strumentale al fine di permettere al Comune di svolgere in modo efficace ed efficiente le proprie funzioni.

In ogni caso i dati personali trattati vengono sempre selezionati secondo il principio di minimizzazione in conformità all'art. 5 GDPR, pertanto il Comune tratta categorie di dati personali solamente qualora siano necessari a raggiungere le relative finalità. Per tale motivo, i trattamenti effettuati dal Comune sono proporzionati.

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.

Inoltre, il Piano Triennale per la digitalizzazione delle Pubbliche Amministrazioni prevede il cd. principio *cloud first*, determinando per il Comune la necessità di adottare primariamente un ambiente cloud in fase di definizione di un nuovo progetto e di sviluppo di nuovi servizi.

9.2 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 o in calce a moduli cartacei o tramite pubblicazione nelle sezioni dedicate del sito internet istituzionale del Comune;
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 ai sensi dell'art. 29 GDPR, riportanti le istruzioni impartite dal Titolare del trattamento;
v. adozione di procedure tecniche volte a garantire il recupero dei dati qualora dovessero essere distrutti o persi;
vi. procedure interne per informare gli interessati in merito ai loro diritti, alle relative limitazioni e alle modalità di esercizio;
vii. assenza di trasferimenti di dati personali verso Paesi terzi;
viii. 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 e conserva e aggiorna costantemente un elenco di tutti i Responsabili del trattamento;
ix. acquisizione del consenso degli interessati che, ove richiesto, viene prestato in modo specifico, esplicito, libero e previa consegna di adeguata informativa;
x. garanzia dell'esercizio dei diritti degli interessati previsti dagli artt. 15-22 GDPR.

Alla luce di quanto rilevato ai paragrafi 9.1 e 9.2, è possibile affermare che i trattamenti risultano necessari e proporzionati e non incidono sul contenuto essenziale dei diritti degli interessati.

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

Il trattamento dei dati personali effettuato dal Comune presenta dei 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.

10.1 VALUTAZIONE DELL'IMPATTO

Nel presente paragrafo si riportano i risultati delle analisi e delle valutazioni svolte nell'allegato file Excel "DPIA Cloud", Foglio "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.

Il livello di impatto può essere descritto come basso, medio, alto o molto atto. Si rileva che:

a) l'impatto della perdita di confidenzialità dei dati trattati sui diritti degli interessati risulterebbe molto alto;
b) l'impatto della perdita di integrità dei dati trattati sui diritti degli interessati risulterebbe molto alto;
c) l'impatto della perdita di disponibilità dei dati trattati sui diritti degli interessati risulterebbe molto alto.

Come si può evincere anche dall'immagine (fonte: ENISA), la valutazione complessiva dell'impatto sui diritti degli interessati è risultata quindi di livello "molto alto":

Impact assessment

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Very High	Very High	Very High
	Overall Impact Evaluation	Very High

10.2 VALUTAZIONE DELLA PROBABILITÀ E LIVELLO DI RISCHIO INERENTE

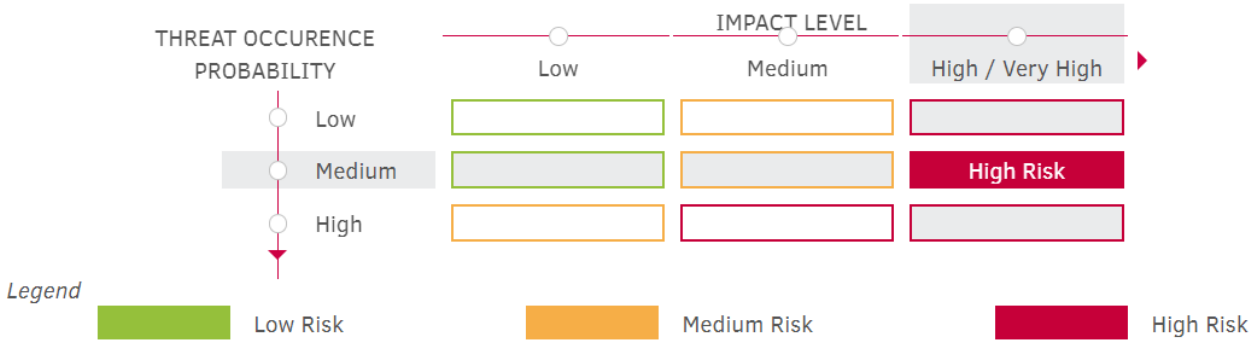
Nel presente paragrafo verranno delineati i principali fattori di rischio che emergono dall'analisi del contesto in cui viene effettuato il trattamento di dati personali, riportando i risultati delle valutazioni documentate nell'allegato file Excel "DPIA Cloud", Foglio "Rischi".

Come si può evincere anche dall'immagine (fonte: ENISA), il livello complessivo di probabilità è medio:

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	Medium	2
Business sector and scale of processing	Medium	2
Overall Threat Occurrence Probability	Medium (8)	

La valutazione del rischio è effettuata combinando i due fattori "impatto" (livello molto alto) e "probabilità" (livello medio), come illustrato negli schemi sottostanti (fonte: ENISA), e risulta essere complessivamente "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. 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.

11. MISURE DI SICUREZZA

Dopo aver analizzato i rischi connessi ai trattamenti dei 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 Cloud", Foglio "Misure" e ai documenti ivi citati predisposti dal Responsabile del trattamento Maggioli S.p.A.

Per l'elenco delle misure di sicurezza, è stato seguito l'"Handbook on security of personal data processing" di ENISA del dicembre 2017. Il suddetto elenco non è stato integrato con le misure di sicurezza individuate da AgID nel Regolamento *ex* art. 33-septies, co. 4, D.L. 179/2019, convertito con modificazioni dalla L. 221/2012, e aggiornate da ACN con successive delibere: la suite Sicraweb EVO è stata qualificata da ACN come cloud di livello 1 (QC1) in data 19/01/2023, con data di scadenza al 18/01/2024, ID scheda n. SA-2412 (All. 1), pertanto tali misure di sicurezza sono da intendersi come implementate, non servendo un'ulteriore valutazione da parte del Comune nella presente Valutazione di Impatto.

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 il fornitore della suite Sicraweb EVO, Maggioli S.p.A., ha conseguito alcune certificazioni relative alle parti di trattamento di dati personali allo stesso 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).

Il servizio di Google Cloud, a cui si appoggia la piattaforma, è conforme a:

- 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));

- Certificazione ISO 27017:2015 (Controlli di sicurezza per i servizi cloud);

- Certificazione ISO 27018 (Codice di Condotta per la protezione delle informazioni personali nei cloud pubblici).

Da ultimo, i data center sui quali si poggia il servizio cloud dispongono di certificazioni ISO, reperibili alla seguente pagina web: link.

È stato altresì preso in considerazione il "Documento di FAQ SicraWEB EVO su Google Cloud" consegnato da Maggioli S.p.A. al Comune (All. 3).

In relazione all'hosting del servizio "Produttività individuale", si rileva che Criticalcase S.r.l. ha conseguito le seguenti certificazioni ISO:

- 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));

- 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)).

Sono state altresì prese in considerazione le informazioni presenti nella seguente pagina web: link.

12. CONCLUSIONI

La presente Valutazione di Impatto ha consentito di determinare un iniziale livello molto alto di rischio del trattamento di dati personali effettuato dal Comune, dato che lo stesso potrebbe potenzialmente avere un impatto critico sulle libertà e i diritti degli interessati.

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

Inoltre, il Comune era altresì soggetto ai vincoli imposti da AgID e ACN in tema di migrazione ad ambiente cloud e scelta dei servizi cloud che fossero stati certificati di livello 1 (QC1), garantendo ulteriormente la implementazione di misure di sicurezza tecniche ed organizzative che si riflettono positivamente anche a vantaggio dei diritti e libertà degli interessati.

Le certificazioni di cui dispongono i fornitori del servizio cloud e di hosting permettono altresì di attestare il possesso di gran parte delle misure di sicurezza tecniche e organizzative ritenute adeguate a 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 dell'arte al 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;

- adottare una policy di sicurezza delle informazioni.