Allegato alla deliberazione di Giunta comunale n.

COMUNE DI RIMINI
MODELLO ORGANIZZATIVO IN MATERIA DI PROTEZIONE DEI DATI PERSONALI
(Regolamento (UE) 2016/679)

TIPO DOCUMENTO: linea guida/policy

REVISIONE DOCUMENTO: 1.1

MODALITÀ ADOZIONE: deliberazione di Giunta comunale

PERIODO ADOZIONE: dicembre 2023

REDAZIONE DOCUMENTO: Team DPO – Direzione Generale

Metodologia di redazione del modello organizzativo

Il presente documento costituisce il modello organizzativo del Comune di Rimini per la protezione dei dati personali, a cui tutti i dipendenti e collaboratori dello stesso fanno riferimento nel perseguimento delle finalità istituzionali dell'Ente, che si esplica nella progettazione e nello svolgimento di tutti i servizi ad esse connessi.

La realizzazione del presente modello organizzativo si basa sulla consapevolezza che il Regolamento UE 2016/679 (di seguito anche GDPR) ha introdotto un approccio multidisciplinare ai processi di trattamento dei dati personali finalizzato a favorire la loro libera circolazione nell'ambito della più ampia strategia europea sul governo dei dati, all'interno di un sistema che rispetti i diritti e le libertà fondamentali delle persone, a prescindere dalla loro nazionalità o dalla loro residenza. Non si tratta, dunque, di adottare misure di sicurezza sul dato, ma di analizzare l'intero trattamento nel quale si inserisce il ciclo di vita del dato personale e adottare misure tecniche ed organizzative che ne garantiscano la sicurezza.

Il presente modello organizzativo traduce nel contesto del Comune di Rimini i principi definiti dal GDPR, le previsioni fissate dal sistema normativo nazionale, nonché gli orientamenti in materia di privacy espressi da Authority ed Agenzie, nazionali ed europee.
Su di esso possono innestarsi ulteriori policy operative adottate dai Dirigenti delegati dal Sindaco, laddove si renda necessario un ulteriore livello di approfondimento in relazione alle attività a questi affidate, purché nel rispetto delle norme e del presente Modello Organizzativo.

> *Le misure indicate nel presente documento vengono adottate nella formazione, gestione, trasmissione, interscambio, accesso, conservazione e distruzione dei documenti cartacei e informatici contenenti dati personali, nonché nelle comunicazioni orali e scritte e nella gestione diretta o indiretta dei servizi, sia all'interno dell'Ente che nei rapporti con terzi*

Esso sostituisce e integra i precedenti provvedimenti assunti in materia dall'Ente, si inserisce nel sistema organizzativo dello stesso e ne rappresenta la specificazione rispetto ai provvedimenti generali assunti in merito ai comportamenti richiesti al personale.

Il modello organizzativo approvato con deliberazione di Giunta comunale n. 357 del 27 novembre 2018 conteneva una prima regolamentazione sulla materia della protezione dei dati personali, in adempimento alle previsioni del Regolamento UE 2016/679. Quel documento veniva elaborato all'inizio di un percorso di riorganizzazione dell'Ente, e rimandava ad una successiva e più puntuale disciplina della materia.

La presente versione viene redatta a seguito di tale percorso di riorganizzazione, che ha visto l'individuazione di un riferimento all'interno dell'organizzazione (il Coordinamento del Gruppo Privacy) e la costituzione di un gruppo di lavoro stabile, in continuo accrescimento e miglioramento, denominato 'Gruppo Privacy';
Il Coordinamento si è riunito con il Gruppo Privacy a partire dall'autunno 2019, compiendo diverse attività, tra cui, in particolare:

1. sono state messe a tema le maggiori criticità di carattere generale presenti nell'Ente in merito alla protezione dei dati personali;
2. sono state condotte specifiche interviste presso i singoli Servizi, con maggiore attenzione a quelli esposti a potenziali rischi per la protezione dei dati personali;
3. sono state analizzate specifiche casistiche e orientare le azioni di conformità;
4. sono stati messi a disposizione documenti di lavoro condivisi attraverso la intranet ed è stata creata una specifica sezione privacy sul sito istituzionale dell'Ente;
5. è stato progressivamente sensibilizzato tutto l'Ente, attraverso più momenti formativi durante l'anno, sfruttando anche le potenzialità della formazione in digitale, e attraverso la divulgazione di moduli di autovalutazione a Dirigenti ed EQ;
6. sono stati proposti 7 Tavoli tematici che hanno stimolato il confronto con il Coordinamento del Gruppo Privacy e che hanno avviato processi di fiducia e conoscenza nei confronti della materia;
7. è stata strutturata una maggiore interlocuzione e collaborazione con il DPO nell'affronto delle specifiche problematiche;
8. sono stati introdotti specifici obiettivi all'interno dei documenti programmatici dell'Ente;

Il presente Modello organizzativo in materia di dati personali sorge, dunque, dall'analisi di contesto del Comune di Rimini e contiene gli strumenti atti ad uniformare l'impostazione by design di tutta l'attività dell'Ente, e a favorire l'operatività di ciascun Dirigente, titolare di Posizione Organizzativa, dipendente o collaboratore

Gli strumenti contenuti nel presente documento sono ispirati al principio di *accountability* che permea la struttura del GDPR, per garantire il tracciamento del flusso dei dati. A tal proposito, ciascun Dirigente può definire eventuali ulteriori misure utili alla protezione dei dati nello svolgimento del Servizio cui viene delegato.

Il documento è suddiviso nelle 8 macro categorie ritenute più rilevanti e funzionali all'elaborazione di un modello condiviso all'interno dell'Ente, è composto da diversi allegati che ne formano parte integrante ed è funzionalmente legato ad altri atti e documenti approvati dall'Amministrazione per garantire la più efficace e trasparente azione amministrativa del complesso organizzativo. Non tutti i documenti attuativi del Modello Organizzativo vengono approvati contestualmente ad esso, poiché si ritiene di renderli strumenti di lavoro flessibili e dinamici in relazione all'evoluzione della materia. Su di essi vengono condotte specifiche istruttorie trasversali con i Dirigenti delegati coinvolti.
Tutto il materiale relativo alla conformità dell'Ente al GDPR è presente

- per le informazioni ad uso dei dipendenti del Comune di Rimini: sullo strumento digitale di informazione interna dell'Ente
- per le informazioni rivolte ai terzi: sul sito web istituzionale dell'Ente

E' prevista un'istruttoria di revisione del presente testo ogni 24 mesi dall'adozione dello stesso, salvo sopraggiunti interventi normativi o diversi orientamenti organizzativi dell'Ente.

Gli orientamenti interpretativi relativi al GDPR sono visibili alle pagine del Garante Privacy italiano https://www.garanteprivacy.it e del Garante Europeo https://edps.europa.eu.

Comune di Rimini

DISCIPLINA

1.1 CONTESTO NORMATIVO DI RIFERIMENTO E GLOSSARIO

La protezione delle persone fisiche, con riguardo al trattamento di dati personali, viene riconosciuto come diritto fondamentale dell'individuo, collegato direttamente alla tutela della dignità umana dalla Carta dei diritti fondamentali dell'Unione Europea.

Il Regolamento UE 2016/679 (General Data Protection Regulation – GDPR) nasce dalla consapevolezza del forte impatto degli sviluppi tecnologici sul trattamento dei dati personali, e del fatto che i nuovi modelli di crescita economica hanno eletto il dato, anche personale, tra le principali monete di scambio del terzo millennio.

Nell'ambito della più ampia strategia sul governo europeo dei dati, che vorrebbe condurre alla sovranità digitale dell'Unione Europea, il GDPR si presenta come un sistema flessibile in grado di rilevare le esigenze di ciascuna realtà organizzativa, tutte raccordate dai generali principi espressi nel Regolamento stesso.

Il GDPR stesso ricorda, tuttavia, che il diritto alla riservatezza dei propri dati peronali non è prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato agli altri diritti fondamentali.

Diversamente dalla previgente disciplina, la protezione dei dati personali non è più oggetto di previsioni puntuali su specifiche casistiche, ma si commisura in base ai principi di liceità, correttezza e trasparenza, e al principio di accountability del soggetto che tratta i dati personali, a cui consegue l'adozione di forme di gestione flessibili e sartoriali per ciascuna organizzazione.

La predeterminazione di principi generali ha permesso di elaborare un sistema in grado di uniformare il più possibile la disciplina della *privacy* di ciascun individuo all'interno dei singoli Stati Membri, sia in relazione a soggetti privati sia in relazione a quelli pubblici, generando un movimento unitario sulla tematica.
Il Regolamento lascia spazio all'azione del legislatore nazionale, che in Italia è intervenuto con la modifica del d.lgs. n. 196/2003, Codice in materia di protezione dei dati personali, ad opera del d.lgs. n. 101/2018, in merito alla specificazione di alcune tematiche ritenute di interesse generale.

Nello svolgimento della propria attività, il Comune di Rimini si relaziona anche con le forze dell'ordine, legittimate al trattamento dei dati personali in base ai casi e alle modalità previste dalla Direttiva 2016/680, recepita in Italia con d.lgs. n. 51/2018, che disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.

L'infografica presente in questa pagina, elaborata dal Garante per la protezione dei dati personali italiano, evidenzia gli elementi fondamentali su cui il Regolamento pone l'attenzione:

- garantire una chiara informazione a coloro dei cui dati personali si tratta;
- ripensare i processi interni;
- oltrepassare l'impostazione meramente adempimentale della protezione dei dati personali.

La regolamentazione europea lascia, ad ogni modo, impregiudicate le disposizioni degli accordi internazionali in materia, comprese adeguate garanzie per gli Interessati al trattamento dei propri dati personali.

Il presente documento è costruito secondo i principi del GDPR, e fa altresì riferimento agli interventi di *soft law*, nazionali ed europei, nonchè internazionali.

Nell'affronto di questi delicati compiti, il Comune di Rimini si avvale di un Responsabile esterno della protezione dei dati personali (RPD/DPO), i cui riferimenti sono presenti sul sito istituzionale dell'Ente alla sezione 'privacy', e vengono puntualmente comunicati al Garante Privacy in caso di cambiamento.

GLOSSARIO GENERALE

TERMINI	DEFINIZIONI
DATO PERSONALE	Si fa riferimento a qualsiasi informazione riguardante una persona fisica identificata o identificabile, qualificata come Interessato. **Quando si considera identificabile una persona fisica?** Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale **Esempi** Sono ricompresi nella definizione, a titolo di esempio, data di nascita, indirizzo di residenza o domicilio, codice fiscale, numeri di telefono, posta elettronica, indirizzo IP, dati di log, video, audio, immagini, dati di geolocalizzazione, IBAN, stato di disagio economico, contributi economici, agevolazioni tributarie/tariffarie e simili, abusi/accertamenti edilizi, permessi a costruire.
DATI PARTICOLARI	**Si intendono i dati personali che rivelino:** - l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati biometrici intesi a identificare in modo univoco una persona fisica; - dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona: gestione dei servizi e sistemi di assistenza sanitaria o sociale, per garantire la continuità degli stessi o per finalità di sicurezza sanitaria, controllo e allerta o fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici in base al diritto dell'Unione o nazionale. Il trattamento di categorie particolari di dati personali può essere necessario per motivi di interesse pubblico nei settori della sanità pubblica, senza il consenso dell'interessato. **Note su dati biometrici:** Si fa riferimento ai dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici

	Note su dati relativi alla salute: Più in generale i dati relativi alla salute possono riguardare tutti gli elementi relativi alla salute, ossia lo stato di salute, morbilità e disabilità incluse, i determinanti aventi un effetto su tale stato di salute, le necessità in materia di assistenza sanitaria, le risorse destinate all'assistenza sanitaria, la prestazione di assistenza sanitaria e l'accesso universale a essa, la spesa sanitaria e il relativo finanziamento e le cause di mortalità. All'interno di essi si trovano anche i dati genetici, ovvero quelli relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione. Tale trattamento viene assoggettato a misure appropriate e specifiche a tutela dei diritti e delle libertà delle persone fisiche.
DATI RELATIVI AI MINORI	Ci si riferisce ai dati personali di soggetti minori degli anni 18, il cui trattamento deve essere autorizzato dai titolari della responsabilità genitoriale. **Disciplina italiana:** In relazione ai servizi della società dell'informazione, ossia quei servizi forniti a distanza per via elettronica o a richiesta individuale, il minore che abbia compiuto almeno 14 anni può esprimere direttamente il proprio consenso.
DATI RIGUARDANTI LE PERSONE DECEDUTE	Nonostante il GDPR indichi al considerando n. 27 una generale disapplicazione del regolamento ai dati delle persone decedute, prevede che gli stessi possano essere disciplinati da ciascun singolo stato membro. **Disciplina italiana:** La normativa italiana vigente trova applicazione e disciplina i diritti riguardanti le persone decedute, nei termini di accessibilità, e più in generale per l'esercizio dei diritti da parte di chi, ha un interesse proprio, a tutela dell'interessato, in qualità di suo mandatario o per ragioni meritevoli di protezione. Non si applica invece l'esercizio di alcuni dei diritti nell'ambito dei servizi della società dell'informazione qualora il soggetto interessato abbia espressamente vietato con dichiarazione scritta al titolare del trattamento. In ogni caso tale divieto non può produrre effetti pregiudizievoli per l'esercizio dei terzi, fra cui i diritti patrimoniali che derivano dal decesso dell'interessato, nonché dal diritto di difesa.
DATI RELATIVI A CONDANNE PENALI E REATI	Si fa riferimento ai dati c.d. giudiziari, cioè i dati che possono rilevare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale, connessi anche a misure di sicurezza o rilevanti la qualità di imputato o di indagato. Essi possono essere trattati solo sotto il controllo dell'autorità pubblica o ove sia previsto per legge.
DATI SUPER	Sono considerate particolarmente delicate alcune informazioni

SENSIBILI	riguardanti i soggetti interessati tutelati da leggi speciali, ed in particolare: sieropositivi o affetti da infezione da Hiv legge 5 giugno 1990, n. 135, interruzione di gravidanza legge 22 maggio 1978, n. 194 e riguardo a persone offese da atti di violenza sessuale art. 734-bis del codice penale. Per tali dati occorre porre una particolare attenzione sia nel trattamento stesso, che nella conservazione, che nell'eventuale richiesta di accesso, nonché nella definizione dei rapporti con affidatari esterni.

GLOSSARIO DI CONTESTO

TERMINI	DEFINIZIONI
BASE GIURIDICA	Consiste nel presupposto legittimante di un trattamento, che è considerato meritevole di tutela rispetto al diritto alla protezione dei dati personali. **Basi giuridiche per il trattamento di dati comuni** Art. 6 del Regolamento UE 2016/679 **Basi giuridiche per il trattamento di dati particolari** Art. 9 del Regolamento UE 2016/679 **Basi giuridiche per il trattamento di dati relativi a condanne penali e reati** Art. 10 del Regolamento UE 2016/679 **Note:** Ulteriori specifiche sulle basi giuridiche sono contenute agli artt. 2-ter e ss. Del D.Lgs. 196/2003
PROFILAZIONE	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica.
TRATTAMENTO	Si considera trattamento qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. come **Attività di trattamento di cui al GDPR:** la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

TRATTAMENTO DI DATI SU LARGA SCALA	Il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala". **Elementi da considerare per l'individuazione della larga scala:** a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; c. la durata, ovvero la persistenza, dell'attività di trattamento; d. la portata geografica dell'attività di trattamento;
TRASFERIMENTO DEI DATI IN PAESI EXTRA UE	Per trasferimento dei dati in Paesi Extra UE si intende il trasferimento dei dati da un soggetto c.d. "esportatore" verso un soggetto c.d. "Importatore". **Note:** Anche il solo accesso da parte di un soggetto ubicato in un Paese Extra UE rientra nella definizione di "trasferimento dati in Paesi Extra UE", pertanto il soggetto esportatore è tenuto all'adozione di misure di garanzia adeguate per tale trasferimento.
TRATTAMENTO TRANSFRONTALIERO	**Si configurano due fattispecie di trattamento transfrontaliero:** **a)** trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; **b)** trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.
ARCHIVIO	Qualsiasi insieme strutturato di dati personali accessibile secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico

VIOLAZIONE DEI DATI PERSONALI	Per violazione dei dati personali si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.
ACCORDO DI FRUIBILITÀ	Accordo per la fruibilità telematica delle banche dati del Comune di Rimini da parte di altre Pubbliche Amministrazioni o di soggetti privati qualificati (es. Gestori di pubblici servizi), identificati da norma di legge o di regolamento nazionali e comunitari, nonché identificati dal Comune in ragione dello svolgimento delle proprie funzioni di interesse pubblico perseguito.
INFORMATIVA	L'informativa è l'insieme di tutte le informazioni, previste dagli articoli 13 e 14 del GDPR, con cui il Titolare comunica prevalentemente all'Interessato le finalità, le modalità del trattamento e di esercizio dei diritti.
CONSENSO	Si tratta di qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'Interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.
TITOLARE DEL TRATTAMENTO	Si tratta della persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.
CONTITOLARE DEL TRATTAMENTO	Si considerano contitolari due o più titolari del trattamento che determinano congiuntamente le finalità e i mezzi del trattamento. **Note:** I Contitolari determinano le rispettive responsabilità mediante apposito accordo in merito all'osservanza degli obblighi derivanti dal GDPR, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14 del GDPR.
RESPONSABILE DEL TRATTAMENTO	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento, secondo quanto definito in appositi accordi.
SUB-RESPONSABILE DEL TRATTAMENTO	Il sub-responsabile del trattamento viene identificato in colui al quale il responsabile del trattamento ricorre per l'esecuzione di

	specifiche attività di trattamento svolte per conto del titolare del trattamento. **Note:** La legittimità al sub Responsabile deriva da previa autorizzazione scritta, specifica o generale, del Titolare del trattamento, e mediante un accordo è sottoposto ai medesimi obblighi in materia di protezione dei dati contenuti nell'accordo tra il Titolare del trattamento e il Responsabile del trattamento.
RESPONSABILE DELLA PROTEZIONE DEI DATI (DI SEGUITO ANCHE RDP/DPO)	La persona fisica o giuridica individuata come Responsabile della protezione dei dati personali ai sensi del GDPR (artt. 37, 38, 39 del Regolamento).
INTERESSATO AL TRATTAMENTO	L'Interessato al trattamento viene identificato nella persona fisica a cui si riferiscono i dati trattati.
DESTINATARIO DEL TRATTAMENTO	Si considera destinatario la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.
REFERENTE GDPR	Il Dirigente preposto alle attività di coordinamento relativamente alla protezione dei dati personali.
DIRIGENTE DESIGNATO	Il Dirigente designato è colui che viene designato dal Titolare del trattamento allo svolgimento di compiti e funzioni connesse al trattamento dei dati personali in relazione al Servizio affidatogli.
AUTORIZZATO AL TRATTAMENTO	La persona fisica, espressamente individuata dal Dirigente, che opera sotto l'autorità del titolare del trattamento, con specifici compiti e funzioni connessi al trattamento dei dati personali. In tale figura rientrano anche i dipendenti titolari di Posizione Organizzativa, ai quali vengono assegnati specifici compiti e funzioni nell'ambito del perimetro di operatività della PO stessa.
GRUPPO PRIVACY	Gruppo permanente di dipendenti che supporta i Dirigenti negli adempimenti continuativi, nello studio e nell'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti delle disposizioni normative in materia di protezione dei dati personali. Tra essi vengono indicate una o più persone che fungano da coordinamento delle attività e che mantengano un rapporto costante con il DPO.

AMMINISTRATORE DI SISTEMA	Con la definizione di amministratore di sistema (nel testo anche ADS) si individuano, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. NB Riveste il ruolo di Amministratore di sistema il soggetto che per mansione o incarico svolge un'attività preordinata alla gestione o manutenzione di un sistema di elaborazione dati, ovvero preposta alla gestione e alla manutenzione di risorse, apparati e infrastrutture del sistema informatico dell'Ente, che per lo svolgimento di tali mansioni dispone della concreta possibilità di accedere a dati personali ulteriori rispetto a quelli a cui sono legittimati gli incaricati del trattamento.
ITBREACH	La struttura tecnica a cui è demandata la gestione degli incidenti di sicurezza in ambito ICT. Tale struttura si avvale della collaborazione dei membri del team RTD che possano collaborare per competenza alla gestione dell'incidente e allo svolgimento delle azioni necessarie alla risoluzione dello stesso.
GARANTE DELLA PROTEZIONE DEI DATI PERSONALI (DI SEGUITO ANCHE GARANTE PRIVACY)	Autorità amministrativa indipendente istituita dalla legge 31 dicembre 1996, n. 675, designata anche ai fini dell'attuazione del Regolamento (UE) 2016/679.
EUROPEAN DATA PROTECTION SUPERVISOR - GARANTE EUROPEO DELLA PROTEZIONE DEI DATI (DI SEGUITO ANCHE EDPS/GEPD)	Autorità istituita per garantire che le istituzioni e gli organi dell'UE rispettino il diritto dei cittadini al trattamento riservato dei dati personali
EUROPEAN DATA PROTECTION BOARD – COMITATO EUROPEO PER LA PROTEZIONE DEI DATI (EDPB)	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.
EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA)	Si tratta dell'Agenzia europea per la cybersicurezza dedicata allo studio e alla definizione di policy sulla sicurezza informatica per tutti i soggetti, pubblici e privati, appartenenti all'Unione Europea.

AGENZIA PER L'ITALIA DIGITALE (AGID)	L'Agenzia per l'Italia Digitale è l'agenzia tecnica della Presidenza del Consiglio che ha il compito di garantire la realizzazione degli obiettivi dell'Agenda digitale italiana e contribuire alla diffusione dell'utilizzo delle tecnologie dell'informazione e della comunicazione, favorendo l'innovazione e la crescita economica. **Note:** AgID ha, inoltre, il compito di coordinare le amministrazioni nel percorso di attuazione del Piano Triennale per l'informatica della Pubblica amministrazione, favorendo la trasformazione digitale del Paese.
AGENZIA PER LA CYBERSICUREZZA NAZIONALE	L'Agenzia tutela gli interessi nazionali nel campo della cybersicurezza e assicura il coordinamento tra i soggetti pubblici coinvolti nella materia.

1.2 I PRINCIPI DEL GDPR E L'IMPOSTAZIONE PREDEFINITA

All'interno di ogni processo di lavoro
potrebbe essere presente un trattamento di dati personali

ACCOUNTABILITY

Il principio di accountability rappresenta uno dei pilastri su cui si fonda il Regolamento UE 2016/679. In italiano il termine è stato tradotto come "responsabilizzazione" e prende in esame diversi aspetti quali l'affidabilità e la competenza di un'Organizzazione nel gestire il proprio patrimonio informativo. I dati sono trattati sotto la responsabilità del titolare del trattamento **che assicura e comprova**, per ciascuna operazione, la conformità alle disposizioni del Regolamento.

Prima di iniziare un trattamento dati, e in fase di revisione dello stesso, ciascun Dirigente delegato applica il principio di privacy by design e di privacy by default e ne dà evidenza tramite compilazione, protocollazione e conservazione di apposita istruttoria.

Il Regolamento UE 2016/679, all'art. 25, individua due elementi essenziali su cui si devono basare i sistemi di protezione dei dati personali, tenendo conto dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche:

Impostazione *by design* secondo cui il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate alla protezione dei dati in fase di determinazione dei mezzi del trattamento.
Impostazione *by default* secondo cui il Titolare del trattamento deve mettere in atto misure tecniche e organizzative adeguate alla protezione dei dati all'atto del trattamento stesso.

PROGETTAZIONE DI UN NUOVO TRATTAMENTO DATI

È necessaria l'effettuazione di una analisi prima di implementare un nuovo strumento che consente il trattamento di dati personali, ad esempio per:

- Nuovo sito internet
- Una nuova APP per gestire le timbrature delle presenze dei dipendenti

Elementi oggetto di analisi in fase di progettazione di un nuovo trattamento dati:

- ✓ Stato dell'arte
- ✓ Costi di attuazione
- ✓ Natura, Ambito di applicazione, Contesto
- ✓ Finalità del trattamento e basi giuridiche
- ✓ Strumenti utilizzati per il trattamento
- ✓ Responsabili esterni eventualmente coinvolti
- ✓ Incaricati
- ✓ Formazione
- ✓ Rischi (probabilità e gravità) per i diritti e le libertà delle persone costituiti dal trattamento
- ✓ Misure di sicurezza tecniche ed organizzative
- ✓ Minimizzazione in relazione a
  - quantità di dati personali raccolti
  - la portata del trattamento
  - il periodo di conservazione e l'accessibilità dei dati

Dall'analisi svolta derivano:

- → le informazioni per adottare le misure tecniche
- → le informazioni per adottare le misure organizzative
- → le informazioni da inserire nel registro dei trattamenti secondo le modalità previste dalla specifica procedura parte integrante del presente modello organizzativo, ancorché adottata successivamente allo stesso
- → le informazioni necessarie a svolgere la valutazione del rischio
- → le informazioni necessarie a svolgere l'eventuale valutazione di impatto (DPIA)

Per misure di sicurezza tecniche si intende:

- tutti quegli strumenti e metodi che consentano di garantire un livello di sicurezza adeguato al rischio in relazione ai dati trattati, tra cui adeguata conservazione e protezione dei dati da eventuali violazioni.

Per misure di sicurezza organizzative si intende:

- gli adempimenti, attività, metodi che consentano la liceità del trattamento di dati personali.

Sia in fase di progettazione che in fase di trattamento vanno considerati i principi di cui all'art. 5 GDPR, che la Commissione Europea interpreta come di seguito:

Liceità, correttezza e trasparenza	I dati personali devono essere trattati in modo lecito e trasparente, garantendo l'equità nei confronti delle persone di cui si trattano i dati.
Limitazione della finalità	Devono sussistere finalità specifiche per il trattamento dei dati e l'organizzazione deve indicarle alle persone quando si raccolgono i loro dati personali. Un'organizzazione non può raccogliere dati personali per scopi non definiti.
Minimizzazione dei dati	L'organizzazione può raccogliere e trattare solo i dati personali necessari alle specifiche finalità individuate. Tra le modalità di minimizzazione rientra la pseudonimizzazione, ovvero il trattamento dei dati personali in modo tale che essi non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.
Esattezza	L'organizzazione deve assicurarsi che i dati personali siano esatti e aggiornati, tenendo conto delle finalità per le quali vengono trattati, e, in caso contrario, correggerli.
Limitazione della conservazione	L'organizzazione non può utilizzare i dati personali per altri scopi non compatibili con la finalità originaria della raccolta e deve

garantire che i dati personali siano conservati per un periodo non superiore a quello necessario agli scopi per i quali sono stati raccolti.

Integrità e riservatezza

L'organizzazione deve predisporre adeguate misure tecniche e organizzative che garantiscano la sicurezza dei dati personali, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita accidentale, la distruzione o il danno, utilizzando tecnologie appropriate.

1.3 La base giuridica quale liceità del trattamento

Il trattamento di dati personali avviene
solo laddove sia necessario
in base a determinati casi di liceità
stabiliti dagli artt. 6 e 9 del Regolamento (UE) 2016/679

In virtù del quadro regolatorio, e in relazione al trattamento dati concreto, il primo adempimento del Dirigente è quello di valutare la base di liceità del trattamento

Le basi giuridiche più ricorrenti nella Pubblica Amministrazione vengono indicate di seguito.

1.3.1.Obbligo legale

Norma: Art. 6, par. 1, lett. c), GDPR

La base giuridica dell'obbligo legale deve soddisfare quattro condizioni:

1. essere definito dalla legge europea o nazionale di uno Stato membro a cui è soggetto il titolare del trattamento;
2. tali disposizioni legali devono stabilire un obbligo imperativo di trattamento dei dati personali, sufficientemente chiaro e preciso;
3. tali disposizioni devono almeno definire le finalità del trattamento in questione;
4. tale obbligo deve essere imposto al titolare del trattamento e non alle persone interessate dal trattamento

1.3.2. Compito di interesse pubblico

Norma: Art. 6, par. 1, lett. e), GDPR

La base giuridica del compito di interesse pubblico costituisce la base legale più ricorrente nell'azione della Pubblica Amministrazione.

1.3.3 Dati particolari

Norma: Art. 9 GDPR

Per il trattamento dei dati particolari di cui all'art. 9, la cui definizione è richiamata in premessa, il Comune di Rimini si adegua al generale divieto di trattare tali categorie di dati personali.

- Il GDPR prevede il trattamento di tali dati in determinati casi, la cui applicabilità è da valutarsi per ciascun trattamento, in base a quanto stabilito dal medesimo articolo 9 GDPR

Trattamento di dati particolari nell'ambito dei compiti di interesse pubblico

Norma: Art. 9, par.2, lettera g), GDPR

Art. 2 sexies, D.Lgs. 196/2003

- In relazione all' art. 9, par.2, lettera g) del GDPR, l'art. 2 sexies del D.Lgs. 196/2003 indica le materie che rientrano nel rilevante interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri.

- In relazione al trattamento dei dati biometrici e relativi alla salute il Comune di Rimini si attiene alle misure di garanzia così come definito nell'art. 2 septies del D.Lgs. 106/2003 che alle prescrizioni relative al trattamento di categorie particolari di dati definite dal Garante Privacy.

Comune di Rimini

RUOLI

2.1 AMBITO SOGGETTIVO DI APPLICAZIONE DEL MODELLO E ORGANIZZAZIONE DELL'ENTE

Il presente Modello trova applicazione ai medesimi soggetti cui si applica il Codice di Comportamento adottato dall'Ente, ovvero:

DIPENDENTI del Comune di Rimini assunti con contratto di lavoro a tempo indeterminato;

DIPENDENTI E COLLABORATORI assunti mediante le forme contrattuali flessibili di cui agli articoli 36 e 7, commi 6 e seguenti del decreto legislativo 30 marzo 2001, n. 165;

PERSONALE DIPENDENTE AD ALTRI ENTI che presta servizio presso il Comune di Rimini attraverso gli istituti del comando o del distacco o attraverso le convenzioni di cui all'articolo 14 del CCNL per il personale dipendente di Regioni e Autonomie locali stipulato in data 22 gennaio 2004. 2;

TUTTI I SOGGETTI A TEMPO DETERMINATO che prestano attività lavorativa ai sensi dell'articolo 90 e 110 del Testo unico delle Leggi sull'Ordinamento degli Enti locali approvato con decreto legislativo 18 agosto 2000, n. 267;

TUTTI I COLLABORATORI E CONSULENTI che prestano la propria attività professionale in favore del Comune di Rimini sulla base di qualsiasi tipologia di contratto o incarico ed a qualsiasi titolo.

- Nei contratti aventi ad oggetto il conferimento a soggetti estranei all'Ente dei predetti incarichi di collaborazione o consulenza, comunque denominati, vengono inserite apposite clausole che stabiliscono la risoluzione o la decadenza del rapporto negoziale in caso di violazione degli obblighi derivanti dalle norme a protezione dei dati personali e dal presente Modello.

- Ai dipendenti e ai collaboratori a qualsiasi titolo delle Società strumentali del Comune di Rimini, che risultino titolari di affidamenti di servizi, lavori e forniture attraverso l'istituto dell'in house providing, si applica il presente Modello secondo gli accordi sottoscritti ai sensi dell'art. 28 GDPR

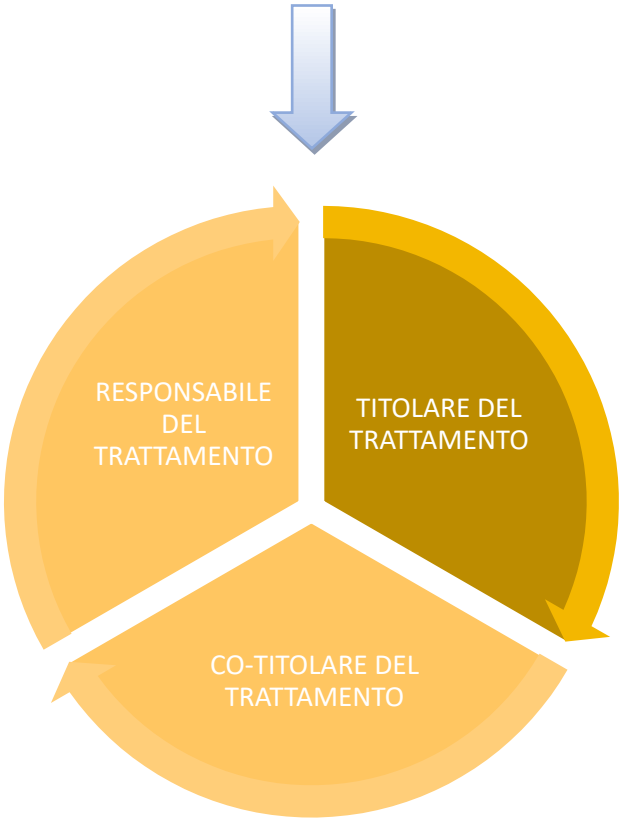
.

2.2 Organigramma e funzioni GDPR del Comune di Rimini

RUOLO	FUNZIONE
Il Sindaco	Rappresenta il Comune di Rimini quale Titolare del trattamento di dati personali
Il Segretario Generale	
I Dirigenti	Sono delegati dal Sindaco a svolgere le funzioni in capo al titolare del trattamento rispettivamente al settore assegnato. Assegnano compiti e funzioni ai titolari di posizione organizzativa (P.O.) in merito allo svolgimento degli adempimenti privacy relativi al perimetro di operatività della posizione organizzativa possono nominare dipendenti e collaboratori quali incaricati del trattamento dei dati personali, inoltre indicano gli Amministratori di Sistema e i referenti del Gruppo Privacy
Il Dirigente che presiede le funzioni dei sistemi informatvi	Nomina gli Amministratori di Sistema indicati dai Dirigenti
I referenti del Gruppo Privacy	Partecipano alle attività del Gruppo Privacy e supportano i Dirigenti nei processi di integrazione della disciplina GDPR all'interno delle proprie strutture di riferimento
Gli Amministratori di Sistema	Presidiano specifici sistemi informatici entro i quali avvengono trattamenti di dati personali, sia nell'ambito delle proprie strutture di riferimento sia in relazione ad altre strutture dell'Ente
Il Responsabile della Protezione Dati	Informa e fornisce consulenza al Titolare del trattamento, sorvegliando l'osservanza della normativa in materia di protezione dei dati personali e fornendo i pareri necessari per il corretto adempimento degli obblighi da questa derivante

2.3 Ruoli interni ed esterni al Comune di Rimini

Che ruolo svolge il Comune di Rimini
nel trattamento dei dati personali degli interessati?



Di seguito vengono identificati i diversi ruoli disciplinati dal GDPR, con l'indicazione specifica di quelli che può assumere il Comune di Rimini nell'ambito dei rapporti con i soggetti sopra considerati.

2.3.1 Il Titolare del trattamento dei dati personali

Il titolare del trattamento
è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che,
singolarmente o insieme ad altri,
determina le finalità e i mezzi del trattamento di dati personali

Il Comune di Rimini

È titolare in tutti i casi stabiliti dalla legge o in tutti i casi in cui determini le finalità e i mezzi del trattamento di dati personali

Quando le finalità e i mezzi di tale trattamento sono determinati da norme di legge nazionale o sovranazionale, il titolare del trattamento, o i criteri specifici applicabili alla sua designazione, possono essere stabiliti dalle norme medesime.

Al fine di individuare correttamente il Titolare del trattamento è possibile porsi alcune domande in grado di favorire una riflessione integrale sul tema e di orientare la decisione del Dirigente delegato.

QUESITI
Chi stabilisce quali devono essere gli elementi essenziali del trattamento per rispondere ai principi di accountability, privacy by design e by default?
Chi determina le finalità e i mezzi del trattamento?
I soggetti che materialmente effettueranno le operazioni di trattamento sui dati agiscono sotto l'autorità diretta dell'Ente?
L'Ente è dotato di autonomia e indipendenza rispetto alle modalità di trattamento dei dati personali o agisce per conto di soggetti distinti?

OBBLIGHI DEL TITOLARE

Il Titolare del Trattamento è sottoposto a molteplici obblighi derivanti dalla legislazione in materia di protezione dei dati personali, tra i quali, *a titolo esemplificativo e non esaustivo*, si elencano:

- Adottare misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR e che le misure sono elaborate tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento
- Tenere e aggiornare il Registro dei trattamenti, e tutti i registri che ritenga di adottare
- Predisporre un'informativa da fornire ai soggetti interessati dai trattamenti riportati nel Registro dei trattamenti
- Predisporre un'informativa da fornire ai dipendenti dell'ente in relazione al loro trattamento dei dati nello svolgimento degli adempimenti di legge in tema di gestione del rapporto di lavoro
- Nominare Responsabile del trattamento unicamente i soggetti che presentino garanzie sufficienti e adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato
- Verificare l'effettivo possesso, e il relativo mantenimento, dei requisiti richiesti al Responsabile del Trattamento
- Fornire precise, espresse e documentate istruzioni relative al trattamento dei dati al Responsabile del trattamento ed, eventualmente, richiedere tutte le informazioni ritenute necessarie per dimostrarne il rispetto, anche tramite ispezioni
- Aderire ad accordi di fruibilità dei dati (art. 50 d.lgs. n. 82/2005 – CAD) per agevolare l'acquisizione dei dati e ottimizzare le risorse
- Individuare i soggetti interni che trattano dati personali sulla base dello specifico settore di appartenenza e qualificarli con atto di designazione come incaricati del trattamento: tale atto deve contenere le istruzioni e le prassi cui è richiesto di attenersi, al fine di delineare l'area di legittima e sicura operatività del dipendente
- Nominare gli Amministratori di Sistema (ADS)
- Riesaminare periodicamente le misure e aggiornarle in caso di modifiche della procedura e del trattamento

2.3.2 Personale dirigente

Al personale dirigente sono affidati tutti gli adempimenti necessari e conseguenti all'attuazione delle norme in materia di protezione dei dati, in coerenza con la previsione dell'art. 107 del D.Lgs. 267/2000

NOMINA DEI DIRIGENTI
I Dirigenti sono nominati dal Sindaco con atto di incarico delle funzioni amministrative

COMPITI E FUNZIONI ASSEGNATI AI DIRIGENTI	
a)	Verificare la legittimità dei trattamenti di dati personali effettuati dalla struttura di competenza
b)	Mappare ed aggiornare costantemente i trattamenti e definire soluzioni *by design e by default* per nuovi trattamenti e per la revisione di quelli già in essere
c)	Adottare misure di protezione a livello logico e a livello informatico delle dotazioni del proprio Servizio, e modalità di gestione dei *data breach* all'interno del proprio Servizio
d)	Applicare le policy adottate dall'Ente in relazione alla gestione del personale, anche in modalità agile
e)	Garantire la gestione delle richieste di esercizio dei diritti degli Interessati nell'ambito proprio Servizio
f)	Implementare e aggiornare costantemente il *Registro delle attività di trattamento* per il Servizio di competenza
g)	Individuare i soggetti interni all'Ente autorizzati a compiere operazioni di trattamento, sovrintendendo e vigilando sull'attuazione delle istruzioni impartite
h)	Identificare uno o più Referenti del Gruppo Privacy e garantendone l'operatività, e la collaborazione con gli altri Servizi dell'Ente, con il Referente GDPR e con il Team del DPO
i)	Designare gli Amministratori di sistema (ADS) e presentare tale designazione al Referente GDPR per la successiva nomina
l)	Predisporre le informative relative agli specifici trattamenti di dati personali condotti nel proprio Servizio, nel rispetto degli articoli 13 e 14 del Regolamento, sulla base dei format messi a disposizione dal Referente GDPR dell'Ente, e conformemente a quanto descritto nel registro dei trattamenti
m)	Verificare periodicamente che i trattamenti eventualmente svolti in base all'acquisizione di consenso dell'Interessato siano legittimi
n)	Inserire, nei contratti di sviluppo di software e piattaforme l'esplicita indicazione di conformità al GDPR del fornitore, nonché l'eventuale presenza di una certificazione ex art. 42 GDPR, disponendo che il mancato rispetto dei requisiti ivi previsti equivale a grave inadempimento, con facoltà per l'Ente di risoluzione del

	contratto. La bozza di contratto viene condivisa con l'RTD e il DPO per la verifica delle soluzioni tecnologiche conformi al GDPR, ed eventualmente con il Referente GDPR
o)	Designare i Responsabili del trattamento sulla base dei format messi a disposizione dal Referente GDPR dell'Ente
p)	Adottare specifici accordi di fruibilità con altre PA e gestori di pubblici servizi per garantire la fruibilità dei dati personali di cui l'Ente è Titolare
q)	Adeguare i processi ai provvedimenti adottati dal Garante per la privacy in relazione al Servizio di competenza
r)	Svolgere una preventiva valutazione dei rischi presenti nei processi del Servizio delegatogli, con eventuale valutazione d'impatto sui trattamenti (DPIA) nei casi di cui all'art. 35 del Regolamento UE 2016/679
s)	Proporre al Referente GDPR la consultazione al Garante della Privacy, ai sensi dell'art. 36 del Regolamento, nei casi in cui la valutazione d'impatto indichi che il trattamento presenta un rischio residuale elevato
t)	Assicurare che il RPD/DPO sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali, fornendogli le risorse necessarie per i compiti assegnategli dal GDPR
u)	Garantire al Referente GDPR e al RPD/DPO i necessari permessi di accesso ai dati ed ai sistemi informativi per l'effettuazione delle verifiche di sicurezza, anche a seguito di incidenti di sicurezza

2.3.3 Struttura competente in materia di sistemi informativi

La struttura è tenuta a mettere in atto tutte le misure adeguate, tecniche ed organizzative, per garantire la sicurezza informatica nei termini previsti dalle norme in materia, predisponendo, nel rispetto dei principi di accountability, evidenze documentali circa le azioni intraprese, le attività svolte e le caratteristiche dei sistemi, da esibire in caso di eventuali attività ispettive da parte degli organi competenti o di sorveglianza sulla conformità al GDPR da parte del RPD/DPO

ATTIVITÀ DELEGATE

- Individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente
- Sottopone a parere preventivo del RPD/DPO tutte le soluzioni che abbiano un significativo impatto sulla protezione dei dati personali, laddove i singoli Dirigenti non abbiano presentato adeguata documentazione in fase di scelta della soluzione
- In caso di problemi di sicurezza provvede a:
  - attivare la struttura cui sono demandati compiti relativi alla gestione degli incidenti di sicurezza
  - consultare tempestivamente il RPD/DPO ai fini della valutazione e dell'eventuale notifica all'Autorità Garante
- Individua misure idonee al miglioramento della sicurezza dei trattamenti dei dati personali, previo parere del RPD/DPO

2.3.4 Il Referente GDPR

Il Dirigente cui vengono delegate le funzioni relative alle attività GDPR di tutto il Comune agisce quale Referente GDPR dell'Ente.

2.3.5 Titolari di incarico di Elevata Qualificazione

Sulla base del vigente assetto organizzativo dell'Ente, i titolari di incarico di elevata qualificazione:

- sono nominati dal Dirigente in adempimento allo schema organizzativo generale definito dalla Giunta comunale
- agiscono secondo le istruzioni definite nel provvedimento di nomina
- sono affidati tutti gli adempimenti necessari e conseguenti alle funzioni conferite dal Dirigente

2.3.6 Gruppo Privacy

Allo scopo di operare in maniera univoca, quale unico Titolare del trattamento dei dati personali, pur in presenza di un elevato numero di uffici, **il Comune di Rimini istituisce un gruppo permanente di dipendenti** che supporti i Dirigenti delegati nel definire gli adempimenti continuativi, nello studio e l'approfondimento degli aspetti normativi, organizzativi e procedurali, derivanti dalle disposizioni in materia di protezione dei dati personali.

COMPONENTI	
1	Uno o più dipendenti del Referente GDPR dell'Ente
2	Un dipendente dell'ufficio Segreteria Generale incaricato della gestione dell'accesso civico
3	Un numero variabile di dipendenti per ciascun Settore, selezionati dal Dirigente delegato di riferimento in base alle peculiarità di ciascun servizio
4	Il Responsabile della gestione documentale dell'Ente

Ciascun membro del Gruppo Privacy:

- è individuato dal Dirigente del Settore cui afferisce.

A seguito della nomina, il Dirigente:

- trasmette il relativo provvedimento al Direttore Generale, laddove istituito, o al Segretario Generale, e per conoscenza al Referente GDPR, presso la stazione di protocollazione appositamente predisposta per le pratiche relative alla privacy.

Il Gruppo Privacy:

- è presieduto dal Referente GDPR
- è previsto un Coordinamento, composto da personale interno con esperienze in materia di protezione dei dati, cui sono attribuiti dal Direttore Generale, laddove istituito, o dal Segretario Generale i compiti di supervisione e di assistenza delle attività relative al GDPR svolte dai Dirigenti delegati

COMPITI E FUNZIONI ASSEGNATI AI REFERENTI DEL GRUPPO PRIVACY	
a)	Apportare contributi di studio e approfondimento in materia di protezione dei dati personali
b)	Collaborare con i Dirigenti del Settore di appartenenza all'attuazione delle misure adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo
c)	Supportare il Dirigente delegato nelle attività di aggiornamento puntuale dei trattamenti e di tutta la documentazione relativa ai ruoli del proprio Settore di afferenza

2.3.7 Autorizzati al trattamento

NOMINA DEL PERSONALE AUTORIZZATO

1 I Dirigenti possono autorizzare per specifiche attività di trattamento i dipendenti appartenenti alla struttura organizzativa di competenza

2 Il Provvedimento di nomina del Dirigente individua l'ambito del trattamento consentito e le istruzioni per il corretto trattamento dei dati

I Soggetti autorizzati:

- operano sotto la diretta autorità del Dirigente che li ha nominati
- si attengono alle istruzioni impartite per iscritto

Elementi necessari dell'autorizzazione:

- individuazione nominativa (nome e cognome) delle persone fisiche in relazione a ciascun trattamento dati assegnato
- istruzioni impartite agli incaricati del trattamento, da diversificare in relazione alle specificità dei singoli trattamenti
- le istruzioni devono contenere un espresso richiamo alle policy dell'Ente in materia di sicurezza informatica, protezione dei dati personali e gestione documentale

Efficacia temporale dell'autorizzazione:

- L'autorizzazione è efficace sino a revoca formalmente adottata, o fino al trasferimento dell'incaricato a struttura organizzativa di competenza di altro dirigente, o fino a cessazione del rapporto

In caso di passaggio del dipendente ad altro Servizio dell'Ente:

- Ogni qualvolta il Dirigente assume sotto di sé nuovi dipendenti, intendendosi per tali anche coloro che passno da un servizio all'altro, questi verranno incaricati allo svolgimento dei trattamenti di dati personali effettuati presso la struttura

2.3.8 Amministratori di Sistema

Gli amministratori di sistema individuati nel glossario del presente documento governano specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati, anche personali.

> *Il sistema di nomina degli ADS avviene secondo il seguente ordine consequenziale:*
>
> *- ciascun Dirigente, in relazione alle funzioni attribuite, laddove necessario, per lo svolgimento di tali compiti e funzioni individua uno o più Amministratori di sistema;*
>
> *- Il Sindaco nomina gli ADS con proprio decreto;*
>
> *- il Dirigente preposto ai sistemi informativi attribuisce specifici profili di autorizzazione, ambiti di operatività e ammontare dell'incentivo riconosciuto per tale attività, individuati da ciascun Dirigente.*

La nomina dell'ADS interno:

- costituisce allegato alla nomina ad incaricato del trattamento
- riporta le istruzioni generali relative allo svolgimento di tali compiti e funzioni, nonché le istruzioni specifiche in relazione agli strumenti assegnati
- avviene previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, indipendentemente dai titoli posseduti, da parte del Dirigente preposto ai sistemi informativi che richiama nella nomina tutte le misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste e richiamate dal presente Modello organizzativo

COMPITI E FUNZIONI ASSEGNATI ALL'AMMINISTRATORE DI SISTEMA INTERNO	
a)	fornisce idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza informatica
b)	presenta annualmente al Dirigente preposto ai sistemi informativi apposita relazione sull'attività svolta e sul rispetto tutte le misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali
c)	è soggetto a valutazione della persistenza dei requisiti da parte del Dirigente preposto ai sistemi informativi, anche sulla base della relazione annuale
d)	partecipa alle almeno due sessioni formative annuali dedicate al gruppo di ADS organizzate dal Dirigente preposto ai sistemi informativi al fine di garantire un adeguato aggiornamento
e)	supporta il Dirigente delegato nella stesura dell'informativa da fornire agli utenti in relazione al sistema informativo gestito

ESTERNALIZZAZIONE DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA

Nei casi in cui vengano esternalizzate le funzioni di ADS sui sistemi dell'Ente, il Comune:

a) nomina il fornitore del servizio quale Responsabile del trattamento, ai sensi dell'art. 28 GDPR

b) richiede al fornitore la comunicazione dei propri amministratori di sistema entro un termine predefinito nell'accordo, provvedendo successivamente al tempestivo aggiornamento

c) definisce i livelli di autorizzazione in base al servizio reso o al bene fornito

Il Dirigente preposto alla gestione dei sistemi informativi:

a) mantiene e aggiorna l'elenco contenente l'identità degli amministratori di sistema nell'ambito della propria organizzazione e i diversi servizi informatici cui questi sono preposti e lo rende disponibile in caso di accertamenti anche da parte dell'Autorità Garante

b) aggiorna annualmente l'elenco e lo pubblica sulla intranet aziendale

2.3.9 Contitolare del trattamento

Nelle ipotesi in cui il Comune di Rimini determini congiuntamente ad altri Titolari del trattamento le finalità e i mezzi del trattamento, entrambi vengono qualificati come Contitolari del trattamento.

In caso di Contitolarità del trattamento, il Comune:

- redige un accordo con l'altro soggetto contitolare, ai sensi dell'art. 26 del GDPR, in modo da disciplinare le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal GDPR stesso

Requisiti dell'accordo di Contitolarità:

- le rispettive funzioni per la redazione, il rilascio e la conoscibilità delle informative di cui agli articoli 13 e 14 del GDPR
- la disciplina dei rispettivi ruoli e i rapporti dei contitolari con gli interessati
- la possibilità di designare un punto di contatto comune per gli interessati
- le modalità di esercizio dei diritti dell'interessato

Il Dirigente delegato:

- effettua le verifiche circa le basi giuridiche, il contesto, le finalità e i mezzi approntati per i trattamenti realizzati congiuntamente ad altri soggetti, al fine di accertare il configurarsi delle ipotesi di contitolarità e avviare le procedure per la redazione dell'accordo

- propone al contitolare, per quanto sia possibile in relazione al tipo e alla natura dei trattamenti oggetto di accordo, il sistema organizzativo previsto dal presente Modello e dalle procedure ad esso allegate

Pubblicità dell'accordo di Contitolarità:

- il contenuto essenziale dell'accordo viene messo a disposizione degli interessati all'interno dell'informativa ex art. 13 GDPR, i quali potranno esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento secondo le modalità preliminarmente concordate tra le parti nell'accordo suddetto

2.3.10 Responsabile della protezione dati (RPD o DPO)

> *Il Regolamento UE 2016/679 prevede in ambito pubblico l'obbligo per il Titolare del trattamento di designare un Responsabile della protezione dati (RPD o DPO).*

Il Responsabile della protezione dei dati:

- svolge compiti di consulenza nei confronti del Titolare e dei soggetti designati o autorizzati al trattamento, e di sorveglianza sull'osservanza del Regolamento UE 2016/679

Affidamento del ruolo di RPD/DPO:

- il ruolo di RPD/DPO può essere affidato a soggetto esterno oppure può essere svolto da un dipendente del Titolare, entrambi in possesso dei requisiti necessari per assolvere a tale compito, secondo le indicazioni fornite dal Garante Privacy nei suoi interventi

RPD/DPO INTERNO

- deve essere garantita sufficiente autonomia e il rapporto diretto con il vertice amministrativo, così come richiesto dall'art. 38 GDPR
- deve prediligersi un Dirigente o un funzionario di alta professionalità, i quali:
  - siano in possesso di una conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati;
  - abbiano capacità adeguate ad assolvere i compiti di cui all'articolo 39 del GDPR;
  - non si trovino in situazioni di conflitto di interessi relativamente ai compiti e alle funzioni assegnategli.
- la nomina interna avviene con deliberazione di Giunta, che ne definisce i compiti e le funzioni secondo quanto indicato dall'art. 37 ss GDPR

- i dati di contatto del DPO vengono comunicati al Garante per la protezione dei dati personali secondo apposita procedura digitale predisposta sul canale dell'Authority, e vengono pubblicati sul sito istituzionale dell'Ente nell'apposita sezione 'privacy'

RPD/DPO ESTERNO

- deve essere garantita sufficiente autonomia e il rapporto diretto con il vertice amministrativo, così come richiesto dall'art. 38 GDPR
- in caso di affidamento esterno del servizio, la scelta soggiace alle regole stabilite dal Codice dei contratti pubblici, d.lgs. n. 50/2016, e i compiti del DPO vengono definiti nell'accordo di cui agli artt. 37 ss del Regolamento UE 2016/679
- il DPO viene nominato con provvedimento del Dirigente cui sono attribuite le funzioni in materia di GDPR, contestualmente o successivamente all'affidamento del Servizio
- i dati di contatto del DPO vengono comunicati al Garante per la protezione dei dati personali secondo apposita procedura digitale predisposta sul canale dell'Authority, e vengono pubblicati sul sito istituzionale dell'Ente nell'apposita sezione 'privacy'

COMPITI DEL RPD/DPO

- il RPD/DPO svolge i compiti indicati dall'art. 39 GDPR

In merito ai pareri da fornire in ordine alla legittimità e alla correttezza dei trattamenti di dati personali, si fa riferimento a quanto di seguito indicato.

A) Pareri da richiedere obbligatoriamente **da parte dell'Ente in ordine a:**

- redazione di valutazione di impatto dei rischi di cui all'art. 35 GDPR e conseguente individuazione di misure poste a mitigazione del rischio, ed eventuali prescrizioni
- consultazione in merito alle violazioni dei dati personali ai fini della valutazione e dell'eventuale notifica, ai sensi dell'art. 33 del Regolamento, al Garante per la protezione dei dati personali

B) Pareri da richiedere in via facoltativa **(se ritenuti utili) da parte dell'Ente in ordine a:**

- progettazione di nuove applicazioni o modifica sostanziale di quelle esistenti, in aderenza al principio della privacy *by design e by default*
- individuazione delle misure che abbiano un significativo impatto sulla protezione dei dati personali che l'Ente intende adottare ai fini della tutela della

riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente, anche a seguito di incidenti di sicurezza o valutazione dei rischi

- valutazione dell'eventuale pregiudizio che l'accesso civico potrebbe comportare agli interessi dei controinteressati, nella misura in cui questi afferiscono alle tutele dei loro dati personali ai sensi del comma 2 dell'art. 5-bis e, in via generale, del Regolamento UE n. 679/2016
- opposizione formulata dai controinteressati nella misura in cui questa sia riferibile ad elementi afferenti alla protezione dei dati personali, valutando la probabilità e la serietà del danno agli interessi degli opponenti
- valutazione delle richieste di esercizio dei diritti GDPR, in caso di particolare complessità

2.3.11 Il Responsabile del trattamento

Il ruolo di Responsabile del trattamento può essere assunto dalla persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

COMPITI E FUNZIONI INTERNI IN RELAZIONE AL PROCESSO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO

- il RPD/DPO svolge i compiti indicati dall'art. 39 GDPR

Il dirigente delegato:

ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato

definisce i ruoli dei soggetti coinvolti nell'ambito del sistema di protezione dei dati personali e sottoscrive uno specifico accordo

definisce gli elementi essenziali dell'accordo in conformità all'art. 28 del Regolamento UE 2016/679 ed alle clausole standard assunte in materia tramite decisione della Commissione europea

In particolare, il Dirigente delegato pone attenzione:

A FORNIRE al Responsabile del trattamento tutte le istruzioni necessarie allo svolgimento del trattamento oggetto di esternalizzazione;

A FORNIRE le eventuali informative agli interessati necessarie allo svolgimento del trattamento oggetto di esternalizzazione;

ALLA CORRETTA INDICAZIONE dei sub-responsabili da parte del Responsabile del trattamento in allegato alla nomina, e all'aggiornamento di essi durante tutta l'esecuzione dell'accordo principale;

A SVOLGERE VERIFICHE nei confronti del Responsabile del trattamento durante l'attuazione dell'accordo, che possono assumere la veste di *audit*, per valutare al persistenza di garanzie sufficienti a mettere in atto misure tecniche e organizzative adeguate. Tali verifiche riguardano esclusivamente i mezzi e le modalità organizzative relative ai trattamenti oggetti dell'accordo sottoscritto tra le parti;

A PREVEDERE LA CORRETTA CANCELLAZIONE E DISTRUZIONE, laddove necessario e in relazione allo specifico servizio, di tutti i dati personali dopo che è terminata, per qualsiasi causa, la prestazione dei servizi relativi al trattamento e la cancellazione delle copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati

A VERIFICARE CHE il Responsabile del trattamento garantisca un adeguato flusso informativo e un supporto in relazione agli specifici casi indicati nell'accordo sottoscritto e derivanti dall'art. 28 GDPR, tra cui ad esempio l'eventuale tempestiva comunicazione del verificarsi di un *data breach*.

Il Referente GDPR:

rende disponibile a tutto l'Ente un format di accordo ex art. 28 GDPR redatto secondo le indicazioni della Commissione UE, da compilare a cura del Dirigente delegato, anche con il supporto del Gruppo Privacy

Il ruolo di Responsabile può essere assunto anche da parte del Comune e, in tal caso, il Dirigente, anche con l'eventuale supporto del Gruppo Privacy, verifica che:

la nomina sia coerente rispetto al servizio reso dal Comune

la nomina sia coerente rispetto a quanto richiesto dall'art. 28 GDPR

la nomina non richieda oneri o vincoli maggiormente gravosi rispetto al servizio reso dal Comune

2.3.11.1 Check list per l'affidamento di servizi o per l'acquisto di beni

In tutti i casi in cui si intenda procedere all'affidamento di un servizio da cui derivi l'individuazione di un Responsabile del trattamento dati, ciascun Dirigente delegato, preventivamente all'affidamento, effettua una valutazione di privacy *by design* secondo quanto indicato nel presente Modello e in base agli orientamenti di *soft law* nazionali ed europei.

In particolare, il Dirigente verifica:

- se il servizio reso dal terzo preveda trattamenti di dati personali in base alla check list contenuta nella procedura definita con apposito documento, da adottarsi contestualmente o successivamente al presente Modello organizzativo, e costituente parte integrante dello stesso

2.3.12 Destinatario e Interessato

Per Interessato si intende:

- la persona fisica, non giuridica, cui afferiscono i dati personali. Esso è titolare di diritti relativi al trattamento dei propri dati personali, che nel prosieguo del presente Modello vengono individuati, e ne vengono altresì indicate le modalità con cui si esplicano in relazione al Titolare Comune di Rimini

Per Destinatario si intende:

- la persona fisica o giuridica, l'autorità pubblica, il servizio, o altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi

- non sono considerati destinatari, anche sulla base di quanto previsto dalla Direttiva 2016/680, recepita in Italia con d.lgs. n. 51/2018, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri

- Il diritto dell'Unione Europea considera, infatti, che il trattamento di tali dati da parte di dette autorità pubbliche sia conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento.

2.3.12.1 Informativa

Ogni qualvolta vi sia un trattamento di dati personali, il Titolare del trattamento o il Responsabile del trattamento devono rendere una informativa agli interessati, che li informi delle finalità e modalità del trattamento dei propri dati personali mediante l'indicazione delle informazioni elencate agli articoli 13 e 14 del GDPR.

L'informativa rappresenta l'attuazione del dovere del Titolare del trattamento o del Responsabile del trattamento di assicurare la trasparenza e la correttezza dei trattamenti fin dalla fase di progettazione degli stessi, e di essere in grado di comprovarlo in qualunque momento.

COMPITI DEL DIRIGENTE DELEGATO IN RELAZIONE ALLE INFORMATIVE

- Il Dirigente delegato predispone l'informativa sulla base del format messo a disposizione tramite gli strumenti di informazione interna, rispettando i criteri fissati dall'art. 12 del GDPR

REQUISITI DELL'INFORMATIVA

- L'informativa predisposta dal Dirigente delegato deve essere:
  - ✓ concisa;
  - ✓ trasparente;
  - ✓ intelligibile;
  - ✓ facilmente accessibile;
  - ✓ scritta con un linguaggio semplice e chiaro.

Nel caso di informazioni destinate specificamente ai minori occorre prestare maggiore attenzione agli elementi richiamati per garantirne la comprensibilità.

CONTENUTO MINIMO DELL'INFORMATIVA AI SENSI DEGLI ARTICOLI 13 E 14 DEL GDPR

- categorie di dati trattati e finalità del trattamento (non le modalitàà del trattamento, ma quali dati vengono trattati, divisi per categorie)
- base giuridica del trattamento, secondo quanto stabilito dagli artt. 6 e 9 del Regolamento europeo
- natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di tale rifiuto
- se il titolare ha intenzione di utilizzare i dati per una finalità diversa da quella per la quale sono stati raccolti
- soggetti destinatari (anche per categorie) ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica)
- se il titolare ha intenzione di trasferire i dati in paesi extra UE occorre indicare se la Commissione UE abbia adottato una decisione di adeguatezza rispetto a quel Paese (ovvero se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato, per cui il trasferimento non necessita di autorizzazioni specifiche)
- il periodo di conservazione dei dati oppure l'indicazione dei criteri per determinarlo
- i diritti dell'interessato
- dati identificativi del titolare del trattamento (nome, denominazione o ragione sociale, domicilio o sede) e un recapito al quale gli interessati potranno rivolgersi per esercitare i propri diritti
- i dati di contatto del Responsabile per la protezione dei dati
- se il trattamento comporta processi decisionali automatizzati (come la profilazione) l'informativa deve specificarlo e deve indicare anche la logica di tali processi decisionali e le conseguenze previste per l'interessato
- Nel caso di raccolta dati presso terzi occorre indicare specificamente anche:
  - ✓ La fonte da cui hanno origine i dati personali (che può essere anche fonte accessibile al pubblico);
  - ✓ si omette, invece, l'informazione circa la natura obbligatoria o meno della comunicazione di dati personali, perché nella fattispecie i dati non sono raccolti presso l'Interessato.

Nel caso in cui i dati dell'interessato non fossero acquisiti direttamente dal Titolare, ma venissero acquisiti presso terze parti (ad esempio: altre Amministrazioni) è necessario integrare l'informativa di cui all'art. 13 con i contenuti di cui all'art. 14 del Regolamento UE 2016/679.

> I dati raccolti per determinate finalità non possono essere trattati per finalità ulteriori, a meno che non si tratti di finalità di rilevante interesse pubblico connesso alle attività istituzionali dell'Ente ed è proporzionato all'obiettivo legittimo perseguito.

Nel caso in cui i dati raccolti venissero trattati per finalità ulteriori occorre:

- tenere conto di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare relativamente alla relazione tra l'Interessato e il titolare del trattamento, della natura dei dati personali, specialmente se siano trattate categorie particolari di dati personali, oppure se siano trattati dati relativi a condanne penali e a reati, delle possibili conseguenze dell'ulteriore trattamento previsto per gli interessati, nonché dell'esistenza di garanzie adeguate, che possono comprendere la cifratura o la pseudonimizzazione

- laddove non sussistano tali condizioni, rilasciare un'informativa per l'ulteriore trattamento o, nel caso in cui si esulasse dalle competenze istituzionali dell'Ente, l'acquisizione del consenso dell'Interessato

- se l'ulteriore trattamento fosse già conosciuto da parte del Titolare al momento della raccolta di dati, le informazioni circa l'ulteriore finalità vengono già esplicitate nell'informativa iniziale, ed eventualmente viene già acquisito il consenso per lo specifico trattamento

MODALITÀ DI GESTIONE DELLE INFORMATIVE

- Le informazioni sono fornite:

  - ✓ per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici;
  - ✓ se richiesto dall'Interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dello stesso;
  - ✓ prima o al massimo al momento di dare avvio alla raccolta dei dati

- Non è necessaria l'informativa quando:

  - ✓ il trattamento è connesso allo svolgimento delle "investigazioni difensive" in materia penale (art. 38 norme di attuazione del c.p.p.) o alla difesa di un diritto in sede giudiziaria (a meno che il trattamento si protragga per un periodo superiore a quello strettamente necessario al perseguimento di tali finalitàà o sia svolto per ulteriori scopi);
  - ✓ il trattamento riguarda dati anonimi (es. aggregati sui quali non è possibile in alcun modo procedere all'associazione ad uno specifico soggetto interessato) o dati di enti o persone giuridiche, ad eccezione di quei dati che possano ricondurre a persone fisiche (es. denominazione della società unipersonale riportante nome e cognome della persona

fisica).

2.3.12.2 Consenso

Definizione di consenso:

- Il consenso dell'Interessato consiste in qualsiasi manifestazione di volontà dello stesso con la quale manifesti assenso al trattamento dei propri dati personali.

I requisiti inderogabili del consenso sono:

1. **LIBERO**

   L'Interessato deve essere in grado di operare una scelta effettiva, non soggetta ad intimidazioni o raggiri, né deve subire conseguenze negative a seguito del mancato conferimento del consenso.

2. **SPECIFICO**

   Il consenso deve essere prestato in relazione alla finalità per la quale è eseguito lo specifico trattamento. In tal senso, qualora il trattamento abbia più finalità, il consenso viene prestato per ciascuna di esse, e in caso di modifiche viene richiesto un nuovo consenso

3. **INFORMATO**

   In base al principio di trasparenza, l'Interessato viene posto in condizioni di conoscere la categoria di dati trattati, le modalità, le finalità e i diritti attribuiti dalla legge. Vengono anche indicate le eventuali conseguenze del mancato rilascio del consenso

4. **INEQUIVOCABILE**

   non è necessario che il consenso sia esplicito, può anche essere implicito, purché non sia tacito. Può desumersi dalle circostanze, purché non sussistano dubbi che con il suo comportamento l'interessato abbia voluto comunicare il proprio consenso. Il consenso deve essere esplicito in caso di trattamento di dati personali particolari, o nel caso di processi decisionali automatizzati (es. profilazione)

5. **REVOCABILE**

6. il consenso può essere revocato in qualsiasi momento, mediante modalità semplificate e senza obbligo di motivazione, salve eventuali altre basi giuridiche per le quali il trattamento deve avere luogo. A tal fine, la procedura di revoca deve corrispondere, o comunque essere simile, a quella del conferimento del consenso. A seguito di revoca del consenso il Dirigente verifica la legittimità della richiesta e, in caso di esito positivo, predispone la cancellazione dei dati raccolti, salvo siano necessari per la conservazione nel pubblico interesse sulla base della normativa vigente

Il consenso costituisce una delle basi giuridiche del trattamento, di cui all'art. 6 GDPR, ma configura una fattispecie residuale nel contesto della disciplina, poiché presuppone un trattamento particolarmente invasivo per l'Interessato.

Il consenso viene richiesto solo laddove ciò sia valutato necessario dal Dirigente, a seguito dell'analisi del processo relativo allo specifico trattamento.

In ogni caso, il consenso non può costituire la base giuridica del trattamento in caso di evidente squilibrio tra le parti e i dati vengono trattati su base giuridica differente. Ad esempio, nel caso di rapporti di lavoro.

Comune di Rimini

LUOGHI, STRUMENTI E RAPPORTI

3.1 LUOGHI, STRUMENTI E RAPPORTI

Il Comune di Rimini agisce quale Titolare del trattamento di dati personali, e tutte le articolazioni ad esso facenti capo concorrono alla sua definizione.
Nel presente capitolo vengono analizzati:

- i rapporti interni al Comune di Rimini che comportino trattamenti di dati personali di terzi o dati personali di dipendenti e collaboratori nell'ambito del rapporto di lavoro
- la condivisione dei dati con altri soggetti pubblici
- il trasferimento dei dati al di fuori dello spazio economico europeo
- gli strumenti organizzativi per la gestione dei trattamenti di dati personali

3.2 I RAPPORTI INTERNI: Il rapporto di lavoro

Il rapporto di lavoro tra il Comune di Rimini e i propri dipendenti e collaboratori comporta reciproci doveri di protezione dei dati, derivanti dalla disciplina europea e nazionale, nonché dalle regole di organizzazione interna adottate dall'Amministrazione.
Di seguito vengono definiti i principali obblighi afferenti al datore di lavoro Comune di Rimini, anche in relazione ai rapporti con le rappresentanze sindacali, nonché gli obblighi posti in capo a dipendenti e collaboratori dello stesso.

3.2.1 Gli obblighi di protezione dei dati personali nei confronti del lavoratore nell'ambito dei rapporti di lavoro.

I trattamenti dei dati personali di dipendenti e collaboratori effettuati dal Comune di Rimini, in qualità di datore di lavoro e Titolare del trattamento nell'ambito del contesto lavorativo, riguardano solo i dati strettamente necessari all'esecuzione del rapporto di lavoro, secondo quanto stabilito dalle norme di settore, quali la l. n. 300/1970, e dagli specifici orientamenti di soft law

CHI PUO' TRATTARE I DATI DERIVANTI DALLA GESTIONE DEL RAPPORTO DI LAVORO?

I dati possono essere trattati solo dal personale incaricato dal Dirigente preposto alla gestione del personale e dal Dirigente, assicurando idonee misure organizzative e di sicurezza per proteggerli da intrusioni o divulgazioni illecite.

Mentre, i dati impiegati nell'ambito delle esigenze della gestione dei sistemi informativi sono trattati solo da personale incaricato dal Dirigente IT.

STRUMENTI INFORMATIVI E CONTROLLO A DISTANZA

Principale normativa di riferimento:

- *Legge 20 maggio 1970, n. 300*

Finalità di trattamento di cui all'art. 4 della L. 300/70

- *esigenze organizzative e produttive;*
- *sicurezza del lavoro;*
- *tutela del patrimonio aziendale.*

Presupposti di legittimità di cui all'art. 4 della L. 300/70

- accordo sindacale;
- autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Individua le misure più adeguate ed efficaci per la tutela della riservatezza, integrità e disponibilità del patrimonio informativo dell'Ente

TRATTAMENTI REALIZZATI DAL COMUNE DI RIMINI NELL'AMBITO DEGLI STRUMENTI INFORMATIVI E CONTROLLO A DISTANZA

Il Comune di Rimini predispone strumenti informativi non finalizzati a controlli sistematici sull'attività lavorativa nei confronti del personale, salvo nel caso di interventi necessari alla salvaguardia del patrimonio del Titolare e alla sicurezza dei dati dello stesso.

Nel rispetto della disciplina di settore, degli specifici orientamenti di *soft law*, nonché della regolamentazione comunale, l'Ente accede alla posta elettronica, ai dati di navigazione e ai dati relativi all'utilizzo delle altre risorse tecnologiche a disposizione del lavoratore solo nei casi di seguito riportati:

qualora gli Amministratori di Sistema debbano effettuare tale accesso al fine di eseguire la dovuta manutenzione tecnica su sistemi informatici, nonché di effettuare le necessarie verifiche sulla funzionalità e sicurezza dei sistemi e dei dispositivi concessi in uso, anche nei casi di incidenti di sicurezza, fermo

restando che in nessun caso, per tali finalità, potranno accedere al contenuto dei singoli file, e-mail, comunicazioni, ecc.;

- nei casi consentiti dalla legge, ove vi siano fondati motivi per ritenere che siano stati commessi abusi o attività illecite o vi sia necessità per l'Ente di esercitare o difendere un proprio diritto in sede giudiziaria

CONTROLLI DIFENSIVI

Resta ferma la possibilità per l'Ente, nei casi consentiti dalla legge, di effettuare controlli difensivi sulla posta elettronica, sui dati di navigazione ad Internet e su ogni altro dato contenuto nelle risorse informatiche concesse in uso al personale, ossia quei controlli diretti ad accertare, sulla base di un fondato sospetto, comportamenti illeciti dei lavoratori, quando tali comportamenti riguardino l'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro.

GARANZIE PER IL RISPETTO DELL'ART. 5 DEL GDPR

Il Comune di Rimini, nella qualità di datore di lavoro e di Titolare del trattamento, nella figura del Dirigente preposto alla gestione del personale, in base ai principi fissati dall'art. 5 GDPR:

- assicura che i dati siano trattati per finalità specifiche e legittime, tenendo in considerazione il principio di limitazione delle finalità, assicurando che i dati raccolti siano adeguati, pertinenti e limitati per la finalità legittima
- fornisce policy in merito alla gestione dei documenti e propone al Dirigente competente in materia di sistemi informativi eventuali policy relative agli strumenti informatici in dotazione all'Ente, relativamente alla gestione del personale;
- favorisce l'esercizio dei diritti dei dipendenti in qualità di Interessati
- assicura l'esattezza dei dati e non li conserva più a lungo del necessario operando, a tal fine, una ricognizione periodica
- adotta tutte le misure necessarie per garantire il corretto impiego degli strumenti di accesso logico ai locali dell'Ente
- assicura che sul luogo di lavoro sia garantita la tutela dei diritti, delle libertà fondamentali e della dignità delle persone anche in relazione alla riservatezza nelle relazioni personali e professionali, verificando periodicamente

l'adeguatezza dei processi degli uffici dedicati alla gestione del personale

predispone, in accordo con il Referente GDPR, piani formativi affinché il personale incaricato dei trattamenti relativi alla gestione del personale sia consapevole degli obblighi in materia di protezione dei dati

ESERCIZIO DEI DIRITTI NELL'AMBITO DEL RAPPORTO DI LAVORO

Il dipendente o il collaboratore che ritenga di aver subìto una lesione di diritti e libertà legati al trattamento dei propri dati personali ha facoltà di rivolgersi direttamente al Titolare del trattamento o al RPD/DPO, tramite i contatti indicati sul sito istituzionale dell'Ente, per segnalare la violazione. La segnalazione al RPD/DPO non costituisce incarico professionale allo stesso, ma è finalizzato a coadiuvare il RPD/DPO nell'esercizio delle proprie funzioni.

3.2.1.1 Attivazione e disattivazione utenze del dipendente o collaboratore

Il contratto di lavoro sottoscritto con il dipendente, o con il collaboratore, contiene una clausola relativa alla sicurezza dei dati personali e alla sicurezza informatica.
In particolare, il dipendente si impegna ad utilizzare gli strumenti informatici di lavoro per le finalità cui sono destinati e secondo le policy definite dal datore di lavoro.
Il Dirigente presso cui è assegnato il dipendente in prima destinazione di lavoro presenta tramite protocollo al Dirigente competente in materia di sistemi informativi la richiesta di creare un'utenza per il neoassunto e l'elenco dei sistemi informativi cui il dipendente deve accedere, unitamente alla relativa nomina ad incaricato del trattamento dei dati personali.

In caso di trasferimento da un servizio ad un altro, all'interno dell'Amministrazione Comunale, il Dirigente presso cui è assegnato il dipendente riceve la lista delle abilitazioni dal Dirigente precedente e conferma al Dirigente competente in materia di sistemi informativi le abilitazioni da mantenere e quelle da dismettere.

Al termine del contratto di lavoro il dipendente o il collaboratore rilascia dichiarazione scritta di non possedere copie di dati e informazioni strettamente attinenti all'attività lavorativa, nonché di aver restituito tutti i beni (laptop, cellulare, etc...) di proprietà dell'organizzazione.

Prima della conclusione del contratto di lavoro, il dipendente trasferisce ai colleghi i dati di ufficio necessari allo svolgimento del lavoro da parte degli stessi.

> *Al dipendente non più contrattualizzato con il Comune di Rimini viene garantito l'accesso al proprio cloud fino al tempo stabilito nella policy sulla sicurezza informatica dalla cessazione del rapporto di lavoro.*

L'utenza rimane attiva presso il Servizio preposto ai sistemi informativi per il tempo necessario e ragionevole alla predisposizione delle misure tecniche per la sua disattivazione, contemperando l'interesse del Titolare ad accedere alle informazioni necessarie all'efficiente gestione della propria attività e a garantirne la continuità con la legittima aspettativa di riservatezza del dipendente, e comunque fino ad un massimo di 3 mesi, o fino a conclusione di eventuale processo o procedimento disciplinare.

3.2.1.2 Informative a dipendenti e collaboratori

Trattamenti oggetto di informativa

- Tutte le attività richiamate nel presente paragrafo
- Eventuali ulteriori trattamenti

Modalità di consegna

- In sede di sottoscrizione del contratto di lavoro
- Tramite pubblicazione di notizia nella home page dello strumento informativo interno dell'Ente
- Invio alla casella di posta elettronica di ciascun dipendente o collaboratore

Ulteriori adempimenti

- Nei casi previsti dalla legge il trattamento segue il previo accordo con le rappresentanze sindacali

FOCUS
Dati giudiziari

In relazione al fatto che il trattamento di dati personali può avvenire solo alla ricorrenza di una delle basi giuridiche di cui all'art. 6 del GDPR, e in riferimento all'art. 2-octies del D.Lgs. 101/2018, il trattamento di dati personali relativi a condanne penali e a reati o a connesse misure di sicurezza è consentito solo se autorizzato da una norma di legge o, nei casi previsti dalla legge, di regolamento, che prevedano garanzie appropriate per i diritti e le libertà degli interessati.

In mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati sono individuate con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante Privacy.

In relazione al trattamento di dati giudiziari relativi al personale dipendente del Comune di Rimini si applicano, dunque, le previsioni stabilite da fonti normative di primo e secondo livello, laddove adottate dall'Autorità pubblica.

3.2.2 Gli obblighi di protezione dei dati da parte del lavoratore

Atti e documenti a cui attenersi durante le attività di trattamento dati da parte del personale comunale in ragione dell'attività svolta per l'Ente

- Contratto di lavoro
- Disposizioni del Codice di Comportamento
- Modello organizzativo di protezione dei dati personali
- Disciplinare con cui il Dirigente incarica il personale al trattamento dei dati personali
- Specifiche indicazioni d'uopo fornite dal Referente GDPR o dal Dirigente nel caso in cui si rendessero necessarie in relazione alla natura di un determinato servizio

Il dipendente è legittimato al trattamento dei dati relativi all'espletamento delle mansioni derivanti dal rapporto contrattuale con l'Ente

L'indicazione dei trattamenti, nonché i limiti delle operazioni realizzabili, vengono specificati nell'atto di autorizzazione al trattamento dei dati in qualità di incaricato del trattamento, che viene consegnata al dipendente.

Il dipendente, pertanto, è designato ed autorizzato al trattamento dati nell'ambito dello svolgimento dei compiti e funzioni in relazione all'ambito di competenza assegnato dal Dirigente

Istruzioni per il trattamento dei dati effettuato anche tramite gli applicativi *hardware* e *software* in dotazione al lavoratore

Il dipendente è tenuto ad adottare le istruzioni generali per il trattamento dei dati indicate all'interno di provvedimento di dirigenziale di nomina/autorizzazione al trattamento, il cui format è disponibile in apposita sezione dello strumento informativo interno dell'Ente.

Lavoro agile e trattamento dati

Il Comune di Rimini organizza il lavoro dei propri lavoratori anche tramite forme di lavoro agile, intese quali modalità di esecuzione del rapporto di lavoro subordinato caratterizzate dall'assenza di vincoli orari o spaziali. Anche in questo caso, il lavoratore viene edotto degli obblighi di protezione dei dati personali in relazione alle circostanze con cui avviene la prosecuzione del lavoro con modalità remota, secondo quanto previsto da apposito Regolamento comunale.

Tra le misure di prevenzione da adottare, il lavoratore è tenuto a:

- utilizzare le risorse informatiche affidate in dotazione dall'Ente solo per rendere la prestazione lavorativa, evitando usi per fini personali;
- evitare la gestione locale di dati;
- non installare programmi o servizi diversi da quelli autorizzati dal Titolare del trattamento e dall'Amministratore di sistema;
- non lasciare incustodito il supporto elettronico ogni qualvolta ci si assenti dal locale nel quale è ubicata la postazione di lavoro, ovvero dal locale adibito allo svolgimento del lavoro agile.

Policy di sicurezza e utilizzo di strumenti personali

Il lavoratore è tenuto ad adottare le istruzioni generali per il trattamento dei dati indicate all'interno della Policy di sicurezza informatica dell'Ente.
Non è consentito l'utilizzo di strumenti personali, salvo particolari condizioni in cui la prestazione si renda necessaria e non vi siano altri mezzi dell'Amministrazione a disposizione del dipendente o collaboratore per renderla.

3.2.3 Gli strumenti di lavoro

Ai fini del presente Manuale Organizzativo, si considerano strumenti di lavoro gli apparecchi, i dispositivi, gli apparati e i congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa dedotta in contratto, e che per tale finalità siano stati posti in uso e messi a sua disposizione

Strumenti di lavoro

Nell'ambito dello svolgimento dei compiti assegnati, i lavoratori utilizzano tutti gli strumenti concessi in dotazione dall'Ente finalizzati a rendere la prestazione lavorativa distinti in due categorie.

Strumenti elettronici	Strumenti manuali
Asset	documenti cartacei contenuti in fascicoli, armadi, ripiani, classificatori e uffici

Mediante l'utilizzo di tali strumenti, il lavoratore può effettuare operazioni di trattamento dati riferiti a soggetti interessati relativi al suo specifico settore di competenza. Al contempo, però, questi stessi strumenti raccolgono anche informazioni riferibili al lavoratore durante l'espletamento dell'attività lavorativa.

Istruzioni

Anche per il trattamento dei dati cartacei, il lavoratore è tenuto a rispettare sempre le indicazioni del Dirigente delegato in merito agli archivi a cui poter accedere e ai documenti che è possibile trattare. Il lavoratore non è legittimato a prendere visione dei documenti per i quali non ha ricevuto autorizzazione da parte del Dirigente che li detiene.

Una volta presi in carico, gli atti e i documenti contenenti dati personali non vengono lasciati incustoditi all'interno o all'esterno dei locali ove si svolge l'attività. Il lavoratore, una volta terminate le operazioni di consultazione, utilizzo o le operazioni comunque affidate sui documenti, è tenuto a riporli negli archivi per finalità di controllo e custodia.

Categorie particolari di dati personali

Tali misure vengono applicate anche in caso di documenti contenenti categorie particolari di dati personali e dati personali relativi a condanne penali e reati. In quest'ultimo caso, i documenti considerati non devono essere resi accessibili a personale privo di autorizzazione.

3.2.3.1 Impianti audiovisivi

Principale normativa di riferimento:

- Legge 20 maggio 1970, n. 300

Finalità di trattamento di cui all'art. 4 della L. 300/70

- esigenze organizzative e produttive;

- *sicurezza del lavoro;*

- *tutela del patrimonio aziendale.*

Presupposti di legittimità di cui all'art. 4 della L. 300/70

- accordo sindacale;

- autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro.

Casi di esclusione e analisi degli strumenti utilizzati

I presupposti di legittimità di cui all'art. 4 della L. 300/70 non si applicano in caso di strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa, nonché per l'utilizzo degli strumenti di registrazione degli accessi e delle presenze che non comportino un controllo a distanza dell'attività del lavoratore.

Nei casi di acquisto e implementazione di nuovi strumenti per il trattamento dei dati dei lavoratori, il Dirigente preposto alla gestione del personale, unitamente al dirigente preposto ai servizi informativi, valuta se dal loro utilizzo derivi un controllo a distanza dell'attività del lavoratore e, in caso affermativo, avvia la procedura per la redazione di un accordo con le rappresentanze sindacali ex art. 4, c. 1, l. n. 300/1970.

Informative

L'Ente deve fornire al lavoratore adeguata informativa circa le modalità d'uso degli strumenti e di effettuazione dei controlli nel rispetto di quanto disposto dalla normativa in materia di protezione dei dati personali.

3.3 I RAPPORTI INTERNI: lo scambio di dati tra i Servizi

In caso di scambio di dati personali tra i diversi Servizi interni al Comune, nell'ambito dell'attività ordinaria, l'Ufficio richiedente fornisce all'Ufficio destinatario le seguenti informazioni:

- i dati personali oggetto di richiesta;
- la motivazione circa la necessarietà dei dati;
- le finalità per le quali i dati vengono richiesti, con l'indicazione della norma di legge o di regolamento legittimanti la richiesta.

La richiesta viene inoltrata a firma del Dirigente delegato tramite protocollo.
Il Dirigente che riceve la richiesta può ritenere di non procedere alle formalità suddette assumendosi la responsabilità di ricostruire il ciclo di vita dei dati eventualmente oggetto di *data breach*.

3.4 I RAPPORTI ESTERNI CON ALTRI SOGGETTI PUBBLICI

Tutte le attività che comportano condivisione o trasferimento ad altre Pubbliche Amministrazioni di dati, anche personali, trattati dal Comune di Rimini in qualità di Titolare del trattamento, sono soggetti alle misure di protezione dei dati personali e alle misure di sicurezza informatica fissate dal sistema normativo nazionale ed europeo in tema di sicurezza informatica, dal GDPR, dalle previsioni del presente Modello organizzativo e da quelle contenute nel Manuale sulla sicurezza informatica dell'Ente.

3.5 GLI ACCORDI DI FRUIBILITÀ SUI DATI DEL COMUNE-TITOLARE DEL TRATTAMENTO

Quando vengono sottoscritti gli accordi di fruibilità?

Quando il Comune di Rimini scambia stabilmente dati, anche personali, con altre Amministrazioni Pubbliche, con gestori di pubblici servizi o con privati qualificati.

Cosa garantiscono gli accordi di fruibilità?

- chiarezza di ruoli
- modalità tecniche di trasferimento dei dati
- maggiore sicurezza delle libertà e dei diritti degli interessati
- completa interoperabilità tra i sistemi informativi

Accordo Quadro e verifica dei contenuti

Coerentemente alla strategia europea sulla *governance* dei dati e alla relativa normativa nazionale, la Giunta comunale adotta uno specifico accordo quadro a riferimento dei successivi specifici accordi sottoscritti da ciascun Dirigente, e ne verifica periodicamente la conformità al sistema normativo e di *soft law* vigente.

L'accordo quadro e i singoli accordi vengono sottoposti a verifica periodica da parte dei Dirigenti delegati al fine di verificare che i contenuti e le modalità di accesso ai dati detenuti dal Comune siano coerenti con i principi e con la disciplina stabiliti dal presente documento, nonché con eventuali interventi normativi e di *soft law*.

Accordi di fruibilità e protezione dati

Tutti gli accordi sottoscritti vengono inviati per conoscenza al Referente GDPR tramite la stazione di protocollazione adibita alle pratiche GDPR.

Il trasferimento di un dato da un sistema informativo a un altro non modifica la titolarità del

dato e del trattamento, i cui ruoli vengono preventivamente definiti dalle parti nell'accordo di fruibilità, o recepiti in ragione di atti pregressi.

3.5.1 Il rilascio di dati del Comune-Titolare del trattamento al di fuori degli accordi di fruibilità

Al di fuori degli accordi di fruibilità, che definiscono le modalità di fruibilità continuativa dei dati, laddove la trasmissione di dati, anche personali, tra il Comune ed altri soggetti pubblici, gestori di pubblici servizi o privati qualificati, debba avvenire *una tantum*, è necessario che il soggetto richiedente individui e comunichi al Comune di Rimini le seguenti informazioni:

- tipologia di dati personali di cui si richiede la comunicazione;
- ragioni per le quali i dati richiesti sono strettamente necessari e non eccedenti;
- le Leggi o i regolamenti che prevedono la comunicazione dei dati richiesti;
- le Leggi o i regolamenti che individuano un compito di interesse pubblico o l'esercizio di pubblici poteri per i quali è prevista la comunicazione di dati personali.

FOCUS

Rapporto con le forze dell'ordine

Rispetto al rapporto con le forze dell'ordine si applicano i principi generali fissati dal GDPR e quanto stabilito dal d.lgs. 51 del 18 maggio 2018, che recepisce la Direttiva UE 2016/680 del 27 aprile 2016. Questa si occupa della protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti, i cui trattamenti, secondo l'art. 2, secondo comma, lett. d) GDPR, non rientrano nell'ambito oggettivo di applicazione del Regolamento stesso.

In tali casi, si considera adeguata alla protezione dei dati la richiesta dell'autorità competente acquisita a protocollo, che certifichi il trattamento dei dati personali per le finalità escluse dall'ambito di applicazione oggettiva del GDPR. Diversamente, anche con le forze dell'ordine viene sottoscritto apposito accordo di scambio dei dati.

3.6 I LUOGHI DEL TRATTAMENTO DATI

Il trattamento di dati personali può avvenire:

- all'interno o all'esterno dei locali dell'Ente
- Online e Offline
- Nell'ambito dello Spazio Economico Europeo, ovvero: Stati membri UE, Norvegia, Liechtenstein e Islanda
- Al di fuori dello Spazio Economico Europeo, solo in presenza di requisiti specifici

Il trattamento dei dati, anche personali, avviene nell'ambito delle strutture fisiche adibite a sedi comunali, ma può avvenire in tutti i locali della Pubblica Amministrazione. In tali luoghi il trattamento avviene secondo i principi e le modalità fissate dal GDPR, dalle Autorità in materia, dal presente Modello Organizzativo, nonché da tutti gli atti relativi al comportamento e all'etica vigenti nel Comune di Rimini e presso le Amministrazioni in cui avviene tale trattamento.

I luoghi fisici dell'Amministrazione in cui hanno luogo i trattamenti di dati personali vengono suddivisi in due categorie

a rischio trascurabile

a rischio non trascurabile

⟹ **Luoghi fisici a rischio trascurabile**

Sono quelli in cui i supporti contenenti dati personali sono meno soggetti ad eventi interni o esterni all'organizzazione e da cui il rischio di gravità e probabilità di accadimento di un data breach può ritenersi trascurabile. Ad esempio, si tratta di uffici singoli forniti di chiave funzionante, o di armadi dotati di chiavi funzionanti, e privi del passaggio di utenti esterni.

⟹ **Luoghi fisici a rischio non trascurabile**

Sono quelli in cui i supporti contenenti dati personali sono più soggetti ad eventi interni o esterni all'organizzazione e da cui il rischio di gravità e probabilità di accadimento di un data breach può ritenersi non trascurabile. Ad esempio: corridoi in cui sono collocati armadi, ancorché chiusi a chiave, contenenti dati personali.

Misure organizzative da adottare

Ciascun Dirigente delegato adotta misure organizzative idonee a tutelare i dati presenti nei luoghi fisici ad esso affidati durante la vigenza della nomina dirigenziale.
In relazione ai luoghi virtuali entro cui opera l'Amministrazione, ciascun Dirigente garantisce misure organizzative idonee a tutelare i dati ad esso affidati durante la vigenza della propria nomina dirigenziale, secondo il Manuale di sicurezza informatica dell'Ente.

3.6.1 Il trasferimento di dati personali all'estero

Se i dati personali trattati dal Comune di Rimini vengono trasferiti all'estero, si possono verificare le seguenti ipotesi.	
①	Il trattamento di dati personali ha luogo in uno **Stato facente parte dello Spazio Economico Europeo**: in tal caso, viene indicato lo Stato o gli Stati riceventi sul Registro dei trattamenti, nelle informative sul trattamento dei dati e nell'eventuale nomina del Responsabile o nell'Accordo di contitolarità, a seconda dei casi.
②	Il trattamento di dati personali ha luogo in uno **Stato non facente parte dello Spazio Economico Europeo, ma elencato nella White list del Garante Privacy**, che contiene tutti gli Stati che garantiscono una idonea protezione dei dati personali in quanto oggetto di una Decisione di adeguatezza da parte della Commissione Europea: in tal caso, viene indicato lo Stato o gli Stati riceventi sul Registro dei trattamenti, nelle informative sul trattamento dei dati e nell'eventuale nomina del Responsabile o nell'Accordo di contitolarità, a seconda dei casi, specificando che il paese terzo in questione ha ricevuto un giudizio di adeguatezza dalla Commissione Europea.
③	il trattamento di dati personali ha luogo in uno **Stato non facente parte dello Spazio Economico Europeo e non presente nella White list del Garante della Privacy:** in tal caso, per permettere il trasferimento dei dati sono necessarie garanzie e misure adeguate da valutare anche sulla base della raccomandazione 01/2020 dell'European Data Protection Board, e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Costituiscono garanzie adeguate, per le quali non è necessaria l'autorizzazione del Garante:

- gli strumenti giuridici vincolanti ed esecutivi tra soggetti pubblici (art. 46, par. 2, lett. a);
- le clausole tipo (art. 46, par. 2, lett. c e lett. d)
- le norme vincolanti di impresa di cui all'art. 47 GDPR;
- le clausole contrattuali tipo adottate dalla Commissione europea, da incorporare come allegato agli accordi per il trasferimento dei dati di cui all'art. 46, par. 2, lett. c e lett. d (es. La decisione di esecuzione della Commissione europea del 4 giugno 2021, n. 2021/914 definisce le clausole da allegare nella nomina a Responsabile del trattamento);
- la presenza di codici di condotta (art. 46, par. 2, lett. e);
- la presenza di meccanismi di certificazione (art. 46, par. 2, lett. f).

Costituiscono garanzie adeguate, per le quali risulta, invece, necessaria l'autorizzazione del Garante

- le clausole contrattuali ad hoc, cioè non riconosciute come adeguate tramite decisione della Commissione europea (art. 46, par. 3, lett. a);
- gli accordi amministrativi tra autorità o organismi pubblici (art. 46, par. 3, lett. b).

In mancanza di una decisione di adeguatezza, di garanzie adeguate, o di norme vincolanti d'impresa, è ammesso il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale soltanto se si verifica una delle deroghe fissate dall'art. 49 GDPR, tra cui il trasferimento necessario per importanti motivi di interesse pubblico.
L'art. 48 GDPR vieta trasferimenti di dati verso titolari o responsabili in un Paese terzo sulla base di decisioni giudiziarie o ordinanze amministrative emesse da autorità di tale Paese terzo, a meno dell'esistenza di accordi internazionali, in particolare di mutua assistenza giudiziaria, o analoghi accordi fra gli Stati.

Procedure interne per la verifica dei trasferimenti di dati personali verso Paesi terzi o Organizzazioni internazionali nell'ambito del cloud computing

Nel caso in cui venga sottoscritto un contratto per servizi in cloud-computing il Dirigente o il RUP della procedura verificano se il fornitore dispone di server in paesi extra-UE. In tal caso, svolge le verifiche indicate ai punti 1) -2) -3) del presente paragrafo.

3.6.2 Il Rappresentante nello Stato italiano

Laddove il Responsabile del trattamento non sia stabilito nell'Unione e trovi applicazione l'art. 3, par. 2, Regolamento (UE) 2016/679, questi designa per iscritto un Rappresentante nello Stato italiano comunicandolo al Comune di Rimini, tramite PEC, in sede di partecipazione alla procedura selettiva.

L'obbligo di nomina del Rappresentante non si applica:

- al trattamento se quest'ultimo è occasionale, non include il trattamento, su larga scala, di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o di dati personali relativi a condanne penali e a reati di cui all'articolo 10, ed è improbabile che presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento; oppure
- alle autorità pubbliche o agli organismi pubblici.

3.7 I SITI WEB DEL COMUNE DI RIMINI

Applicazione del principio di Privacy by Design

In sede di ideazione e di realizzazione di un sito web, o di un servizio on-line supportato da un sito web già esistente, vengono adottate misure di protezione dei dati personali fin dalla progettazione, in aderenza a quanto stabilito dal sistema nazionale ed europeo in tema di protezione dei dati personali e di sicurezza informatica, tenendo conto degli obiettivi di accessibilità ai servizi e di usabilità dei dati.
La creazione, o la modifica, di un sito web basato sul trattamento di dati personali, o l'erogazione di un servizio in modalità digitale tramite canale web, viene anticipata da un'istruttoria in cui è coinvolto il Referente GDPR tramite invito inoltrato alla stazione di protocollo adibita alle pratiche privacy.

Ciascun sito web deve contenere almeno:

- la Privacy Policy;
- la Cookie Policy.
- un banner per il consenso ai Cookies, secondo le finalità per cui vengono utilizzati e gli orientamenti del Garante Privacy di volta in volta espressi

3.7.1 La sezione privacy del sito web istituzionale

Qul è il contenuto minino della sezione privacy del sito web istituzionale?

- tutte le informazioni relative all'attività di conformità svolta dal Comune di Rimini in merito alla protezione dei dati personali;
- tutte le informazioni utili agli Interessati al trattamento dei dati personali;
- la Privacy Policy del sito, che si concreta in un'informativa redatta ai sensi degli articoli 13 e 14 del Regolamento UE 2016/679, cui si aggiunge una descrizione delle peculiarità dei dati personali trattati dal sito web (es. indirizzo IP), collocata nel footer di ciascuna pagina web del sito

3.7.2 La Cookie Policy

La Cookie Policy spiega nel dettaglio le tipologie e il funzionamento dei cookie presenti sul sito web istituzionale.

Cosa sono i cookie?

- Un cookie è un'informazione che un sito web comunica ad un browser durante la navigazione del sito stesso. Questa informazione viene memorizzata sul computer e permette di migliorare le prestazioni di navigazione. Tecnicamente, si tratta di una porzione (o stringa) di codice che assiste il titolare di un sito web nella corretta e più efficiente erogazione del servizio oltre che importanti e diverse funzioni tra cui il monitoraggio di sessioni, la memorizzazione di informazioni su specifiche configurazioni riguardanti gli utenti che accedono al server, l'agevolazione nella fruizione dei contenuti online o per tenere traccia delle informazioni utilizzate per la compilazione di un modulo informatico.

Esistono diverse tipologie di cookie:

- di prima parte
- di terze parti
- tecnici
- analitici
- di profilazione

- di sessione
- persistenti

Alcuni cookie richiedono il consenso esplicito dell'utente.

All'accesso al sito web dell'Ente viene inserita una maschera di preferenza dei cookies, sulla base delle indicazioni fornite dal Garante per la protezione dei dati tramite apposite Linee Guida.
Laddove il sito utilizzi cookie analitici di terze parti e cookie di profilazione di prima parte o di terze parti viene inserito nella pagina web un banner per acquisire il consenso, strutturato secondo le modalità indicate dal Garante Privacy.

3.7.3 I servizi aggiuntivi

Nel caso in cui il Comune eroghi servizi aggiuntivi a quelli strettamente connessi alle proprie finalità istituzionali e siano presenti campi compilabili, come quelli inseriti nella sezione "Contatti" o "Newsletter", ciascun campo contiene la richiesta dei soli dati strettamente necessari e il consenso ove applicabile in relazione al servizio erogato (Newsletter).

Ad esempio

Non richiedere l'indirizzo di residenza o il domicilio, il codice fiscale o il luogo di nascita se non necessari per le finalità del servizio

Nella pagina in cui sono presenti i campi compitabili è inserita una breve e specifica informativa privacy che qualifica la natura del servizio ed evidenzia la relativa acquisizione del consenso ai fini della sua erogazione, in assenza del quale il servizio non può essere reso.
L'utente contrassegna con una spunta (cd *flag)* la dicitura 'ho letto l'informativa privacy' prima di poter accettare la sottoscrizione del servizio aggiuntivo erogato dall'Ente.

3.8 L'IMPIEGO DI STRUMENTI DIGITALI CHE ELABORANO IMMAGINI

Laddove il Comune di Rimini si avvalga di strumenti digitali che permettano la raccolta e l'elaborazione di informazioni sul territorio, anche tramite trattamento di immagini, il Dirigente delegato:

- individua la base giuridica che legittimi il trattamento in relazione alle funzioni proprie dell'ente locale e verifica la necessarietà di una DPIA informando sia il RDP/DPO che il Referente GDPR dell'Ente;
- verifica se il trattamento rientri nelle casistiche di cui all'art. 36 del Regolamento (UE) 2016/679 per la richiesta di consultazione preventiva al Garante Privacy.

Sicurezza urbana

In relazione alle finalità di sicurezza urbana la Polizia Locale adotta apposito Regolamento di videosorveglianza urbana che definisce i ruoli e i reciproci accordi con le forze dell'ordine chiamate a svolgere attività di pubblica sicurezza, e che disciplina le modalità di impiego degli strumenti finalizzati alla sicurezza urbana nel Comune di Rimini (ad esempio, fototrappole o *bodycam*).

Formazione specifica

Agli incaricati del trattamento del Comune di Rimini che impiegano strumenti digitali che permettano la raccolta e l'elaborazione di informazioni sul territorio, anche tramite trattamento di immagini, viene somministrata apposita formazione.

3.8 Gli strumenti organizzativi dell'Ente in materia di protezione dei dati

Il Regolamento UE 2016/679 impone la tenuta di alcuni strumenti organizzativi finalizzati a garantire l'*accountability* del Titolare o del Responsabile del trattamento dei dati:

> Registro dei trattamenti dati da parte del Titolare
>
> Registro dei trattamenti dati in qualità di Responsabile
>
> Registro degli incidenti informatici e di *data breach*

Il Comune di Rimini decide di prevedere anche un

> Registro relativo all'esercizio dei diritti degli interessati

Tali registri vengono istituiti e mantenuti non solo per garantire un miglior presidio dei processi che si svolgono all'interno di ciascun Servizio, ma anche per governare più adeguatamente i processi in cui intervengono soggetti esterni.

La gestione e la tenuta dei registi adottati dall'Ente in materia di protezione dei dati personali e di sicurezza informatica degli stessi viene regolata tramite apposito documento da adottarsi contestualmente o successivamente al presente Modello organizzativo, e costituente parte integrante dello stesso.

A seguito dell'adozione del presente Modello i trattamenti relativi ai dati sensibili e giudiziari definiti nel "Regolamento per il trattamento dei dati sensibili e giudiziari", approvato con deliberazione di Consiglio comunale del 15 dicembre 2005, n. 168, e con esso l'allegata lista di tutti i trattamenti effettuati dall'Ente alla data di approvazione di tale Regolamento, confluiscono nel Registro dei trattamenti dati del Comune-Titolare.

4.1 IL TRATTAMENTO DEI DATI PERSONALI NELLA GESTIONE DOCUMENTALE DELL'ENTE

La gestione documentale all'interno del Comune di Rimini, relativamente alla formazione, registrazione, classificazione, fascicolazione, archiviazione e conservazione, è disciplinata da apposito Manuale redatto dal Responsabile del servizio archivistico, nominato ai sensi dell'art. 61 del DPR n. 445/2000, in collaborazione con il Responsabile della transizione digitale di cui all'art. 17 del d.lgs. n. 82/2005 e con il Referente GDPR.

Il Manuale di gestione documentale contiene anche previsioni relative alla protezione dei dati personali e alla circolazione di essi nella gestione documentale interna ed esterna all'Ente, cui tutti i dipendenti sono chiamati ad adeguarsi. In ogni caso, il trattamento dei dati relativi alla gestione documentale avviene in aderenza al presente Modello organizzativo, strutturato sui principi del GDPR. In particolare, il trattamento di dati personali avviene tramite adeguate misure tecniche e organizzative previste dal GDPR, tra cui la pseudonimizzazione, che consente il trattamento e la conservazione di informazioni in una forma tale da impedire l'identificazione dell'utente, senza l'utilizzo di informazioni aggiuntive. A tal fine, i dati e le informazioni aggiuntive devono essere materialmente o digitalmente conservati in differenti documenti o zone, al fine di impedire un facile ricongiungimento.

4.1.1 Gli atti amministrativi

Sin dalla fase di redazione di atti e documenti, i dati personali da utilizzare vengono selezionati secondo le disposizioni previste dal Manuale sulla gestione documentale del Comune di Rimini, in aderenza ai principi stabiliti dal GDPR e dal d.lgs. n. 196/2003, così come modificato dal d.lgs. n. 101/2018 in materia di Pubblica Amministrazione.

In ogni caso, laddove si proceda alla formazione di un atto amministrativo o di un documento, considerando come tale sia il testo che l'oggetto e gli allegati parte integrante, è necessario:

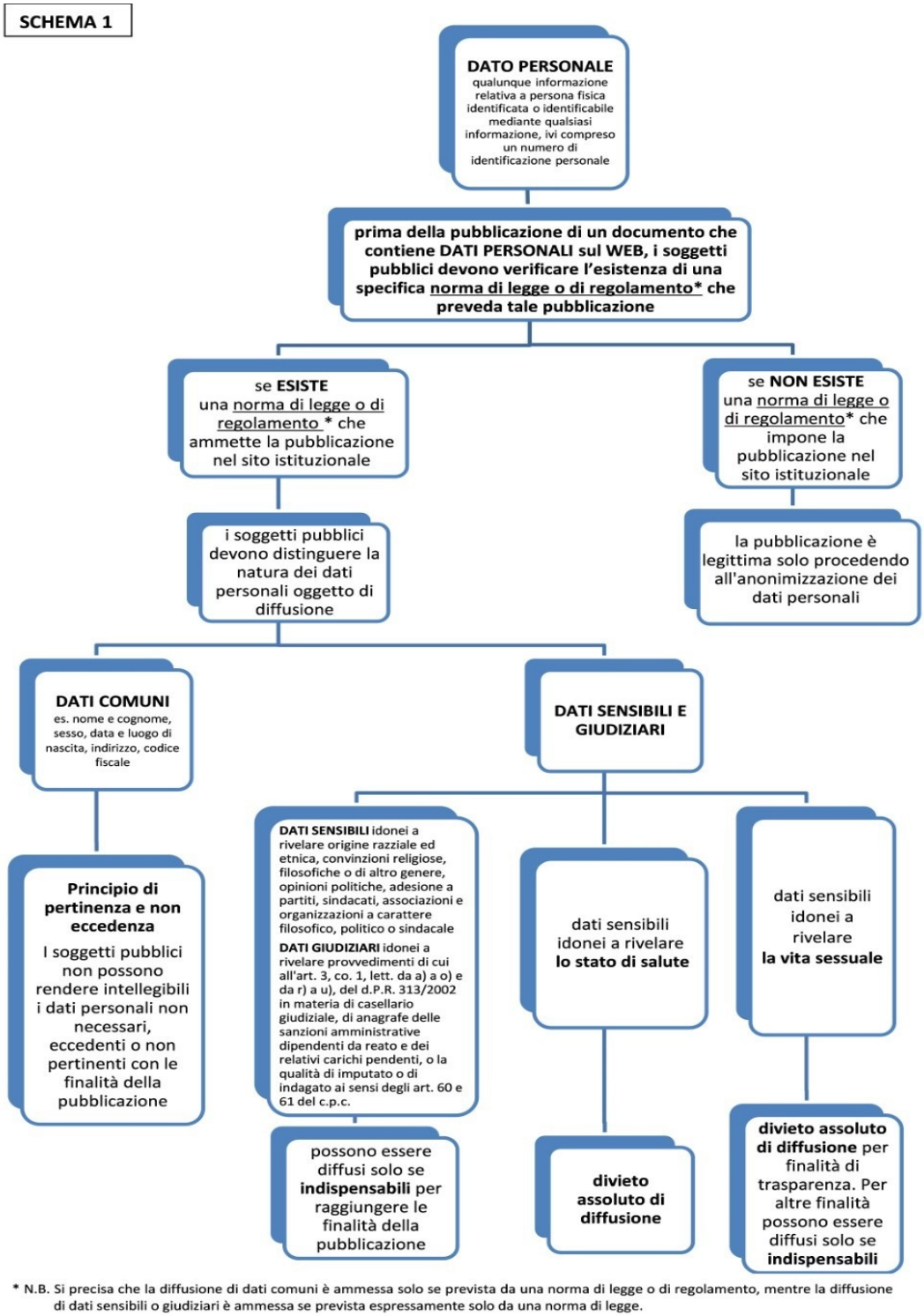
- individuare il presupposto di legge o di regolamento in base al quale viene redatto l'atto o il documento, e se esso sia destinato alla pubblicazione o meno;
- verificare il presupposto di legge che legittima la diffusione del dato personale contenuto nell'atto o nel documento;
- ridurre al minimo l'impiego di dati personali, indipendentemente dalla pubblicazione o meno dell'atto o documento. In particolare, prestare attenzione a dati personali, dati particolari, dati biometrici, dati relativi alla salute, dati giudiziari;
- trattate e diffondere i soli dati personali la cui inclusione in atti e documenti sia realmente necessaria e proporzionata al raggiungimento delle finalità perseguite dall'atto o documento;

Nei casi in cui ricorra l'obbligo di pubblicazione dell'atto amministrativo:

- selezionare i dati personali da inserire nell'atto o documento verificando, caso per caso, se ricorrono i presupposti per la minimizzazione o per l'oscuramento di essi.
- laddove oscurati i dati personali, produrre una copia del documento da conservare agli atti dell'ufficio, dentro il quale sia riportato il testo per esteso;
- esporre i soli dati necessari per raggiungere le specifiche finalità perseguite con la pubblicazione on line dei documenti e degli atti amministrativi, normativamente previste;
- assicurare il rispetto delle specifiche disposizioni di settore che individuano circoscritti periodi di tempo per la pubblicazione di atti e provvedimenti amministrativi contenenti dati personali, rendendoli accessibili sul proprio sito web istituzionale solo per l'ambito temporale individuato dalle disposizioni normative di riferimento, anche per garantire il diritto all'oblio degli interessati (es. art. 124, del d. lgs. 18 agosto 2000, n. 267, riguardante la pubblicazione di deliberazioni sull'albo pretorio degli enti locali per quindici giorni consecutivi);
- sottrarre all'indicizzazione i dati personali una volta trascorso il periodo di pubblicazione previsto dalla legge.

Si riporta di seguito uno schema prodotto dal Garante Privacy a supporto del percorso di valutazione circa la pubblicazione di atti e documenti.

SCHEMA 1



* N.B. Si precisa che la diffusione di dati comuni è ammessa solo se prevista da una norma di legge o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di legge.

Schema tratto dalle "Linee guida 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" [doc. web n. 3134436]

Regole per la conservazione

- La conservazione di atti e documenti avviene secondo le regole stabilite nel Manuale sulla gestione documentale del Comune di Rimini.
- Il tempo di conservazione di atti e documenti è imposto dalla natura e dalle funzioni di ciascuno di essi.

4.2 ATTI E DOCUMENTI AFFERENTI PROCEDURE PUBBLICHE

In relazione alla gestione di atti e documenti afferenti procedure pubbliche si applicano le regole generali stabilite dalla legislazione vigente:

- Regolamento UE 2016/679
- D.lgs. n. 196/2003
- Regole di funzionamento contenute nel presente Modello Organizzativo
- Specifiche procedure sull'acquisto di beni e servizi definite in apposito Regolamento comunale

Indicazioni circa la gestione di atti e documenti afferenti procedure pubbliche

- Predefinire in sede di gara clausole di protezione dei dati personali, compresi eventuali accordi sui ruoli, sulle modalità tecniche di scambio dei dati e le caratteristiche di accessibilità degli strumenti informatici
- Inserire quale elemento di valutazione dell'offerta tecnica di gara la presenza di adeguate garanzie di protezione dei dati personali, anche in relazione ai requisiti di sicurezza adottati dal Comune, considerata la dimensione aziendale del fornitore, provata anche tramite eventuale certificazione ex art. 42 GDPR
- In relazione ai verbali delle procedure concorsuali e di aggiudicazione viene prodotto un documento omissivo dei dati personali, quali la firma dei commissari,

e un documento contenente tali dati. Nel primo viene indicata la presenza di un documento originale, contenente dati personali, tenuto agli atti dell'ufficio

4.3 CONSERVAZIONE E DISTRUZIONE DEI DOCUMENTI CONTENENTI DATI PERSONALI

La conservazione, cancellazione e distruzione dei dati personali segue le previsioni normative in materia di scarto, selezione e riordino dei documenti e le regole stabilite dal Manuale sulla gestione documentale e dal manuale di conservazione e scarto documentale dell'Ente, anche in relazione alle forme e al supporto in cui sono incorporati

Tempi di conservazione

Regolamento (UE) 2016/679 - art. 5, par. 1, lett. e)

I dati personali vengono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Condizioni per estendere i tempi di conservazione dei dati personali

Regolamento (UE) 2016/679 - art. 89, par. 1

I dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal GDPR a tutela dei diritti e delle libertà dell'interessato.

Misure per la distruzione

Tra le misure adeguate al trattamento in deroga per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, vi è la pseudonimizzazione.

Al fine di tutelare adeguatamente gli interessati, ciascun Dirigente delegato verifica periodicamente che la conservazione dei dati personali sia giustificata, e procede all'eventuale distruzione di essi secondo quanto indicato dalle previsioni normative in materia di scarto, selezione e riordino dei documenti e le regole stabilite dal Manuale sulla gestione documentale dell'Ente; in tal caso garantisce l'effettiva e definitiva

eliminazione dei dati personali da parte di tutti i Servizi dell'Ente. Dell'avvenuta attività di rilevazione periodica viene dato conto nel monitoraggio semestrale predisposto e somministrato dal Referente GDPR.

Comune di Rimini

SICUREZZA

5.1 VALUTAZIONE DEI RISCHI

Ciascun trattamento di dati personali viene impostato in maniera predefinita, in conformità ai principi fissati dall'art. 5 GDPR, allo scopo di individuare le misure tecniche e organizzative adeguate alla protezione dei dati personali e alla loro libera circolazione, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

Ciò comporta una preventiva valutazione di tali rischi, che si presentano, in particolare, se:

il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo

gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano

sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza

in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali

sono trattati dati personali di persone fisiche vulnerabili, in particolare minori

il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati

Modalità per effettuare la Valutazione dei rischi

Per la valutazione dei rischi dei propri trattamenti di dati personali il Comune di Rimini adotta il modello di analisi predisposto dall'European Union Agency for Cybersecurity (ENISA - Agenzia dell'Unione Europea per la Cybersicurezza) con il contributo del Garante per la Protezione dei Dati Personali.

Nella valutazione del rischio il Dirigente delegato procede come segue:

a) accede allo strumento digitale prescelto dal Comune di Rimini

b) inserisce tutte le informazioni richieste dalla piattaforma, che guidano l'utente ad una corretta rilevazione e valutazione dei rischi

c) definisce l'entità del rischio, le misure da adottare e i rischi residui da accettare, in ragione della fisiologica impossibilità di azzerare completamente il rischio

d) conserva nelle pratiche relative al GDPR il report finale

e) informa gli incaricati del trattamento delle misure definite e dei rischi residui

L'entità finale del rischio viene determinata dalla combinazione di tre fattori:

1. probabilità del rischio stesso: da altamente probabile a improbabile
2. gravità del danno derivante dal rischio: da gravissimo a trascurabile
3. fattori di mitigazione. Si tratta di tutte le misure messe in atto per prevenire ed eventualmente ridurre il rischio: insufficienti, minime o adeguate

Quando fare la valutazione dei rischi

In ragione di tale modello di analisi dei rischi ciascun Dirigente delegato effettua l'analisi preventivamente all'avvio di ogni nuovo trattamento dati

.

5.2 VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI (DPIA)

Normativa

Regolamento (UE) 2016/679 - art. 35

Laddove vengano rilevati trattamenti di dati personali che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il dirigente delegato conduce una valutazione d'impatto sulla protezione dei dati (c.d. DPIA-*Data Protecion Impact Assessment*), al fine di determinare i pericoli che gravano su tali diritti e libertà delle persone fisiche e le relative conseguenze, stimando la gravità di tale rischio ed individuando le misure da adottare.

Ex Gruppo di Lavoro Articolo 29 per la Protezione dei Dati (oggi, Comitato Europeo per la Protezione dei Dati) - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679

La valutazione d'impatto sulla protezione dei dati va effettuata "prima del trattamento" (articolo 35, paragrafi 1 e 10, considerando 90 e 93). Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78).

La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento.

Realizzare una valutazione d'impatto sulla protezione dei dati è un processo continuo, non un esercizio una tantum.

Se il trattamento è esternalizzato

Qualora il trattamento sia esternalizzato, in tutto o in parte, tenuto conto della natura del trattamento stesso e delle informazioni a disposizione del responsabile del trattamento, il Dirigente delegato gli richiede assistenza tramite istruttoria documentata.

5.2.1 I presupposti e le modalità di una DPIA

L'esecuzione di tale analisi spetta a ciascun Dirigente delegato, anche con il supporto del Referente GDPR, di concerto con il Responsabile dei sistemi informativi dell'Ente. Il Dirigente delegato informa il RPD/DPO all'avvio della DPIA.

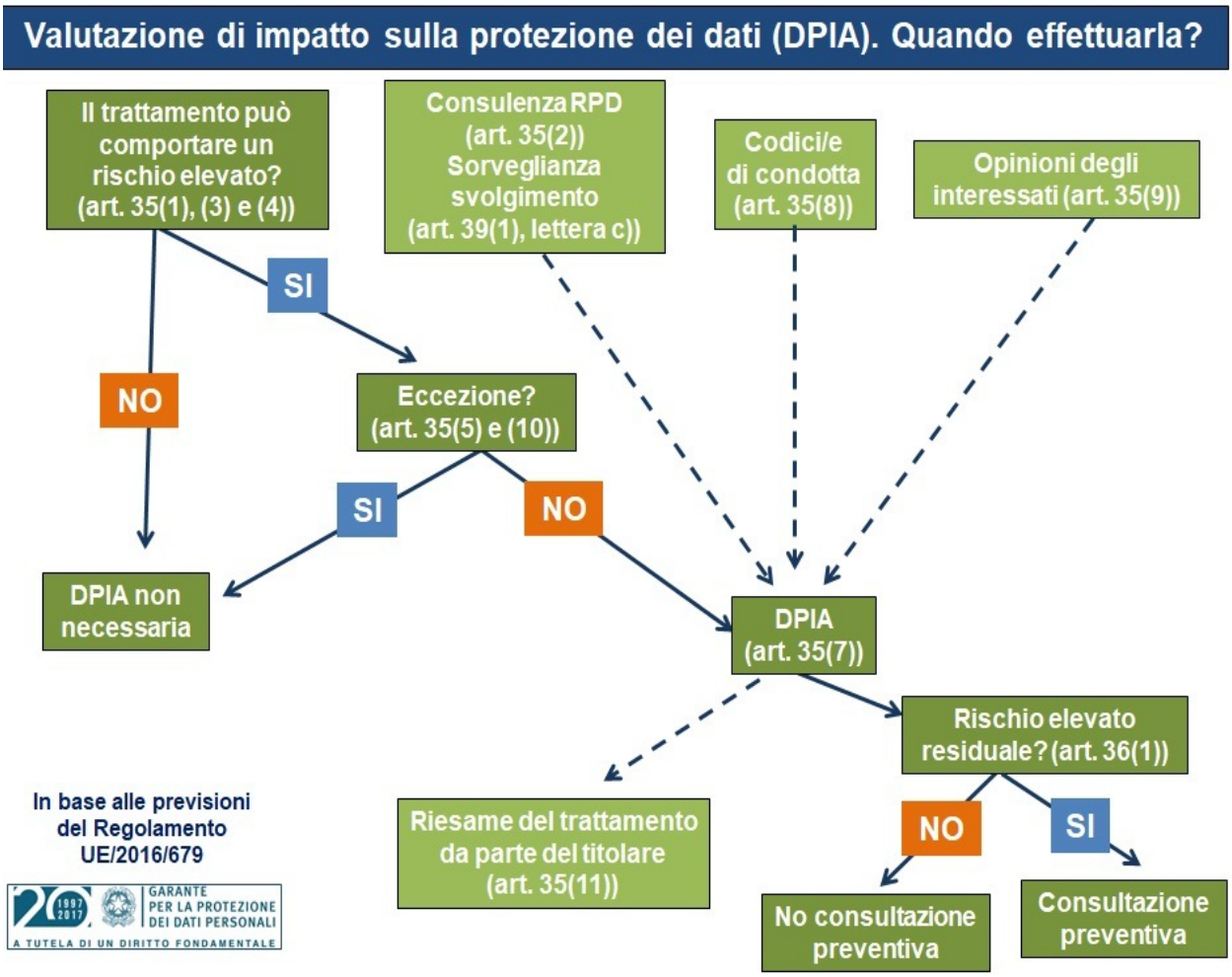
Modello per l'esecuzione della DPIA

La DPIA viene condotta sulla base del modello predisposto dalla Commissione nazionale per l'informatica e le libertà (CNIL), Autorità Garante per la Protezione dei dati in Francia, tramite lo strumento digitale prescelto dal Comune di Rimini.

La valutazione di impatto:

1. viene effettuata prima dell'inizio del trattamento, e precisamente nella fase in cui esso viene ideato e progettato, ma può essere condotta anche a seguito di data breach, laddove il Dirigente delegato valuti necessario approntare ulteriori o nuove misure di protezione dei dati in merito ai quali si è verificata la violazione.
2. per i trattamenti già in essere la DPIA viene condotta allo scopo di correggere il processo organizzativo per una maggiore tutela dei diritti e delle libertà connessi ai dati personali degli Interessati
3. viene garantito l'aggiornamento dell'analisi nel corso del tempo, qualora ad esempio cambino le caratteristiche del trattamento o i mezzi utilizzati per farlo
4. può avere ad oggetto uno o più trattamenti che presentino analogie, oppure più trattamenti che fanno parte di un unico progetto
5. qualora i trattamenti dati presentino rischi elevati analoghi nel medesimo contesto di riferimento di una precedente valutazione, il dirigente può integrare ed aggiornare tale valutazione
6. nello svolgimento di una DPIA è possibile prevedere anche la raccolta delle opinioni degli Interessati o dei loro rappresentanti, qualora lo si ritenga opportuno. In tal caso, la scelta di avvalersi o meno dell'opinione degli interessati o dei loro rappresentanti viene motivata e le risultanze vengono opportunamente documentate

Di seguito si riporta lo schema di sintesi predisposto dal Garante Privacy e presente sul sito istituzionale www.garanteprivacy.it.



5.2.2 I casi in cui effettuare una DPIA

Secondo quanto indicato dal Garante Privacy, la DPIA è obbligatoria per i seguenti trattamenti, ove applicabili in relazione alle funzioni del Comune:

Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad *"aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato*"

Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)

Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi)

Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

Trattamenti su larga scala di dati aventi carattere estremamente personale: si fa 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)

Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti

Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo)

Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*). A titolo esemplificativo:

- per la valutazione o l'assegnazione di un punteggio;
- che implichino un processo decisionale automatizzato con effetto giuridico;

- per il monitoraggio sistematico;
- per il trattamento di dati sensibili o aventi carattere altamente personale;
- per il trattamento di dati su larga scala;
- per la creazione di corrispondenze o combinazioni di dati;
- per il trattamento di dati relativi a soggetti vulnerabili;
- per trattamenti che possono impedire di esercitare un diritto o avvalersi di un servizio o di un contratto

Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche

Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment)

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

Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

5.2.3 I risultati della DPIA

Al termine della valutazione d'impatto il Dirigente referente del trattamento per cui la valutazione è stata effettuata:

- redige un documento finale di analisi da firmare e protocollare
- trasmette al RPD/DPO la DPIA per un Suo parere;
- in caso di parere negativo del RPD/DPO il Dirigente delegato motiva adeguatamente l'eventuale scelta di proseguire nel trattamento;
- protocolla il parere del RPD/DPO e ne dà notizia al Sindaco tramite la stazione di protocollazione ad esso afferente.
- conserva la documentazione relativa all'istruttoria e all'adozione della DPIA
- pubblica gli estremi della DPIA sul sito istituzionale dell'Ente e informa il referente GDPR di tale pubblicazione

Durante tutti i passaggi dell'analisi e dello scambio di corrispondenza con il RPD/DPO il Dirigente delegato mantiene informato il Referente GDPR inserendolo nei destinatari

delle comunicazioni al RDP/DPO oppure trasmettendo autonome comunicazioni. In ogni caso, le comunicazioni al Referente GDPR avvengono tramite la stazione di protocollazione dedicata al GDPR.

5.2.4 Aggiornamento e Riesame

Qualora insorgano variazioni del rischio rappresentato dalle attività relative al trattamento dati di cui si è effettuata una DPIA il Dirigente delegato procede ad un riesame per valutare se il trattamento dei dati personali sia ancora conforme alla valutazione d'impatto svolta.

5.3 Incidenti informatici e Data breach del Titolare del trattamento

In cosa consiste una violazione

La violazione dei dati personali consiste nella violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati, tali da comportare una perdita di riservitezza, integrità e disponibilità degli stessi.

Procedura

Con apposito documento, da adottarsi contestualmente o successivamente al presente Modello organizzativo e costituente parte integrante dello stesso, viene disciplinata una specifica procedura che presenti i seguenti contenuti:

- Ruoli e rapporti interni per la gestione degli incidenti informatici e rapporti con i Responsabili del trattamento nel caso di incidenti informatici occorsi ai dati personali di cui il Comune è Titolare del trattamento;
- Criteri e modalità per gestire gli incidenti informatici, distinguendo quelli da cui possano derivare data breach, così come disciplinato dal GDPR;
- Modalità per registrare tutte le violazioni avvenute, e distinguere quelle eventualmente comunicate al Garante della protezione dei dati personali;
- Criteri e modalità di monitoraggio e aggiornamento della procedura definita.

In ogni caso, la procedura di gestione degli incidenti informatici si ispira ai principi di trasparenza, efficienza ed imparzialità.

Comune di Rimini

DIRITTI

6.1 Bilanciamento tra diritti fondamentali

La protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale, è un diritto fondamentale.

Carta dei diritti fondamentali dell'Unione europea – art. 8, par. 1

Trattato sul Funzionamento dell'Unione Europea - art. 16, par. 1

Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Bilanciamento

Ogni qualvolta si ponga la necessità di applicare il diritto alla protezione dei dati personali rispetto ad altri diritti soggettivi riconosciuti tali dall'ordinamento nazionale e sovranazionale occorre effettuare un bilanciamento tra essi, ovvero contemperarli tramite una valutazione caso per caso.

6.1.1 Rapporto con la trasparenza dell'attività amministrativa

Il Comune è tenuto a pubblicare sul proprio sito istituzionale i dati necessari a raggiungere le specifiche finalità di trasparenza perseguite con la pubblicazione on-line dei documenti e degli atti amministrativi.

> *Per ogni caso concreto di pubblicazione viene posto in essere un bilanciamento tra le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali, nonché la dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*

Tenuto conto dello schema 1 contenuto nella sezione Atti del presente documento, nell'ambito della pubblicazione dei documenti sul web occorre distinguere:

- ***Obblighi di pubblicazione*** **per finalità di trasparenza** (previsti dal d.lgs 33/2013)

  Note

  Tali obblighi di pubblicazione riguardano l'organizzazione e le attività delle pubbliche amministrazioni e sono esplicitati negli articoli del D.lgs. n. 33/2013

- ***Obblighi di pubblicazione*** **per altre finalità** (contenuti in altre disposizioni di settore non riconducibili a finalità di trasparenza, quali ad es. le pubblicazioni matrimoniali)

  Note

  Tutte le ipotesi di pubblicità non riconducibili a finalità di trasparenza, qualora comportino una diffusione di dati personali sono escluse dall'oggetto del decreto stesso e dall'ambito di applicazione delle relative previsioni fra cui, in particolare, quelle relative all'accesso civico (art. 5), all'indicizzazione (art. 4 e 9), al riutilizzo (art. 7), alla durata dell'obbligo di pubblicazione (art. 8) e alla trasposizione dei dati in archivio (art. 9)

- ***Pubblicazione spontanea*** **di dati da parte di ciascuna Amministrazione per finalità di trasparenza** (facoltà di cui all'art. 7bis, co. 3, d.lgs. n. 33/2013)

  Note

  Tutte le ipotesi di pubblicità non riconducibili a finalità di trasparenza, qualora comportino una diffusione di dati personali sono escluse dall'oggetto del decreto stesso e dall'ambito di applicazione delle relative previsioni fra cui, in particolare, quelle relative all'accesso civico (art. 5), all'indicizzazione (art. 4 e 9), al riutilizzo (art. 7), alla durata dell'obbligo di pubblicazione (art. 8) e alla trasposizione dei dati in archivio (art. 9)

Contemperamento tra esigenze di trasparenza, pubblicità e riservatezza

In tutti i casi di pubblicazione, nel contemperamento tra le esigenze di trasparenza e pubblicità e quelle alla riservatezza e alla tutela dell'identità personale, vanno distinti:

- **I dati personali semplici**

  Note

  Questi possono essere pubblicati solo se necessari e pertinenti alle finalità della pubblicazione

→ **I dati particolari o dati relativi a condanne penali e reati**

Note

Tali dati possono essere pubblicati se sono necessari a raggiungere le finalità della pubblicazione, e vengono resi non intelligibili i dati non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione. I dati relativi alla salute non sono oggetto di pubblicazione, mentre i dati personali idonei a rilevare l'orientamento sessuale non possono essere pubblicati, salvo che ciò non risulti indispensabile

Casi di specie

- → Nel caso in cui non sia presente una normativa di riferimento che imponga la pubblicazione, questa può avvenire solo a seguito di anonimizzazione dei dati personali presenti nel provvedimento (es. utilizzo degli *omissis* o di codici alfanumerici).
- → I dati pubblicati si intendono rilasciati come dati di tipo aperto ai sensi del d.lgs. n. 82/2005, ad eccezione dei casi in cui la pubblicazione riguardi dati personali.
- → Nella sezione 'Amministrazione trasparente' del sito web del Comune di Rimini viene esplicitato che i dati personali sono riutilizzabili in termini compatibili agli scopi per i quali sono stati raccolti e nel rispetto del GDPR.
- → All'interno di ciascuna sezione di trasparenza, laddove necessario, vengono individuati i dati del sito web soggetti a licenza d'uso, che possono essere riutilizzati a fini commerciali solo previa sottoscrizione di accordi con il Comune. A tal fine, in sede di gara l'Amministrazione sottoscrive con il fornitore una specifica clausola sulle legittime modalità di riuso dei dati oggetto di licenza, in modo che il Comune possa trattare i dati ricevuti in licenza secondo quanto concordato.

Indicizzazione dei dati

L'indicizzazione delle informazioni pubblicate sul web è prevista solo per pubblicazioni con finalità di trasparenza, ai sensi del D.lgs. 33/13. Per tutte le altre pubblicazioni non viene autorizzata l'indicizzazione tramite motori di ricerca generalisti.

I **dati particolari e quelli giudiziari** non sono riutilizzabili e sono sottratti all'indicizzazione.

Alcuni esempi

- **curricula**: non è possibile pubblicare i recapiti personali, data e luogo di nascita, codice fiscale E firma autografa per esteso, al fine di non agevolare il furto di identità.

- **dichiarazioni dei redditi**: l'obbligo di pubblicare le dichiarazioni reddituali può ritenersi assolto con la pubblicazione del quadro riepilogativo della dichiarazione dei redditi
- **compensi**: non è possibile pubblicare la versione integrale di documenti contabili, dati di dettaglio risultanti dalle dichiarazioni fiscali oppure dai cedolini dello stipendio di ciascun lavoratore, recapiti individuali e coordinate bancarie utilizzate per effettuare pagamenti.

Nell'ambito della trasparenza amministrativa si collocano l'accesso civico semplice e l'accesso generalizzato, *ex* d.lgs. n. 33/2013. L'art. 5-bis di tale decreto indica le eccezioni e i limiti all'accesso di trasparenza, specificando in particolare che:

l'accesso generalizzato è rifiutato se il diniego è necessario ad evitare un pregiudizio concreto alla tutela dei dati personali, secondo il sistema normativo di riferimento per la materia;
l'accesso generalizzato viene escluso in relazione agli archivi anagrafici e di stato civile;
l'accesso civico viene sempre escluso per i dati particolari, specialmente relativi alla salute, genetici e biometrici.

Per la pubblicazione di atti amministrativi si faccia riferimento allo schema del Garante Privacy contenuto nel Capitolo 4 del presente documento.

6.1.2 Rapporto con l'accesso agli atti amministrativi

Anche per l'accesso ad atti e documenti detenuti dalla Pubblica Amministrazione ai sensi della l. n. 241/1990 occorre compiere un bilanciamento tra i due diritti, nel caso di specie.

Riferimenti

- *Manuale per la gestione documentale dell'Ente (impostazione dei documenti by design)*

  Per permettere una maggiore capacità di definizione di ciascun caso e la determinazione del contenuto in vista delle modalità con cui esso potrebbe essere osteso a terzi.

- *Regolamenti comunali in materia di accesso documentale e civico*

  Sulla base dei criteri e modalità di esercizio del diritto di accesso disciplinato dagli appositi e vigenti Regolamenti comunali in materia di accesso documentale viene valutato il pregiudizio eventualmente derivante dalla conoscenza generalizzata e dalla pubblicità che ai dati personali implicati possa derivare.

Ostensibilità di dati e informazioni

Nell'ostensione del dato vengono considerate anche le conseguenze legate alla sfera morale, relazionale e sociale che potrebbero derivare all'interessato dalla conoscibilità da parte di chiunque del dato richiesto.

Alcuni esempi

- future azioni da parte di terzi nei confronti dell'interessato
- situazioni che potrebbero determinare l'estromissione o la discriminazione dello stesso individuo
- altri svantaggi personali e/o sociali
- l'eventuale esposizione a minacce, intimidazioni, ritorsioni o furti di identità

Le ragionevoli aspettative dell'interessato al momento in cui i suoi dati personali sono stati raccolti vengono valutate ai fini dell'ostensibilità del documento contenente il dato personale.

Per tale motivo, la somministrazione dell'informativa in fase di raccolta dei dati personali viene elaborata nella maniera più esaustiva possibile in relazione al trattamento cui possono essere soggetti i dati rilasciati all'Ente.

Al fine di valutare correttamente la richiesta di accesso a dati, documenti e informazioni del Comune occorre verificare il tipo di dato personale presente all'interno di essi. In particolare:

Dati personali semplici

Laddove presente tale categoria di dati si rende necessario l'oscuramento di essi, accertandosi che non sia possibile neppure un riconoscimento indiretto. In tal caso, è possibile concedere il solo accesso parziale.

Qualora siano indispensabili i dati personali di terzi per dare seguito alla richiesta di accesso, questi vengono coinvolti secondo quanto previsto sia dalla l. n. 241/1990 e dal D.P.R. 12 aprile 2006, n. 184 "Regolamento recante disciplina in materia di accesso ai documenti amministrativi".

Il coinvolgimento dei controinteressati è escluso in tutti quei casi in cui la richiesta di accesso abbia ad oggetto dati la cui pubblicazione è prevista dalla legge come obbligatoria. L'accesso va privilegiato rispetto al diritto alla riservatezza dei terzi quando esso sia esercitato per la difesa di un interesse giuridico, nei limiti in cui esso sia necessario alla difesa di quell'interesse.

Occorre, dunque, una valutazione, caso per caso, di ciascuna situazione giuridica che si presenta per verificare l'effettività e la concretezza del collegamento dell'accesso al documento con la dichiarata esigenza di tutela;

Dati particolari e dati relativi a condanne penali e reati

La tutela di questa categoria di dati prevale su una generica esigenza di trasparenza amministrativa.

É sempre vietato l'accesso a meno che non sia indispensabile nei casi di accesso difensivo. É necessario anche in questo caso valutare l'effettiva correlazione tra l'esercizio del diritto di difesa e la conoscenza di tali tipologie di dati.

In relazione agli studiosi e ai ricercatori, l'accesso agli atti è disciplinato anche dalle Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 il 19 dicembre 2018.

Dati particolari e dati relativi a condanne penali e reati

La tutela di questa categoria di dati prevale su una generica esigenza di trasparenza amministrativa.

É sempre vietato l'accesso a meno che non sia indispensabile nei casi di accesso difensivo. É necessario anche in questo caso valutare l'effettiva correlazione tra l'esercizio del diritto di difesa e la conoscenza di tali tipologie di dati.

In relazione agli studiosi e ai ricercatori, l'accesso agli atti è disciplinato anche dalle Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o per scopi di ricerca storica pubblicate ai sensi dell'art. 20, comma 4, del d.lgs. 10 agosto 2018, n. 101 il 19 dicembre 2018.

Accesso agli atti e ruolo del DPO

In relazione all'accesso agli atti, il RPD/DPO svolge attività di supporto ai Dirigenti delegati competenti sulle singole richieste di accesso relativamente agli aspetti di protezione dei dati personali dei soggetti controinteressati. A tal fine, il Dirigente delegato invia richiesta scritta al RPD/DPO inserendo per conoscenza il Dirigente preposto ai sistemi informativi dell'Ente.

6.2 DIRITTO DI ACCESSO AI CONSIGLIERI COMUNALI

Normativa

D.lgs. n. 267/2000 (TUEL) – Art. 43

L'articolo 43 del d.lgs. n. 267/2000 (TUEL) garantisce ai consiglieri comunali non solo l'accesso ai documenti amministrativi formati e detenuti dall'Amministrazione ma anche alle notizie ed informazioni in loro possesso utili all'espletamento del mandato elettivo.

L'esercizio di tale diritto nei confronti di documenti contenenti dati personali è consentito se strettamente necessario allo svolgimento della funzione di controllo, di indirizzo politico, di sindacato ispettivo e di altre forme di accesso a documenti riconosciute dalla legge e dai regolamenti degli organi interessati per l'espletamento di un mandato elettivo.

Tutte le richieste di accesso agli atti presentate dai consiglieri comunali seguono l'iter procedurale stabilito da apposito regolamento

Regolamento (UE) 2016/679 – Art. 5, par. 1, lett. c) (principio di minimizzazione)

Quando la richiesta di accesso riguarda categorie particolari di dati personali o dati relativi a condanne penali o a reati, il Titolare è tenuto al rispetto rigoroso del principio di minimizzazione dei dati ex art. 5, par. 1, lett. c) del GDPR, consentendo l'accesso alle sole informazioni che risultino indispensabili per lo svolgimento del mandato, sempre garantendo il rispetto di misure organizzative e di sicurezza adeguate e specifiche per la tutela dei diritti fondamentali e per gli interessi dell'Interessato.

In ogni caso, il Dirigente delegato accerta in concreto la posizione di pretesa del consigliere all'ottenimento delle informazioni di carattere personale.

6.3 DIRITTI DEGLI INTERESSATI

Nella gestione delle pratiche relative ai diritti degli Interessati il Comune di Rimini procede nel rispetto dei principi fissati dal GDPR e, in particolare, a quelli di trasparenza, efficacia ed imparzialità di cui alla l. n. 241/1990

Il Regolamento (UE) 2016/679 sancisce per gli Interessati specifici diritti nei confronti del Titolare e del Responsabile del trattamento.

Al fine di salvaguardare adeguatamente i diritti degli Interessati, con apposito documento da adottarsi contestualmente o successivamente al presente Modello organizzativo, e costituente parte integrante dello stesso, viene disciplinata specifica procedura con la quale si regolamentano le attività, i ruoli e le responsabilità che l'Ente, in qualità di Titolare dei dati trattati, pone in essere per la ricezione, la gestione e l'evasione delle richieste ricevute da parte degli Interessati nell'esercizio dei diritti di protezione dei propri dati personali, ai sensi degli artt. 15-22 del Regolamento UE 2016/679, in relazione al sistema generale di gestione documentale dell'Ente.

La procedura disciplina anche i rapporti tra il Titolare e il Responsabile del trattamento nel caso in cui la richiesta di esercizio dei diritti GDPR venisse presentata al Responsabile.

Ciascun Dirigente delegato porta a conoscenza del Referente GDPR le richieste pervenute e mantiene un registro delle stesse nonchè delle risposte evase, secondo quanto indicato nell'apposita procedura.

Comune di Rimini

SANZIONI REATI E DANNI

7. Sanzioni, reati e danni

7.1 Il danno nel GDPR

Ai sensi dell'art. 82 del GDPR, '*chiunque subisca un danno materiale o immateriale causato da una violazione del GDPR ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*'.

Il considerando n. 146 del GDPR enuncia che '*il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito.*'

Il combinato disposto dell'art. 82 e del considerando 146 conduce ad interpretare il concetto di danno nel GDPR nel senso di non escludere dal novero dei danni risarcibili quelli derivanti da una violazione di disposizioni non espressamente previste nel GDPR.

Di seguito si riportano le previsioni normative di maggiore rilievo.

7.2 Sanzioni amministrative

Il GDPR, unitamente al Decreto Legislativo 30 giugno 2003, n.196 (c.d. Codice Privacy) s.m.i., distinguono due gruppi di sanzioni di natura amministrativa:

1. *Sanzione amministrativa pecuniaria fino a 10 milioni di euro oppure, per le imprese, al 2% del fatturato mondiale annuo dell'esercizio precedente, se superiore*

In tal caso, la sanzione viene comminata laddove manchino, o siano inadeguati, i adempimenti:

GDPR	Oggetto
Art. 8	Informazione ai minori
Artt. 11, 25	Privacy by design e by default
Artt. 26, 27, 28, 29	Obblighi relativi a Titolari del trattamento e Responsabili del trattamento
Art. 30	Registri delle attività di trattamento
Artt. 31, 32 ,33, 34	Sicurezza e Notifica di data breach

Artt. 35, 36	Valutazione d'impatto sulla protezione dei dati e Consultazione preventiva
Artt. 37, 38, 39	Obblighi relativi alla figura del Data Protection Officer
Artt. 42, 43	Certificazioni

Codice Privacy	Oggetto
Art. 2-quinquies, comma 2	Informazione ai minori
Art. 2 quinquiesdecies	Trattamenti di pubblico interesse a rischio elevato
Art. 92, comma 1	Stesura e conservazione cartelle cliniche
Art. 93, comma 1	Certificato di assistenza al parto
Art. 123, comma 4	Informazioni sui dati relativi al traffico
Art. 128	Trasferimento automatico della chiamata
Art. 129, comma 2	Elenchi dei contraenti
Art. 132-ter	Informazioni sui rischi (servizi di informazione elettronica accessibili al pubblico
Art. 110, comma 1	Ricerca medica, biomedica, epidemiologica; omessa valutazione d'impatto; omessa valutazione preventiva del Garante

2. Sanzione amministrativa pecuniaria fino 20 milioni di euro o, per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore

GDPR	Oggetto
Artt. 5, 6, 7, 9	Principi di base e consenso
Artt. 12, 13, 14, 15. 16, 17, 18, 19, 20, 21, 22	Informativa e diritti degli interessati
Artt. 44, 45, 46, 47, 48, 49	Trasferimenti transfrontalieri di dati personali e inosservanza di ordini dell'Autorità

Codice Privacy	Oggetto
Art. 2-ter	Base giuridica trattamenti di pubblico interesse/esercizio di pubblici poteri
Art. 2-quater	Regole deontologiche
Art. 2-quinquies, comma 1	Consenso del minore
Art. 2-sexies	Trattamenti di dati particolari per rilevanti interessi pubblici
Art. 2-septies, comma 8	Misure garanzia per dati biometrici
Art. 2-octies	Trattamenti di dati relativi a condanne e reati
Art. 2 terdecies, commi 1,2,3 e 4	Dati relativi a persone decedute
Art. 52, commi 4 e 5	Diffusione di dati in sentenze
Art. 75	Specifiche condizioni in ambito sanitario
Art. 78	Informazioni di medico/pediatra
Art. 79	Informazioni da parte di strutture pubbliche e private che erogano

	prestazioni sanitarie e socio-sanitarie
Art. 80	Informazioni da parte di altri soggetti
Art. 82	Emergenze e tutela della salute e dell'incolumità fisica
Art.92, comma 2	Cartelle cliniche
Art. 93, commi 2 e 3,	Certificato di assistenza al parto
Art. 96	Trattamento di dati relativi a studenti
Art. 99	Durata del trattamento
Art. 100, commi 1, 2 e 4	Dati relativi ad attività di studio e ricerca
Art. 101	Modalità di trattamento (Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica)
Art. 105, commi 1, 2 e 4	Modalità di trattamento (Trattamento a fini statistici o di ricerca scientifica)
Art. 110-bis, commi 2 e 3	Trattamento ulteriore da parte di terzi dei dati personali a fini di ricerca scientifica o a fini statistici
Art. 111	Regole deontologiche per trattamenti nell’ambito del rapporto di lavoro
Art. 111-bis	Informazioni in caso di ricezione di curriculum
Art. 116, comma 1	Conoscibilità di dati su mandato dell'interessato (Istituti di patronato e di assistenza sociale)
Art. 120, comma 2	Sinistri
Art. 122	Informazioni raccolte nei riguardi del contraente o dell'utente (Comunicazioni elettroniche)
Art. 123, commi 1, 2, 3 e 5	Dati relativi al traffico (Comunicazioni elettroniche)
Art. 124	Fatturazione dettagliata (Comunicazioni elettroniche)
Art. 125	Identificazione della linea (Comunicazioni elettroniche)
Art. 126	Dati relativi all'ubicazione (Comunicazioni elettroniche)

Art. 130, commi da 1 a 5	Comunicazioni indesiderate (Comunicazioni elettroniche)
Art. .131	Informazioni a contraenti e utenti (Comunicazioni elettroniche)
Art. .132	Conservazione di dati di traffico per altre finalità (Comunicazioni elettroniche)
Art. 132-bis, comma 2	Procedure istituite dai fornitori (Comunicazioni elettroniche)
Art. 132-quater	Informazioni sui rischi (Comunicazioni elettroniche)
Art. 157	Richiesta di informazioni e di esibizione di documenti (Accertamenti e controlli)

7.3 Sanzioni penali

Per ciò che concerne le sanzioni penali, il GDPR non le disciplina direttamente. A norma dell'articolo 83, le violazioni non soggette a sanzioni amministrative pecuniarie possono essere disciplinate dal singolo Stato membro, adottando tutti i provvedimenti necessari per assicurarne l'applicazione.

Al riguardo, gli illeciti penali individuati dal Decreto Legislativo 30 giugno 2003, n.196 sono elencati nella tabella di seguito riportata.

Codice Privacy	Oggetto
Art. 167	Trattamento illecito dei dati
Art. 167-bis	Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala
Art. 167-ter	Acquisizione fraudolenta di dati personali oggetto di trattamento su larga scala
Art. 168	Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante
Art. 170	Inosservanza dei provvedimenti del Garante
Art. 171	Violazioni delle disposizioni in materia di controlli a distanza e indagini sulle opinioni dei lavoratori

7.4 Ripartizione delle responsabilità

Il Titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento che violi il GDPR, e la richiesta di risarcimento può essere proposta anche nei confronti dell'eventuale Responsabile del trattamento limitatamente all'inadempimento degli obblighi a lui imposti dal GDPR, o se abbia agito in modo difforme o in contrasto con le istruzioni ricevute dal titolare.

Il Responsabile del trattamento risponde per il danno causato dal trattamento se:

- non ha adempiuto gli obblighi del GDPR specificatamente diretti ai responsabili del trattamento;
- ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento.

Il Titolare o il Responsabile del trattamento sono esonerati dalla responsabilità se dimostrano che l'evento dannoso non gli è in alcun modo imputabile.

Qualora più Titolari del trattamento o Responsabili del trattamento, oppure entrambi, siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno causato dal trattamento, ogni Titolare o Responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Comune di Rimini

AGGIORNAMENTO E RIESAME

8.1 AGGIORNAMENTO E RIESAME

Il presente Modello organizzativo viene adottato in relazione all'assetto organizzativo del Comune di Rimini presente al momento dell'approvazione dello stesso, ma contiene una disciplina flessibile ad eventuali mutamenti della struttura, in modo che possa sopravvivere ad eventuali riorganizzazioni, salvo che non vengano apportate modifiche alla normativa europea o nazionale, o non vengano assunti ulteriori e diversi orientamenti da parte del Garante per la protezione dei dati personali nazionale ed europeo, o si manifesti la necessità di introdurre nuove politiche di gestione dei dati personali all'interno dell'Ente.

Ai fini del monitoraggio sulla conformità GDPR, il Comune potrà dotarsi di uno strumento informatico *ad hoc* che permetta a tutti i Dirigenti delegati di gestire in un unico punto tutte le relative attività di conformità. In assenza di tale strumento, tutte le attività di conformità vengono comunque garantite e tracciate da **ciascun Dirigente delegato**, che per le attività di monitoraggio produce e conserva:

- *il Registro dei trattamenti di dati personali afferente al servizio cui è delegato;*
- *l'elenco di tutti i Responsabili del trattamento nominati per il proprio Servizio di riferimento, con indicazione delle eventuali verifiche svolte sul Responsabile del trattamento;*
- *l'eventuale revisione degli accordi di fruibilità e delle modalità di accesso ai dati detenuti dal Comune di Rimini;*
- *l'eventuale revisione delle policy integrative eventualmente adottate dai singoli Dirigenti delegati per il servizio di riferimento;*
- *le informative prodotte;*
- *l'elenco degli interessati che hanno esercitato il diritto di accesso;*
- *gli esiti delle verifiche sull'avvenuta cancellazione dei dati personali da qualsiasi sistema, informatico o cartaceo, in dotazione all'Ente a seguito di richiesta da parte di Interessati;*

Il Referente GDPR dell'Ente, con l'ausilio del Coordinamento del Gruppo Privacy, fino all'adozione di un apposito strumento informatico provvede:

- ad attivare semestralmente l'aggiornamento del Registro dei trattamenti dell'Ente;

- in base alle necessità riscontrate, a sottoporre a tutti i Dirigenti delegati - audit interni, in accordo con il DPO;

- a promuovere la formazione a tutti gli incaricati , anche in collaborazione con i Dirigenti preposti alle funzioni correlate;

- a verificare in maniera continuativa l'adeguatezza e la funzionalità delle misure organizzative adottate dall'Ente all'interno del presente documento organizzativo e a valutarne l'eventuale revisione.