1. INTRODUZIONE ALLA PROTEZIONE DEI DATI PERSONALI: CONCETTI CHIAVE, QUADRO NORMATIVO E AMBITO DI APPLICAZIONE

Cosa sono i dati personali? L'indirizzo di posta elettronica di una persona? Il suo numero di telefono? Il numero della carta d'identità? L'immagine di qualcuno ripresa da una telecamera? Il fatto che una persona sia stata derubata del portafogli? La lamentela o il reclamo sporti da qualcuno al proprio Comune? Tutte queste fattispecie costituiscono dati personali. Un concetto importante è che i dati identificativi di una persona costituiscono dati personali, ma non sono gli unici.

Dati personali sono tutte le informazioni relative a una persona fisica identificata o identificabile. E quando viene identificata una persona? Quando il suo nome e cognome, il numero di cellulare, il numero di carta d'identità o qualsiasi altro dato ne permette l'identificazione.

Sono dati personali anche le informazioni relative a una persona non identificata, ma la cui identificazione è possibile. E quando è identificabile una persona? Quando se ne può determinare l'identità a partire da qualsiasi elemento, ad esempio un codice identificativo come il numero di dipendente o un luogo di lavoro con una sola persona, come la segretaria di un Comune o il controllore finanziario.

Altri concetti chiave nell'ambito della protezione dei dati sono:

- Trattamento di dati personali: qualsiasi operazione effettuata su dati personali, per procedure automatizzate o meno. Di conseguenza, si parla di trattamento anche quando una persona presenta un'istanza in formato cartaceo. È considerato trattamento di dati personali l'acquisizione degli stessi, ma anche consultazione, utilizzo o divulgazione, distruzione compresa, per cui la loro eliminazione deve avvenire in tutta sicurezza. In conclusione, un trattamento è qualsiasi azione compiuta su dati personali.

- Titolare del trattamento: persona fisica o giuridica che decide le finalità e i mezzi del trattamento. Il titolare è quindi chi decide di avviare l'acquisizione e il trattamento di dati personali in quanto li considera necessari per uno scopo.

- Responsabile del trattamento: persona fisica o giuridica che sottopone a trattamento dati personali per conto del titolare.

- Dati rientranti in particolari categorie: sono il tipo di dati personali a cui la normativa sulla protezione dei dati conferisce la massima protezione. Di questo gruppo fanno parte dati relativi all'origine etnica o razziale, opinioni politiche, religione, affiliazione a sindacati, dati genetici o biometrici, dati sullo stato di salute o quelli relativi a vita e orientamento sessuale. In relazione a tali categorie particolari di dati sussiste il divieto generale di trattamento ed esso è consentito solo in casi molto specifici.

- Pseudonimizzazione, sinonimo di anonimizzazione. La pseudonimizzazione consiste nel sottoporre a trattamento i dati in modo che essi non siano più attribuibili ad alcuno senza ulteriori informazioni, che devono essere conservate separatamente e con misure di sicurezza

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

molto rigide. Ad esempio, i poliziotti non vengono identificati con nome e cognome, ma tramite un codice.

- Dati anonimi: sono i dati il cui filo rosso tra informazioni e persona fisica è stato tagliato, pertanto l'identificazione è impossibile. La normativa sulla protezione dei dati non si applica a questi ultimi, a differenza di quanto accade con i dati pseudonimizzati, a cui è invece applicabile.

Il diritto alla protezione dei dati è contenuto nel Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, nota anche come Regolamento generale sulla protezione dei dati (GDPR). Dal maggio 2018, tutti gli stati dell'Unione Europea sono obbligati al rispetto del GDPR.

Per quanto riguarda l'ambito di applicazione, il GDPR si applica al trattamento totalmente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un fascicolo o destinati ad esservi inseriti. Il trattamento di dati automatizzati avviene tramite mezzi elettronici. Questo è il caso di documenti digitali conservati da una persona nel proprio computer. Al contrario, il trattamento non automatizzato avviene su supporto cartaceo.

Tuttavia, questa norma non si applica nei seguenti casi:

- Alle attività non comprese nell'ambito di applicazione della legislazione della UE, come ad esempio sicurezza nazionale o politica estera.
- Ai trattamenti effettuati da una persona fisica nell'esercizio di attività esclusivamente personali o domestiche (ad es. inviando un messaggio WhatsApp a un amico).
- Ai trattamenti di dati relativi a persone decedute.

Oltre a queste eccezioni, la normativa di protezione dei dati personali non si applica neanche ai trattamenti di dati relativi a persone giuridiche. Di conseguenza, un Comune, un'impresa o un consiglio di quartiere non sono titolari del diritto di protezione dei dati personali.

Dal punto di vista dell'ambito di applicazione territoriale, il GDPR dispone l'applicazione ai trattamenti di dati personali elencati di seguito:

1. Trattamenti effettuati su attività di un'entità all'interno della UE da parte del titolare o del responsabile, anche se essi hanno luogo al di fuori dell'Unione.
2. In relazione a persone interessate all'interno della UE, effettuati da un titolare o da un responsabile con sede fuori dalla UE, qualora il trattamento sia correlato all'offerta di beni o servizi rivolti a interessati all'interno della UE, ovvero se il trattamento è associato al controllo del comportamento di soggetti che si trovano nella UE, se tale comportamento ha luogo all'interno dell'Unione.
3. L'ultimo caso è relativo al trattamento di dati effettuato da un titolare con sede fuori dalla UE, ma all'interno di un luogo in cui si applica il diritto degli Stati membri della UE.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

2. PRINCIPI RELATIVI AL TRATTAMENTO DI DATI PERSONALI

I principi relativi al trattamento di dati personali sono contenuti nell'articolo 5 del Regolamento europeo e sono elencati di seguito:

- Il principio di liceità comporta che si possono sottoporre a trattamento dati personali solo se sussiste almeno una base giuridica che lo consente. Vedremo questo principio nella sezione successiva.
- Il principio di lealtà vieta l'acquisizione di dati personali con mezzi fraudolenti, sleali o illeciti. Un esempio di acquisizione sleale di dati è un sondaggio sulla soddisfazione degli utenti relativo alla qualità del servizio della raccolta differenziata, in cui l'anonimato viene garantito quando in realtà non è così, e le risposte permettono invece di risalire al partecipante al sondaggio.
- Il principio di trasparenza obbliga a informare gli interessati delle finalità della raccolta dei loro dati.
- Il principio di limitazione della finalità comporta l'acquisizione dei dati per scopi precisi, espliciti e legittimi, e che in seguito essi non possano essere trattati in modo incompatibile con dette finalità. Ciò significa che i dati raccolti per una determinata finalità non possono essere utilizzati per scopi completamente diversi. Tuttavia, non è ritenuto incompatibile il successivo trattamento dei dati personali con le finalità di archiviazione nel pubblico interesse, ricerca scientifica e storica o statistica.
- Il principio di minimizzazione dei dati prevede che i dati personali sottoposti a trattamento siano adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Ciò significa che si devono acquisire e sottoporre a trattamento solo i dati necessari alla finalità corrispondente, ed è necessario evitare di trattare dati non necessari.
- Il principio di esattezza obbliga a sottoporre a trattamento dati personali esatti e aggiornati. Pertanto, è necessario eliminare o correggere tempestivamente i dati personali inesatti o obsoleti.
- Il principio di limitazione del periodo di conservazione comporta che il periodo di conservazione dei dati che consentono di identificare un soggetto si limiti al tempo necessario per le finalità perseguite. Dopo tale periodo, si potranno conservare per fini di ricerca, statistici o di archiviazione nel pubblico interesse.
- Il principio di integrità e riservatezza obbliga a garantire una protezione adeguata mediante l'adozione di misure tecniche o organizzative appropriate, al fine di evitare che soggetti non autorizzati vengano a conoscenza dei dati o che essi vengano smarriti. In relazione a tale principio, tutto il personale è tenuto all'obbligo di riservatezza.
- Il principio di responsabilizzazione proattiva o *accountability* impone al titolare del trattamento un comportamento coerente, diligente e proattivo in merito a tutti i trattamenti di dati personali. Pertanto, il titolare è tenuto a garantire il rispetto di tutti i diritti previsti dalla

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

normativa per la protezione dei dati, ma adempiere ad essa non è sufficiente, occorre anche avere la capacità di dimostrare tale adempimento.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

3. LICEITÀ DEI TRATTAMENTI DI DATI

Ai fini della liceità del trattamento di dati personali, occorre che sussista almeno una delle basi giuridiche previste dall'articolo 6 del GDPR, descritte di seguito.

- Uno dei fondamenti o basi giuridiche che consentono il trattamento dei dati è il consenso dell'interessato che, per essere ritenuto valido, deve essere libero, specifico, informato e inequivocabile (articolo 6.1.a GDPR). Il consenso è la base giuridica che legittima l'inserimento di un modello di consulenza personalizzato mediante una piattaforma digitale di messaggistica istantanea (KAYT). Se si effettua la profilazione, il consenso deve essere esplicito. Approfondiremo la profilazione nella sezione successiva.

- Per l'esecuzione di un contratto o l'applicazione di misure precontrattuali su richiesta dell'interessato (articolo 6.1.b GDPR). Ciò permette di sottoporre a trattamento i dati dei rappresentanti delle imprese incaricate da un ente locale o di quelle che si presentano a una gara d'appalto.

- Il trattamento deve essere lecito anche quando è necessario per adempiere a un obbligo legale (articolo 6.1.c GDPR).

- Quando il trattamento è necessario per la salvaguardia di interessi vitali (articolo 6.1.d GDPR). Quest'ultima è una base giuridica secondaria, che entra in gioco solo se non è possibile il ricorso ad altre basi giuridiche e in situazioni in cui l'interessato non ha le capacità, fisiche o giuridiche, per prestare il consenso, ovvero quando il trattamento dei dati è necessario in situazioni di emergenza umanitaria, in particolare in casi di catastrofi di origine naturale o umana, oppure per il controllo di epidemie.

- Un'altra base giuridica che legittima il trattamento sussiste quando esso è necessario per esercitare un compito di interesse pubblico connesso all'esercizio di pubblici poteri conferiti al titolare (articolo 6.1.e GDPR). Questa è la base giuridica in cui rientra la maggior parte dei trattamenti di dati effettuati dagli enti pubblici e comprende la prestazione del servizio di raccolta rifiuti che permette l'identificazione degli utenti, l'adozione di un sistema di tariffazione puntuale o le operazioni di monitoraggio, controllo e ispezione. Riguardo a quest'ultimo punto, occorre sottolineare l'importanza di illustrare in modo dettagliato tutte le operazioni di questo tipo nelle relative ordinanze comunali dell'ente locale, spiegando le norme che attribuiscono tali competenze a detto ente e definendo chiaramente chi sono gli agenti che si occuperanno della loro realizzazione e con quali modalità, cosa che consentirà di stabilire i profili degli utenti che potranno sottoporre a trattamento i dati e gli effettivi trattamenti che potranno effettuare.

- Il trattamento si considera lecito anche quando è necessario per la soddisfazione di interessi legittimi del titolare o di terzi (articolo 6.1.f GDPR). Ad esempio, un'impresa che addebita costi per le chiamate di assistenza al cliente. Tuttavia, la base giuridica dell'interesse legittimo non è applicabile alle amministrazioni pubbliche durante l'esercizio delle loro funzioni.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

4. LA PROFILAZIONE

La profilazione è un trattamento di dati finalizzato alla valutazione di determinati aspetti personali di un soggetto, in particolare, all'analisi o alla previsione di aspetti relativi a preferenze personali, interessi, affidabilità, comportamento, posizione e movimenti. Ad esempio, durante la navigazione in Internet, determinati *cookie* tracciano le ricerche dell'utente per determinarne le preferenze e presentargli in tal modo inserzioni pubblicitarie personalizzate.

La gestione della tariffa PAYT per i rifiuti può comportare la profilazione comportamentale degli utenti del servizio di raccolta rifiuti. In pratica, con l'analisi dei dati generati con la prestazione del servizio e associati all'utente dello stesso mediante l'indirizzo, è possibile determinare routine o preferenze degli interessati nell'utilizzo del servizio. Ciò significa che è possibile valutare determinati aspetti del comportamento degli utenti.

La profilazione può finire per avere effetti significativi e addirittura giuridici nel caso dell'adozione di un sistema PAYT (ad esempio, nella decisione se applicare un bonus o meno) o se si usano i dati ottenuti al fine di controllare le modalità di smaltimento dei rifiuti (ad esempio, nel caso si sanzioni una separazione errata). In tali casi, detti effetti devono essere necessari per perfezionare o dare esecuzione a un contratto tra l'interessato e un titolare del trattamento che siano previsti dalla legislazione dell'Unione Europea o degli Stati membri o che si basino sul consenso esplicito.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

5. CONTRATTI DI RESPONSABILE DI TRATTAMENTO DI DATI

Quando un Comune (titolare del trattamento) ricorre a un'impresa (responsabile) per la prestazione del servizio di raccolta rifiuti, dal punto di vista della normativa per la protezione dei dati, è necessario disciplinare tale rapporto mediante un contratto o altro atto giuridico, ad esempio un accordo, che deve rispettare il contenuto minimo di cui all'art. 28.3 del Regolamento europeo sulla Protezione dei Dati, facendo riferimento tra l'altro a:

a) Oggetto, durata, natura e finalità del trattamento.

b) Tipo di dati personali e categorie di persone interessate.

c) Obblighi e diritti del titolare.

d) Istruzioni del titolare al responsabile.

Il responsabile può assegnare determinate attività a un incaricato. A tal fine, è necessario redigere un contratto tra i due con gli stessi obblighi di protezione dei dati sanciti nel contratto originario sottoscritto con il titolare. Inoltre, è fondamentale che il titolare del trattamento autorizzi il responsabile a designare un incaricato.

Ad esempio, un'impresa che gestisce il servizio di raccolta rifiuti (responsabile) che incarica un'altra impresa (incaricato) della fornitura della tecnologia necessaria per un nuovo modello di raccolta rifiuti, con la conseguenza che quest'ultima avrà accesso ai dati degli utenti del servizio.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

6. VALUTAZIONE DI IMPATTO NELLA PROTEZIONE DEI DATI

Le valutazioni di impatto relative alla protezione dei dati (DPIA), da effettuarsi **prima di iniziare il trattamento**, non sono previste per ogni tipo di trattamento di dati personali, ma solo nel caso in cui sussista un **elevato rischio** per diritti e libertà personali, per natura del trattamento, portata e contesto, finalità o uso di nuove tecnologie.

Il Regolamento europeo (GDPR) contiene una lista di trattamenti per cui è richiesta la PDIA:

a) quando la finalità è la valutazione "sistematica e completa" di aspetti della persona effettuata con mezzi automatizzati. Ad esempio, durante la profilazione con effetti giuridici, cosa che può verificarsi in determinati casi di impiego dell'intelligenza artificiale nel settore pubblico;

b) quando si sottopongono a trattamento categorie particolari di dati su larga scala, come nel caso degli ospedali, o dati relativi a condanne e reati penali; e

c) quando si effettua l'osservazione sistematica su larga scala di una zona di pubblico accesso, come nel caso di un sistema di videosorveglianza in un'infrastruttura utilizzata quotidianamente da migliaia di persone.

L'elenco di casi per cui, secondo il GDPR, occorre svolgere una PDIA per valutare se i trattamenti presuppongono un rischio elevato non è chiuso, per questo il GDPR prevede che le autorità di controllo possano pubblicare elenchi di tipi di trattamenti che richiedono una PDIA e l'elenco dei trattamenti per cui essa non è necessaria (gli elenchi pubblicati dal Garante per la protezione dei dati sono consultabili qui).

I requisiti minimi per lo svolgimento di una PDIA, qualora sia obbligatoria, sono i seguenti: descrizione del trattamento, a titolo esemplificativo ciclo di vita dei dati, finalità o base giuridica, valutazione di necessità e proporzionalità del trattamento, valutazione di rischi e misure per ridurli al minimo etc.

Se dalla valutazione di impatto risulta che il titolare riscontra ancora un rischio elevato non mitigabile o riducibile con mezzi ragionevoli in linea con la tecnologia disponibile e i costi dell'applicazione, prima di iniziare il trattamento deve consultare l'autorità di controllo, che deve consigliare il titolare, potendo anche vietare il trattamento.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

7. ALTRI OBBLIGHI

Oltre agli obblighi illustrati finora, il GDPR ne impone ulteriori al titolare del trattamento.

Il primo di questi è costituito da politiche di protezione dei dati, rispetto alle quali il GDPR non detta il contenuto. Tali politiche si configurano come una delle misure tecniche e organizzative che il titolare deve adottare e devono contenere informazioni sui trattamenti dei dati svolti dall'organizzazione, come pure gli impegni di questa in relazione alla protezione dei dati (ad esempio, identificazione di titolare e responsabile della protezione dei dati, modalità di esercizio dei diritti etc.).

L'obbligo successivo è il registro delle attività di trattamento (RAT). Il RAT ha sostituito il precedente obbligo di esibire i documenti alle autorità di controllo, scomparso con il GDPR. Gli enti pubblici come i comuni sono tenuti a redigere il Registro.

Il GDPR dispone quale deve essere il contenuto del Registro (finalità del trattamento, categorie di interessati e dati personali e descrizione generale delle misure di sicurezza tecniche e organizzative, tra le altre).

In determinati casi, anche i responsabili del trattamento possono essere tenuti a redigere il RAT, con contenuti analoghi in cui deve essere identificato anche il titolare per conto del quale essi agiscono.

Di seguito si illustra in cosa consiste la Privacy by design e la Privacy by default. Prima di tutto, la Privacy by design comporta il dovere di considerare tutti gli obblighi e i requisiti previsti dalla normativa per la protezione dei dati, dal momento in cui si progetta un nuovo trattamento. In particolare, obbliga ad adottare misure tecniche e organizzative adeguate come la pseudonimizzazione, ad applicare in modo efficace i principi della protezione dei dati e a integrare le garanzie necessarie per rispettare gli obblighi imposti dal GDPR e proteggere i diritti degli interessati. Ad esempio, se un ente locale decide di creare un canale elettronico per favorire l'adesione della cittadinanza, prima di procedere deve valutare se è necessaria l'identificazione delle persone, quali dati verranno raccolti, come se ne garantirà la sicurezza, come sarà possibile esercitare i propri diritti etc.

In secondo luogo, la Privacy by default è il principio per cui un'organizzazione (titolare del trattamento) assicura che verranno sottoposti a trattamento per impostazione predefinita (default) solo i dati strettamente necessari per ogni finalità specifica dello stesso (senza l'intervento dell'utente). Pertanto, quando una persona si iscrive a un social network, la Privacy by default implica che, senza dover configurare nulla, il profilo deve essere privato. Se però l'utente desidera che continui ad essere pubblico, deve apportare egli stesso una modifica in tal senso.

Il Regolamento europeo impone altresì di adottare misure adeguate o appropriate al fine di garantire la protezione dei dati. Per determinare quali siano le misure di protezione adeguate, è necessario effettuare un'analisi dei rischi.

Questa deve considerare i seguenti elementi: la natura dei dati (ad esempio, se vengono sottoposte a trattamento categorie particolari di dati), il numero di interessati o la mole (volume dei dati), ovvero la varietà di trattamenti (ad esempio, se è possibile la profilazione).

Il GDPR prevede che le misure di protezione possano consistere in:

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

- Riduzione al minimo del trattamento di dati.
- Pseudonimizzazione o crittografazione dei dati.
- Capacità di garantire riservatezza, integrità, disponibilità e resilienza costanti dei sistemi e dei servizi di trattamento, vale a dire, la capacità di opposizione o ripristino (ad es. in caso di attacco informatico).
- Capacità di ripristinare disponibilità e accesso ai dati personali con rapidità, in caso di incidente fisico o tecnico (ad es. con back-up).
- Procedura per verificare, valutare e monitorare regolarmente l'efficacia delle misure di sicurezza. Ciò si può conseguire, a titolo esemplificativo, con audit di dette misure.

Un altro obbligo è la comunicazione delle violazioni della sicurezza. Tale obbligo comporta che, in caso di violazione o incidente di sicurezza dei dati che comporti un rischio per diritti e libertà degli interessati, il Comune titolare del trattamento debba inviarne comunicazione all'autorità di controllo competente. Tale comunicazione deve avvenire tempestivamente, al massimo entro le 72 ore successive al momento in cui ci si è resi conto della violazione. Se invece è improbabile che la violazione costituisca un rischio per diritti e libertà delle persone, non è necessario inviare alcuna comunicazione.

Nei casi in cui sia necessario dare comunicazione all'autorità competente in quanto il rischio è probabile, se l'ente locale ritiene che la violazione della sicurezza possa comportare un rischio elevato per diritti e libertà delle persone, oltre ad avvisare l'autorità competente deve avvisare anche gli interessati e fornire loro consigli per mitigare detti rischi.

Ad ogni modo, nel caso di qualsiasi genere di incidente che possa avere conseguenze sulla sicurezza dei dati, anche in quelli che non richiedono comunicazione all'autorità, l'ente locale titolare deve documentare internamente l'incidente, annotando fatti, conseguenze e misure correttive adottate. Tale documentazione interna deve essere a disposizione dell'autorità di controllo, al fine di consentire ad essa di effettuare le verifiche del caso.

Infine, la designazione di una persona come Responsabile della Protezione Dati (RPD) è obbligatoria in alcuni casi specifici, e sempre quando il titolare o il responsabile del trattamento sono un'autorità o un organismo pubblico. Pertanto, un Comune è obbligato a disporre di un RPD. È comunque possibile designare lo stesso RPD per diversi enti.

L'RPD è il referente dell'organizzazione in materia di protezione dei dati e, tra gli altri requisiti, deve avere esperienza nel settore.

Le funzioni dell'RPD sono descritte nella normativa per la protezione dei dati. Le più rilevanti sono le seguenti:

- Informare e offrire consulenza a titolare o responsabile, così come ai loro dipendenti, sugli obblighi che devono rispettare in materia di protezione dei dati.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

È inoltre tenuto a supervisionare l'adempimento della normativa per la protezione dei dati e delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati, compresa l'assegnazione di responsabilità, la formazione e sensibilizzazione del personale e gli audit del caso.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

8. DIRITTI DELLE PERSONE A ESSERE INFORMATE

Il diritto di informazione fa parte del nucleo centrale del diritto alla protezione dei dati personali, in quanto permette di esercitare il potere di controllo o utilizzo delle persone in merito ai propri dati personali. Tale diritto di tutti a controllare le proprie informazioni personali è effettivo solo se le persone vengono preventivamente informate sugli utilizzi dei dati e su altri aspetti illustrati successivamente.

In generale, il titolare del trattamento è tenuto a rendere effettivo il diritto di informazione, anche se, qualora l'acquisizione dei dati avvenga da parte del responsabile, si può stabilire nel contratto del responsabile del trattamento che sia quest'ultimo ad assumere il compito di informare.

Se i dati vengono raccolti dallo stesso interessato, le informazioni devono essere fornite all'atto dell'acquisizione. In tali casi, le informazioni che devono essere fornite alla persone sono indicate all'art. 13 del GDPR.

Se invece i dati non vengono acquisiti dall'interessato, bensì da altra fonte (ad esempio, da un'altra amministrazione), le informazioni da fornire sono quelle di cui all'art. 14 del Regolamento europeo, che prevede che esse debbano essere fornite entro un termine ragionevole, e comunque entro un mese dal ricevimento dei dati.

Il GDPR prevede alcuni casi in cui non è necessario informare l'interessato, come nel caso in cui questi sia già in possesso di tali informazioni. Non è necessario fornire informazioni neanche qualora i dati non vengano acquisiti direttamente dall'interessato, ma da altra fonte, e la comunicazione delle informazioni risulti impossibile o comporti uno sforzo sproporzionato, ovvero se l'acquisizione o la trasmissione dei dati è prevista dalla legislazione della UE o degli Stati membri.

Per quanto riguarda il contenuto delle informazioni da fornire, nel caso di acquisizione dei dati direttamente dall'interessato, l'art. 13 del Regolamento europeo impone al titolare di informare in merito a diversi aspetti all'atto dell'acquisizione stessa: identità del titolare e modalità di contatto, dati di contatto del Responsabile della Protezione Dati, finalità del trattamento e sua base giuridica, destinatari o categoria di destinatari a cui si possono comunicare i dati, periodo di conservazione degli stessi, possibilità di esercitare i diritti illustrati successivamente, quali il diritto al ritiro del consenso, il diritto a presentare un reclamo all'autorità di controllo etc.

Pertanto, se i dati personali vengono acquisiti tramite modulo, la persona dovrà essere contestualmente informata di tutti questi aspetti.

Se i dati non sono stati acquisiti direttamente dall'interessato, l'art. 14 del GDPR indica che questi deve essere informato sulle categorie di dati di cui si tratta, la fonte, o l'origine, da cui provengono i dati personali e, qualora applicabile, se questi provengono da fonti accessibili al pubblico, come Internet.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

9. ALTRI DIRITTI ESERCITABILI DALLE PERSONE: ACCESSO, RETTIFICA, SOPPRESSIONE, LIMITAZIONE, PORTABILITÀ, OPPOSIZIONE A DECISIONI AUTOMATIZZATE

Il GDPR conferisce alle persone, in rapporto al trattamento dei propri dati personali, i seguenti diritti: accesso, rettifica, soppressione, opposizione, limitazione, portabilità e diritto a opporsi a decisioni automatizzate. Tali diritti sono personalissimi, pertanto li può esercitare solo la persona titolare dei dati, anche se tramite un rappresentante legale o volontario.

Il termine per dare risposta alla richiesta di esercizio di qualsiasi diritto è di un mese, prolungabile a due se necessario, tenendo conto della complessità e del numero di richieste. Se il titolare ritiene che la richiesta di esercizio di un determinato diritto non debba essere soddisfatta, deve comunque dare tempestivamente risposta entro il termine massimo di un mese, illustrando all'interessato i motivi del diniego. L'interessato deve essere anche informato sulla possibilità di esercitare le azioni di cui ha facoltà, in particolare, la presentazione di un reclamo all'autorità di controllo.

Di seguito si illustra ciascuno di questi diritti:

- Accesso**:** questo diritto prevede che chiunque possa sapere quali dei suoi dati saranno oggetto di trattamento da parte di un ente locale. Se una persona esercita questo diritto e il titolare sottopone a trattamento i suoi dati personali, deve fornire all'interessato una copia dei dati oggetto del trattamento, nonché altre informazioni, in gran parte coincidenti con il contenuto del diritto di informazione (finalità del trattamento, categorie di dati personali, destinatari o categorie di destinatari, periodo di conservazione previsto o criteri usati per determinarlo etc.). Il diritto a ottenere una copia dei dati non può avere conseguenze negative su diritti e libertà di terzi.

- Rettifica: con questo diritto, l'interessato può richiedere la modifica dei dati errati o il completamento di quelli incompleti. Quando si esercita questo diritto, è necessario indicare nella richiesta di rettifica a quali dati ci si riferisce e la rettifica da apportare; inoltre, è necessario eventualmente allegare la documentazione giustificativa dell'errore o del carattere incompleto dei dati oggetto del trattamento.

- Soppressione o diritto all'oblio: è il diritto dell'interessato a ottenere la soppressione dei propri dati personali in determinati casi: quando i dati non sono più necessari per le finalità perseguite, quando l'interessato ritira il consenso, se si oppone al trattamento e non prevalgono altri motivi legittimi per il trattamento, sei i dati sono stati sottoposti a trattamento illecito etc. Il Regolamento europeo elenca alcuni casi in cui tale diritto non si applica, considerando che il trattamento è necessario al fine di esercitare il diritto alla libertà di espressione e informazione, per adempiere a un obbligo legale che richiede il trattamento di dati, come nel caso in cui la conservazione di documenti contenenti dati sia imposta dalla legge, ovvero per esercitare un compito di interesse pubblico o nell'esercizio di pubblici poteri conferiti al titolare, etc.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

- Limitazione del trattamento: consente all'interessato di pretendere che i dati si possano utilizzare solo in determinati casi. In altre parole, è come sospendere il trattamento dei dati, ma senza eliminarli. Questi diritti si possono richiedere nei quattro casi riportati di seguito: quando l'interessato contesta l'esattezza dei dati personali, entro il termine che consente al titolare di verificarne la correttezza; quando il trattamento è illecito, ma l'interessato si oppone alla soppressione dei dati e, anziché sopprimerli, ne richiede la limitazione dell'uso; quando il titolare non ha più necessità di conservare i dati per le finalità del trattamento, ma l'interessato ne ha bisogno per formulare, esercitare o presentare reclami, e quando l'interessato si è opposto al trattamento in base a una situazione particolare, mentre si verifica se i motivi legittimi del titolare prevalgono su quelli dell'interessato.

- Portabilità: si può esercitare se il trattamento viene effettuato con mezzi automatizzati e se esso si basa sul consenso dell'interessato o sull'esecuzione di un contratto. Pertanto, il diritto alla portabilità non entra in gioco quando il trattamento viene effettuato dalle amministrazioni pubbliche per esercitare un compito di interesse pubblico o nell'esercizio di pubblici poteri conferiti al titolare, ovvero per l'adempimento di un obbligo legale.

  Nei casi in cui spetti questo diritto, l'interessato può chiedere la trasmissione dei propri dati a un altro titolare, oppure chiedere che i dati che ha consegnato al titolare gli vengano forniti in un formato strutturato.

- Opposizione: in virtù di questo diritto, si richiede al titolare l'interruzione di un determinato trattamento dei dati, e tale richiesta si basa su motivi correlati alla particolare situazione del richiedente, se si tratta ad esempio di una vittima di violenza di genere, un testimone sotto protezione etc.

  Questo diritto si può esercitare quando il trattamento, compresa la profilazione, si basa sull'interesse pubblico o sull'esercizio di poteri pubblici conferiti al titolare, sull'interesse legittimo perseguito dal titolare del trattamento o da un terzo, o si effettua con finalità di ricerca scientifica o storica, ovvero finalità statistiche, a meno che non siano necessari per esercitare un compito di interesse pubblico. In tali casi, il titolare deve interrompere il trattamento, a meno che non adduca motivi legittimi che prevalgono su interessi, diritti e libertà dell'interessato, ovvero a meno che il trattamento non sia necessario per formulazione, esercizio o presentazione di reclami.

- Se non è oggetto di decisioni automatizzate individuali, compresa la profilazione: nel caso delle amministrazioni pubbliche, queste decisioni possono venire adottate nei casi di trattamenti automatizzati dei dati personali, ad esempio se nella raccolta rifiuti si implementano sistemi PAYT. Tale diritto, tuttavia, non sussiste quando la decisione automatizzata è necessaria per sottoscrivere o eseguire un contratto tra l'interessato e un titolare del trattamento, quando si basa sul consenso esplicito dell'interessato o quando è autorizzato dalla legislazione della UE o degli Stati membri.

Fatta eccezione per quest'ultimo caso in cui la decisione sia autorizzata da una norma UE o degli Stati membri, il soggetto ha diritto a ottenere l'intervento umano da parte del titolare, a esprimere il suo punto di vista e a impugnare la decisione.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

10. L'AUTORITÀ DI CONTROLLO E IL SISTEMA DI GARANZIE DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

In caso di eventuali violazioni dei diritti sanciti dal Regolamento europeo sulla Protezione dei Dati o dei diritti riconosciuti alle persone, è possibile presentare un reclamo all'autorità di controllo competente.

Per quanto riguarda il regime delle sanzioni, il GDPR stabilisce due elenchi di violazioni, sanzionabili con multe che vanno dai 10 ai 20 milioni di Euro al massimo, o, nel caso di imprese, da un importo equivalente al 2% o al 4% massimo del fatturato mondiale totale annuo dell'esercizio finanziario precedente, e tra le due opzioni si deve scegliere l'importo più alto.

Nonostante ciò, il GDPR non esclude che l'ordinamento giuridico degli Stati membri possa non contemplare sanzioni amministrative.

D'altro lato, la persona che subisce danni e pregiudizi, materiali o immateriali (ad es. morali) in conseguenza di una violazione del Regolamento europeo, ha diritto a ricevere dal titolare o dal responsabile del trattamento un risarcimento da parte del Titolare o del Responsabile del trattamento per i danni e pregiudizi subiti.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

11. TRASFERIMENTI INTERNAZIONALI DI DATI

I trasferimenti internazionali di dati consentono il flusso di dati personali dal territorio di uno Stato membro a destinatari con sede in paesi fuori dallo Spazio Economico Europeo, trasferimento che può avere luogo solo nei seguenti casi:

- In paesi, territori o settori specifici in merito ai quali la Commissione Europea ha adottato una decisione che riconosce che offrono un livello di protezione adeguato.
- Quando sono state offerte garanzie adeguate sulla protezione che i dati riceveranno nella destinazione, mediante:
  - ✓ Uno strumento vincolante e avente efficacia esecutiva tra autorità e organismi pubblici.
  - ✓ Norme vincolanti d'impresa (BCR).
  - ✓ Clausole tipo di protezione dei dati adottate dalla Commissione Europea o dall'autorità di controllo competente.
  - ✓ Con l'autorizzazione dell'autorità di controllo, in base a clausole contrattuali o disposizioni inserite in accordi vincolanti tra organismi pubblici che comprendano diritti aventi efficacia esecutiva.
  - ✓ Un codice di condotta che preveda impegni vincolanti e aventi efficacia esecutiva.
  - ✓ Un meccanismo di certificazione che preveda impegni vincolanti e aventi efficacia esecutiva.
- Quando sussistono una o più delle eccezioni previste dall'art. 49 del GDPR che consentono di trasferire i dati senza garanzie di protezione adeguata, per necessità legate all'interesse del titolare dei dati ovvero a interessi generali.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.

12. CONCLUSIONI

Uno degli elementi da considerare nell'adozione di un sistema raccolta rifiuti è la protezione dei dati personali. Per quanto riguarda questo punto, è opportuno sottolineare che gli enti locali con competenze in materia di raccolta rifiuti possono sottoporre a trattamento i dati strettamente necessari.

Il trattamento di questi dati è legittimato per esercitare un compito di interesse pubblico o un esercizio di pubblici poteri. Pertanto, per la prestazione del servizio di raccolta rifiuti non è necessario acquisire il consenso dell'interessato. Nel caso in cui la raccolta rifiuti comporti profilazione con conseguenze sull'utente del servizio, come nel caso in cui si decidesse di istituire l'applicazione di bonus in base ai conferimenti individuali effettuati, è necessario il consenso dell'interessato, che la legislazione della UE o degli Stati membri preveda tale profilazione, ovvero un contratto tra interessato e titolare.

È inoltre necessario valutare se, prima di implementare il sistema di raccolta rifiuti, è possibile effettuare una valutazione di impatto relativa alla protezione dei dati, soprattutto se si svolge una profilazione nei termini illustrati, come nel caso dei sistemi PAYT.

Infine, si sottolinea che qualsiasi impresa o entità che presti un servizio a un ente locale nell'ambito della realizzazione del servizio di raccolta rifiuti che comporti l'accesso a dati personali sarà considerata responsabile del trattamento. In questo caso, sarà necessario sottoscrivere l'accordo o il contratto di responsabile del trattamento come previsto.

Il progetto REthinkWASTE ha ricevuto finanziamenti dal Programma LIFE dell'Unione Europea.
Il contenuto di questa pubblicazione è di esclusiva responsabilità di ARC e non rispecchia necessariamente l'opinione dell'Unione Europea.