



**Assemblea Territoriale d'Ambito (A.T.A.) Rifiuti  
dell'Ambito territoriale ottimale 1 – Pesaro e Urbino**

**Regolamento per l'attuazione del Regolamento UE n. 2016/679 relativo  
alla protezione delle persone fisiche con riguardo al trattamento dei  
dati personali**

**Assemblea Territoriale d'Ambito (ATA) dell'Ambito territoriale ottimale 1 - Pesaro e Urbino**

*Ente di regolazione del servizio di gestione integrata dei rifiuti urbani*

Sede: Viale XI Febbraio n. 11, 61121 Pesaro (PU) –

Cod Fisc. 92049850412

Tel. 0721 / 63 90 56 0721 – 0721 / 30 379

Web: [www.atarifiuti.pu.it](http://www.atarifiuti.pu.it) Email: [segreteria@atarifiuti.pu.it](mailto:segreteria@atarifiuti.pu.it)

Email Pec: [ata1.marche@pec.it](mailto:ata1.marche@pec.it)

## **INDICE**

- Art.1 – Quadro normativo di riferimento
- Art.2 – Oggetto e finalità del trattamento
- Art.3 – Definizioni
- Art.4 – Titolare del trattamento
- Art.5 – Responsabile del trattamento
- Art.6 – Responsabile della protezione dati
- Art.7 – Sicurezza del trattamento
- Art.8 – Registro delle attività di trattamento
- Art.9 – Valutazione d’impatto sulla protezione dei dati
- Art.10 – Violazione dei dati personali
- Art.11 – Modalità di trattamento di particolari categorie di dati personali
- Art.12 – Modalità di trattamento dei dati personali relativi a condanne penali e reati
- Art.13 – Modalità di trattamento dei dati nei servizi esternalizzati
- Art.14 – Comunicazione interna e utilizzo interno di documenti contenenti dati personali
- Art.15 – Rinvio

## **Art. 1**

### **Quadro normativo di riferimento**

1. Il quadro normativo di riferimento è costituito da:
  - 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 (RGPD);
  - D.lgs. 30 giugno 2003 n. 196 “*Codice in materia di protezione dei dati personali*” per le parti non abrogate o modificate dal d.lgs. 10 agosto 2018 n. 101;
  - D.lgs. 10 agosto 2018 n. 101 recante disposizioni per l’adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679.
2. Ai sensi dell’art. 22 comma 1 del d.lgs. 101/2018 le disposizioni del “*presente decreto e le disposizioni dell’ordinamento nazionale si interpretano e si applicano alla luce della disciplina dell’Unione Europea in materia di protezione dei dati personali e assicurano la libera circolazione dei dati personali tra gli Stati membri ai sensi dell’art. 1, paragrafo 3 del Regolamento (UE) 2016/679*”.

## **Art. 2**

### **Oggetto e finalità del trattamento**

1. Il presente Regolamento ha per oggetto le misure procedimentali e le regole di dettaglio ai fini della migliore funzionalità ed efficacia dell’attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con “RGPD”, Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, dell’ATA Rifiuti n. 1 di Pesaro e Urbino.
2. I trattamenti sono compiuti dall’Ente per le seguenti finalità:
  - l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri. Rientrano in questo ambito i seguenti trattamenti:
    - a. personale – gestione del rapporto di lavoro del personale impiegato a vario titolo presso l’Ente;
    - b. gestione dei dati relativi agli organi istituzionali dell’ATA nonché dei rappresentanti dell’Ente presso altri enti, aziende e istituzioni;
    - c. attività di comunicazione istituzionale;
    - d. attività politica, di indirizzo e di controllo, di sindacato ispettivo e inerente la documentazione dell’attività istituzionale dell’ATA;
    - e. esercizio di ulteriori funzioni amministrative per i servizi di competenza statale affidate all’Ente in base alla vigente legislazione.La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.
  - l’adempimento di un obbligo legale al quale è soggetto l’Ente. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;
  - l’esecuzione di un contratto con soggetti interessati;
  - per specifiche finalità diverse da quelle di cui alle precedenti lettere, purché l’interessato esprima il consenso al trattamento.

## **Art. 3**

### **Definizioni**

1. Ai fini del presente Regolamento, in conformità all'art. 4 del RGPD si intende per:

*Dato personale:* qualsiasi informazione riguardante una persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento ad un identificativo come il nome, il 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;

*Particolari categorie di dati personali:* si tratta dei dati c.d. “sensibili”, cioè quelli che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché dati genetici, 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;

*Dati genetici:* dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscano informazioni univoche sulla fisiologia o sulla salute di detta persona e che risultino in particolare dall'analisi di un campione biologico della persona fisica in questione;

*Dati biometrici:* dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentano o confermino l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

*Dati relativi a condanne penali e reati:* si tratta dei dati c.d. “giudiziari”, cioè quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato;

*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 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;

*Sicurezza del trattamento:* l'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

*Titolare del trattamento:* persona fisica o giuridica, autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, determini le finalità e i mezzi del trattamento di dati personali;

*Responsabile del trattamento:* persona fisica o giuridica, autorità pubblica, servizio o altro organismo che tratti dati personali per conto del Titolare del trattamento;

*Responsabile della protezione dei dati:* (RDP) persona fisica o giuridica, anche estranea

all'organizzazione del Titolare o del Responsabile del trattamento, che svolga i compiti di cui all'art. 39 del RGPD o ulteriori compiti affidatigli dal Titolare del trattamento;

*Responsabile della sicurezza informatica*: figura professionale finalizzata alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti, nonché all'amministrazione di basi di dati, di reti e di apparati di sicurezza e di sistemi software complessi;

*Data Protection Impact Assessment (DPIA)* – *valutazione d'impatto sulla protezione dei dati*: processo volto a descrivere un trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo;

*Data breach*: qualsiasi violazione di sicurezza dei dati personali che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati;

*Garante*: Autorità di controllo, ossia il Garante per la Protezione dei Dati Personali.

2. Per le altre definizioni qui non riportate o per una definizione più esaustiva si fa riferimento all'art. 4 del RGPD.

## **Art. 4**

### **Titolare del trattamento**

1. Il titolare del trattamento dei dati personali raccolti in banche dati automatizzate e/o cartacee è l'ATA Rifiuti n. 1 di Pesaro e Urbino.
2. Le attribuzioni dell'Ente quale titolare del trattamento dei dati personali sono esercitate dai suoi organi secondo la ripartizione che segue.
  - **L'Assemblea:**
    - a) emana le norme regolamentari in materia di protezione dei dati personali;
    - b) stanza nel bilancio di previsione le risorse finanziarie necessarie per l'efficiente e l'efficace esercizio delle funzioni in materia di trattamento dei dati personali;
  - **Il Presidente:**
    - a) emana le norme regolamentari in materia di ordinamento degli uffici e dei servizi utili per garantire l'efficienza dell'apparato strutturale anche in relazione alla protezione dei dati personali;
    - b) assegna al Direttore, con il piano esecutivo di gestione, le risorse necessarie all'adeguata protezione dei dati personali, anche ai fini, in carenza di professionalità interne, del supporto di specialisti esterni;
    - c) rappresenta l'Ente nei rapporti con il Garante;
    - d) designa il Responsabile della protezione dei dati personali (RPD);
    - e) sovrintende sull'osservanza delle disposizioni in materia di trattamento di dati personali;
    - f) procede alle notifiche ed alle comunicazioni al Garante;
  - **Il Direttore:**
    - a) ai sensi degli artt. 107 e 109 del d.lgs. 267/2000 esercita le funzioni dell'Ente Titolare del trattamento con le prerogative e le responsabilità che la legge e la normativa interna all'Ente gli attribuisce;
    - b) designa le persone autorizzate al trattamento. Per le operazioni di trattamento i soggetti designati devono attenersi alle istruzioni loro impartite per iscritto, le quali individuano specificatamente l'ambito del trattamento consentito;

- c) risponde dell'operato dei soggetti designati per specifiche attività di trattamento, anche ai fini del risarcimento di eventuali danni causati dal trattamento stesso, salvo dimostri che l'evento dannoso non è in alcun modo a lui imputabile;
  - d) garantisce che chiunque agisce sotto la sua direzione sia in possesso di apposita formazione ed istruzione.
- 3. I soggetti di cui al comma 2 sono responsabili, ciascuno nell'ambito di propria competenza, del rispetto dei principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.
  - 4. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Ente da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la **contitolarità** di cui all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

## **Art.5**

### **Responsabile del trattamento**

- 1. Il titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 2, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
- 2. Due condizioni sono indispensabili per configurare il ruolo di responsabile del trattamento: essere un soggetto distinto rispetto al titolare del trattamento e trattare dati personali per conto del titolare del trattamento.
- 3. Il responsabile deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 7 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.
- 4. Gli atti che disciplinano il rapporto tra il titolare ed il responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione Europea.
- 5. È consentita la nomina di sub-responsabili del trattamento da parte di ciascun responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il titolare ed il responsabile primario.
- 6. Il responsabile risponde dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.
- 7. Il responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.
- 8. Il responsabile del trattamento dei dati provvede a tutte le attività previste dalla legge e a tutti i compiti che gli sono affidati. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

- tratti i dati personali soltanto su istruzione documentata da parte del titolare del trattamento;
- garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
- adotti tutte le misure tecniche e organizzative per garantire la sicurezza dei trattamenti;
- ricorra ad un altro responsabile del trattamento solo se autorizzato dal titolare e nel rispetto di tutte le condizioni contenute nel contratto originario tra il titolare e sé medesimo;
- assista il titolare negli obblighi di cui all'art. 32 e 36 del GRPD, tenendo conto della natura del trattamento e delle informazioni a sua disposizione;
- cancelli o restituisca al titolare del trattamento tutti i dati personali dopo che è terminata la prestazione di cui al contratto e cancelli le copie esistenti;
- metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'art. 28 GRPD.

## **Art.6**

### **Responsabile della protezione dati**

1. Il responsabile della protezione dei dati (in seguito indicato con “RPD”) può essere individuato nella figura unica di un dipendente di ruolo dell’Ente, in possesso di idonee qualità professionali, ovvero (in alternativa) nel professionista esterno scelto nel rispetto delle procedure per l’affidamento dei servizi.
2. Il RPD può essere scelto fra i dipendenti dell’Ente purché in possesso di idonee qualità professionali, con particolare riferimento alla comprovata conoscenza specialistica della normativa e della prassi in materia di protezione dei dati, nonché alla capacità di promuovere una cultura della protezione dati all’interno dell’organizzazione dell’Ente. Il titolare ed il responsabile del trattamento provvedono affinché il RPD mantenga la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione. Nel caso in cui il RPD non sia un dipendente dell’Ente, l’incaricato è selezionato fra soggetti aventi le medesime qualità professionali richieste al dipendente, che abbiano maturato un’approfondita conoscenza del settore; i compiti attribuiti al RPD sono indicati in apposito contratto di servizi.
3. Il RPD è incaricato dei seguenti compiti:
  - a) informare e fornire consulenza all’Ente, nonché ai dipendenti designati per eseguire il trattamento dei dati in merito agli obblighi derivanti dalla normativa relativa alla protezione dei dati. In tal senso il RPD può indicare i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;
  - b) sorvegliare l’osservanza dalla normativa relativa alla protezione dei dati. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l’analisi e la verifica dei trattamenti in termini di loro conformità, l’attività di informazione, consulenza e indirizzo;
  - c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere nell’Ente;
  - d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il RPD viene consultato in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi alla normativa;

- e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato al Garante;
  - f) altri compiti e funzioni a condizione che questi non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.
3. Il RPD è tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.  
È reso edotto tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta oppure orale. Il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificatamente tale decisione. Il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.
4. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:
- a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
  - b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - concentrandosi sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati.
5. Al RPD sono assicurate autonomia personale nonché risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.
6. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento; in particolare, risultano incompatibili (in relazione alle dimensioni organizzative dell'Ente):
- il responsabile per la prevenzione della corruzione e per la trasparenza;
  - il responsabile del trattamento;
  - qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.
7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.  
Il RPD non può essere rimosso o penalizzato per l'adempimento dei propri compiti. Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Presidente.  
Nel caso in cui siano rilevate o sottoposte all'attenzione del RPD decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso, il medesimo è tenuto a manifestare il proprio dissenso, comunicandolo al Presidente.

## **Art. 7**

### **Sicurezza del trattamento**

1. L'Ente mette in atto misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della



natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento comprendono: la pseudonimizzazione; la minimizzazione; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
3. Costituiscono misure tecniche ed organizzative:
  - sistemi di autenticazione, sistemi di autorizzazione, sistemi di protezione (antivirus, firewall, altro);
  - misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.
4. La conformità del trattamento dei dati alla normativa è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.
5. L'Ente si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
6. I nominativi e i dati di contatto del titolare, del RPD sono pubblicati sul sito istituzionale dell'Ente nella sezione "Amministrazione Trasparente", oltre che nella sezione "Privacy" eventualmente già presente.

## **Art. 8**

### **Registro delle attività di trattamento**

1. Il registro delle attività di trattamento svolte dal titolare del trattamento reca almeno le seguenti informazioni:
  - a) il nome e i dati di contatto dell'Ente – Titolare del trattamento ed eventualmente dei controllori, dei responsabili del trattamento e del RPD;
  - b) le finalità del trattamento;
  - c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
  - d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
  - e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
  - f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
  - g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.8.
2. Il Registro è tenuto dall'Ente in forma telematica o cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.
3. Il titolare del trattamento può affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo titolare.

## **Art. 9**

### **Valutazioni d'impatto sulla protezione dei dati**

1. Nel caso in cui un tipo di trattamento, specie se prevede l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. I criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:
  - a) trattamenti valutativi, compresa la profilazione e attività predittive, concernenti 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;
  - b) decisioni automatizzate che producono significativi effetti giuridici o di analogia natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono, in modo analogo, significativamente su dette persone fisiche;
  - c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
  - d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
  - e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
  - f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
  - g) dati relativi a interessati vulnerabili, meritevoli di specifica tutela in quanto posti in una situazione di disequilibrio nel rapporto con il titolare/responsabile del trattamento, come i dipendenti dell'Ente;
  - h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
  - i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, effettuare una DPIA, salvo che il Direttore ritenga motivatamente che non può presentare un rischio elevato; lo stesso può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra, occorra comunque l'effettuazione di una DPIA.

3. Il Direttore garantisce l'effettuazione della DPIA ed è responsabile della stessa. Lo stesso può affidare l'effettuazione materiale della DPIA ad un altro soggetto, interno o esterno all'Ente. Il Direttore deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al titolare per lo svolgimento della DPIA.
4. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il Responsabile della sicurezza informatica, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al titolare per lo svolgimento della DPIA.

5. La DPIA non è necessaria nei seguenti casi:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del 25 maggio 2018 in condizioni specifiche che non hanno subito modifiche;
- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RPD e che proseguano con le stesse modalità oggetto di tale verifica.

## **Art. 10**

### **Violazione dei dati personali**

1. Per violazione dei dati personali (in seguito "*data breach*") 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 non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Ente.
2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Ogni figura coinvolta è obbligata ad informare il Presidente, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.
3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:
  - danni fisici, materiali o immateriali alle persone fisiche;
  - perdita del controllo dei dati personali;
  - limitazione dei diritti, discriminazione;
  - furto o usurpazione d'identità;
  - perdite finanziarie, danno economico o sociale;
  - decifratura non autorizzata della pseudonimizzazione;
  - pregiudizio alla reputazione;
  - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).
4. Se il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, questi devono essere informati, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:
  - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
  - riguardare categorie particolari di dati personali;
  - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati

- di localizzazione, finanziari, relativi alle abitudini e preferenze);
  - comportare rischi imminenti e con un'elevata probabilità di accadimento;
  - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).
5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.
  6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni vigenti.

## **Art. 11**

### **Modalità di trattamento di particolari categorie di dati personali**

1. L'ATA Rifiuti n. 1 di Pesaro e Urbino, generalmente, non tratta dati personali che rientrano nelle categorie di cui agli articoli 9 e 10 del RGPD. Nei casi in cui sia necessario trattare tali categorie di dati personali, l'Ente adegua il trattamento a quanto previsto dagli articoli 2-sexies, 2-septies e 2-octies del d.lgs. 196/2003 e ai citati articoli 9 e 10.
2. Il trattamento delle particolari categorie di dati personali è consentito quando si verifichi una delle seguenti ipotesi:
  - a) l'interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
  - b) il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici dell'Ente o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dalla vigente normativa nazionale e/o comunitaria o da un contratto collettivo, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
  - c) il trattamento sia necessario per la tutela di un interesse vitale dell'interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
  - d) il trattamento riguardi dati personali resi manifestamente pubblici dall'interessato;
  - e) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
  - f) il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base della vigente normativa nazionale e/o comunitaria, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
  - g) relativamente ai dipendenti dell'Ente, il trattamento sia necessario per finalità di valutazione della capacità lavorativa dei medesimi;
  - h) il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici laddove sia proporzionato alla finalità perseguita, rispetti l'essenza del diritto alla protezione dei dati e preveda misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.
3. Il Titolare/Responsabile del trattamento adottano idonee e preventive misure di sicurezza che valgono a ridurre al minimo i rischi di distruzione o perdita, anche accidentale dei dati stessi nonché di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità

della raccolta, al fine di evitare che l'Ente possa incorrere in responsabilità civile, penale, amministrativa e/o contabile.

## **Art. 12**

### **Modalità di trattamento dei dati personali relativi a condanne penali e reati**

1. Il trattamento dei “*dati personali relativi a condanne penali e reati*” deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dalla vigente normativa nazionale e/o comunitaria che preveda garanzie appropriate per i diritti e le libertà degli interessati.
2. Pertanto, il trattamento dei predetti dati è consentito solo nei limiti previsti dall'articolo 12 del presente regolamento.

## **Art. 13**

### **Modalità di trattamento dei dati nei servizi esternalizzati**

1. Nel caso in cui l'Ente affidi a soggetti pubblici o privati esterni, tramite delega o concessione o contratto lo svolgimento di compiti e/o servizi di propria competenza cui debba conseguire il trattamento di dati personali, il provvedimento o contratto di affidamento deve prevedere norme specifiche attraverso le quali si provvede:
  - a nominare il soggetto pubblico o privato ovvero la persona fisica affidatario quale responsabile del trattamento dei dati personali, ex art. 28 del RGPD, per l'intera durata dell'affidamento;
  - ad obbligare il soggetto affidatario ad osservare le prescrizioni di cui alla vigente normativa nazionale e comunitaria nonché del presente Regolamento in materia di protezione dei dati personali;
  - a consentire le verifiche sul rispetto delle predette disposizioni normative.
2. Il Direttore comunica con la massima sollecitudine al RPD l'affidamento del compito/servizio e vigila che il soggetto esterno osservi le predette prescrizioni.

## **Art. 14**

### **Comunicazione interna e utilizzo interno di documenti contenenti dati personali**

1. La comunicazione di documenti amministrativi, secondo la definizione di cui all'art. 1, comma 1, lettera a) del DPR n. 445/2000, contenenti dati personali ai componenti degli organi di governo ovvero all'interno della struttura organizzativa dell'Ente, per ragioni d'ufficio e nell'ambito delle specifiche competenze delle articolazioni interne, non è soggetta a limitazioni particolari, salvo quelle espressamente previste dalla vigente normativa.

## **Art. 15**

### **Rinvio**

1. Per tutto quanto non espressamente previsto dal presente regolamento, si rinvia alle disposizioni del RGPD e alle vigenti fonti del diritto in materia.