DETERMINA DIRETTORE GENERALE

N. 07 del 15.02.2024

OGGETTO: Trattamento dei dati personali previsto dal d.lgs. 24/2023 riguardante la protezione delle persone che segnalano violazioni del diritto dell'unione e delle disposizioni normative nazionali. Approvazione valutazione di impatto sulla protezione dei dati e modifica del registro delle attività di trattamento.

PREMESSO CHE ai sensi della L.R. n.69/2011, come modificata in ultimo dalla L.R. n. 10/2018:

- A far data dal 1° gennaio 2012 è stata istituita l'Autorità per il servizio di gestione integrata dei rifiuti urbani Ato Toscana Sud quale ente rappresentativo di tutti i Comuni appartenenti all'ambito territoriale ottimale comprendente i comuni delle province di Arezzo, Siena e Grosseto (art. 30 e 31);
- L'Autorità ha personalità giuridica di diritto pubblico ed è dotata di autonomia organizzativa, amministrativa e contabile (art. 31);
- ai sensi dell'art. 33 della citata L.R. 69/2011 "[…], all'autorità si applicano le disposizioni di cui al titolo IV della parte I e quelle di cui ai titoli I, II, III, IV, V, VI e VII della parte II del decreto legislativo 18 agosto 2000, n.267 (Testo unico delle leggi sull'ordinamento degli enti locali)";
- Gli organi delle autorità servizio rifiuti sono l'assemblea, il direttore generale e il revisore unico dei conti (art. 34);

PRESO ATTO CHE:

- con Deliberazione dell'Assemblea n. 12 del 30.11.2023 è stato approvato il bilancio di previsione 2024-2026 dell'Autorità Ato Toscana Sud;
- con Determinazione del Direttore Generale n. 140 del 27.12.2023 è stato approvato il Piano Esecutivo di Gestione (PEG) 2024-2026;

CONSIDERATO CHE al sottoscritto è stato affidato l'incarico di Direttore Generale dell'Autorità Ato Toscana Sud con delibera di Assemblea n. 24 del 06.07.2022, perfezionato con contratto stipulato con il Presidente dell'Assemblea il 12.09.2022 a valle dell'intesa rilasciata dal Presidente della Regione Toscana;

RISCONTRATA pertanto la propria competenza all'emanazione del presente atto ai sensi dell'art. 107 del D.Lgs. 267/2000, dell'art. 10 dello Statuto dell'Autorità Ato Toscana Sud e dell'art. 18 del vigente regolamento di organizzazione dell'Ente;

DATO ATTO CHE:

- in data 15/07/2023 è entrato in vigore il D.Lgs. n. 24 del 10/03/2023 (attuativo della Direttiva UE 2019/1937), che raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti sia del settore pubblico che privato (c.d. *WHISTLEBLOWING*).
- l'ANAC, in ottemperanza all'art. 10 del D.Lgs. n. 24/2023, ha adottato, con delibera n. 311 del 12/07/2023, le "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle*

disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne";

ATTESO CHE:

- l'art. 13 del D.Lgs. n. 24/2023 rubricato "*Trattamento dei dati personali*" nel dettare la disciplina sul trattamento dei dati personali connessi al ricevimento e gestione delle segnalazioni, prescrive alcuni adempimenti in capo ai titolari del trattamento;
- il paragrafo 4.1.3 delle citate Linee Guida adottate da ANAC esplicita in modo ancor più dettagliato chi sono i soggetti interessati a cui va assicurata la tutela dei dati personali, le qualifiche dei soggetti che trattano i dati personali, i principi da rispettare e le attività da compiere al fine di ossequiare detti principi;

RICORDATO CHE nell'ambito dell'attività di compliance in materia di procedimenti di whistleblowing l'Ente ha espletato le seguenti azioni:

- con delibera dell'Assemblea n. 10 del 29/09/2023 è stato approvato il Disciplinare per la gestione delle segnalazioni di illeciti-whistleblowing;
- l'Ente ha istituito un proprio canale informatico e telefonico per la ricezione delle segnalazioni (piattaforma WHISTLEACTA di Actainfo);
- il fornitore della piattaforma informatica è stato nominato quale Responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR 2016/679;
- il personale incaricato della gestione delle segnalazioni è stato autorizzato al trattamento dei dati ed è stato formato;
- è stata redatta e pubblicata sul sito istituzionale l'informativa sul trattamento dei dati personali;

DATO ATTO CHE tra gli ulteriori adempimenti previsti dall'art. 13 del D.Lgs. 24/2023 sono i seguenti:

- approvazione del documento di valutazione di impatto sulla protezione dei dati personali (DPIA);
- aggiornamento del Registro delle attività di trattamento;

CONSIDERATO CHE l'ente ha approvato il Registro delle attività di trattamento dei dati personali con Determinazione del Direttore Generale n. 73 del 15.06.2023;

VISTI i contenuti della DPIA e del nuovo "*Registro delle attività del trattamento*" e ritenuto di condividerne le risultanze ("**Allegato n. 1 e n. 2**");

VISTO il parere positivo rilasciato dal DPO con nota assunta agli atti in data 08/11/2023 prot. n. 4219, riguardo all'adozione della presente valutazione d'impatto ("**Allegato n. 3**");

VISTO il documento "DOCUMENTAZIONE A SUPPORTO DEL TITOLARE DEL TRATTAMENTO PER LA VALUTAZIONE DI IMPATTO DEI DATI TRATTATI CON IL SOFTWARE" trasmesso da Actainfo srl il 15.01.2024 e assunto al protocollo dell'ente n. 239/2024;

DETERMINA

1. Le premesse formano parte integrante e sostanziale del presente atto.
2. di approvare:
- il documento di valutazione di impatto sulla protezione dei dati personali (DPIA), (Allegato n. 1);
- il Registro delle attività di trattamento istituito con Determina dello scrivente n. 73/2023 ("Allegato n. 2");
3. di dare atto che le misure di sicurezza individuate nella DPIA sono state adottate dalle strutture organizzative dell'Ente;
4. di dare atto che il vigente Registro delle attività di trattamento dell'Ente, approvato con Determinazione del Direttore Generale n. 73 del 15.06.2023, è sostituito da quello approvato con il presente atto;
5. di prendere atto del parere positivo rilasciato dal DPO con nota assunta agli atti in data 08/11/2023 prot. n. 4219, riguardo all'adozione della presente valutazione d'impatto ("Allegato n. 3");
6. di prendere atto del documento "DOCUMENTAZIONE A SUPPORTO DEL TITOLARE DEL TRATTAMENTO PER LA VALUTAZIONE DI IMPATTO DEI DATI TRATTATI CON IL SOFTWARE" trasmesso da Actainfo srl il 15.01.2024 e assunto al protocollo dell'ente n. 239/2024;
7. di trasmettere il presente atto:
   a) al Dirigente dell'Area Amministrativa ed al personale dipendente;
   b) al Responsabile della Protezione dei Dati dell'Ente;
   c) al Responsabile del procedimento di Pubblicazione per la pubblicazione dello stesso:
      - all'Albo pretorio *on-line* per la durata di 15 gg. consecutivi;
      - nella sezione "*Privacy*" presente sul sito istituzionale dell'Ente.

IL DIRETTORE GENERALE
Ing. Enzo Tacconi (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

AUTORITA' PER IL SERVIZIO DI GESTIONE INTEGRATA DEI RIFIUTI URBANI ATO TOSCANA SUD

Visto di regolarità contabile attestante la copertura finanziaria

(D.lgs. 18.08.2000, n.267 art. 153)

Si attesta la copertura finanziaria della spesa prevista dalla presente determinazione ai sensi dell'art. 153 e la compatibilità del programma dei conseguenti pagamenti con i relativi stanziamenti di cassa.

Data _____

IL DIRIGENTE DELL'AREA
AMMINISTRATIVA E CONTABILE
Marco Morgione (*)
(*) *Documento amministrativo informatico sottoscritto con firma digitale ai sensi dell'art.24 del D.Lgs. 82/2005*

ORIGINALE IN FORMATO ELETTRONICO CON FIRME DIGITALI Le firme, in formato digitale, sono state apposte sull'originale elettronico del presente atto ai sensi dell'art. 24 del D.Lgs. 7/3/2005 n. 82 e s.m.i. L'originale elettronico del presente atto è conservato negli archivi informatici dell'ATO Toscana Sud ai sensi dell'art. 22 del D.Lgs. 7/3/2005 n. 82.

AUTORITA' PER IL SERVIZIO DI GESTIONE INTEGRATA DEI RIFIUTI URBANI ATO TOSCANA SUD

Documento di Valutazione di impatto sulla protezione dei dati (DPIA - *DATA PROTECTION IMPACT ASSESSMENT*)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "*possa presentare un rischio elevato*".

REDAZIONE del documento

Titolare del trattamento:
Titolare del trattamento dei dati è l'Autorità per il servizio di Gestione dei Rifiuti Urbani ATO Toscana Sud, nella persona del Direttore Generale (Legale Rappresentante)
E-mail: segreteria@atotoscanasud.it
PEC: segreteria@pec.atotoscanasud.it

Responsabile della protezione dei dati (RPD/DPO):
Avv. Marco Giuri
Sede
Via della Pace, 37, int. 9 – Località Renaccio – 53100 SIENA

Data
Settembre 2023

MOTIVAZIONE DELLA VALUTAZIONE

In data 30/03/2023 è entrato in vigore il D.Lgs. n. 24 del 10/03/2023 (attuativo della Direttiva UE 2019/1937), che raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti ed alle persone menzionate e coinvolte nella segnalazione sia del settore pubblico che privato. Ne consegue una disciplina organica e uniforme finalizzata a una maggiore tutela del whistleblower, in tal modo, quest'ultimo è maggiormente incentivato all'effettuazione di segnalazioni di illeciti nei limiti e con le modalità indicate nel decreto.

L'ANAC, in ottemperanza all'art. 10 del D.Lgs. 24/2023, ha adottato, con **delibera n. 311 del 12/07/2023,** le Linee Guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Le disposizioni, ivi previste, per i soggetti del settore pubblico hanno effetto dal 15 luglio 2023.

L'art. 13 del D.Lgs. 24/2023 detta la disciplina sul trattamento dei dati personali relativi al ricevimento e gestione delle segnalazioni prescrivendo alcuni adempimenti in capo ai soggetti di cui all'art. 4 ed il paragrafo 4.1.3, avente il medesimo oggetto, esplicita in modo ancor più dettagliato chi sono i soggetti interessati[1] a cui va assicurata la tutela dei dati personali, le qualifiche dei soggetti che trattano i dati personali, i principi da rispettare e le attività da compiere al fine di ossequiare detti principi tra cui:

- Attivare un canale di segnalazione interno;
- Effettuare la valutazione di impatto sulla protezione dei dati;
- Rendere ai possibili interessati una informativa sul trattamento dei dati personali;
- Aggiornare il registro delle attività di trattamento;
- Adottare una procedura che illustri gli illeciti che si possono segnalare e le modalità per farlo;
- Adottare misure tecniche ed organizzative adeguate a proteggere i dati personali;
- Disciplinare il rapporto con eventuali fornitori esterni che trattano dati personali per conto dei soggetti di cui all'art. 4 del D.Lgs. 24/2023, ai sensi dell'art. 28 del GDPE 2016/679;
- Nominare e formare il personale interno incarico della gestione della segnalazione;

L'Autorità per il servizio di gestione integrata dei rifiuti urbani, ATO Toscana Sud, in ottemperanza a quanto disposto dalla nuova normativa ha eseguito le seguenti attività:

- Istituzione di un proprio canale interno attraverso l'attivazione della piattaforma WHISTLEACTA di Actainfo;
- Nomina del fornitore quale Responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR 2016/679;
- Adozione del disciplinare per la gestione delle segnalazioni di illeciti – whistleblowing;
- Nomina e formazione del personale incaricato della gestione del canale di segnalazione;

Il presente documento, alla luce di quanto sopra riportato, viene elaborato in ossequio alle nuove disposizioni normative ed ai sensi dell'articolo 35 del Regolamento UE 679/2016.

[1] La tutela dei dati personali va assicurata non solo alla persona segnalante o denunciante ma anche ad altri soggetti cui si applica la riservatezza di dati personali quali il facilitatore, la persona coinvolta e la persona menzionata nella segnalazione in quanto "interessati" dal trattamento dei dati.

L'Autorità per il servizio di gestione integrata dei rifiuti urbani, ATO Toscana Sud, con sede in Via della Pace, 37, int. 9 – Località Renaccio – 53100 SIENA, quale Ente Pubblico, ritiene, pertanto, necessario procedere ad una valutazione di impatto, sui

Trattamenti di dati personali connessi al ricevimento e gestione delle segnalazioni di illeciti

DEFINIZIONI

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato); 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 (art. 4 del Regolamento UE 2016/679).

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 (art. 4 del Regolamento (UE) 2016/679).

Titolare del trattamento: 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; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri (art. 4 del Regolamento (UE) 2016/679).

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 (art. 4 del Regolamento (UE) 2016/679).

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. Tuttavia, 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 non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento (art. 4 del Regolamento (UE) 2016/679).

Terzo: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile (art. 4 del Regolamento (UE) 2016/679).

Rischio: scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità (Linee-guida 17/EN WP248).

Gestione del rischio: l'insieme coordinato delle attività finalizzate a guidare e monitorare un ente o organismo nei riguardi di tale rischio (Linee-guida 17/EN WP248).

"*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, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*"[2].

La valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità.

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
    - "*affrontare i rischi*";
    - "*dimostrare la conformità al presente regolamento*".

In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- valutando il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio";*
- valutando i rischi: *" valutare la particolare probabilità e gravità del rischio";*
- trattando i rischi: *"attenuando tale rischio*", "*assicurando la protezione dei dati personali*" e "*dimostrando la conformità al presente regolamento*".

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del Regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori (ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.

CRITERI PER LA VALUTAZIONE DI RISCHIO E DI IMPATTO

In esplicazione di quanto detto nel presente documento, sono riportati gli elementi previsti dalla normativa vigente (art. 35, comma 7):

[2] Cfr. anche il Considerando 84:*"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento".*

1. La descrizione sistematica dei trattamenti previsti e delle finalità del trattamento;
2. La valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
3. La valutazione dei rischi per i diritti e le libertà degli interessati;
4. Le misure previste per affrontare i rischi.

Le principali norme di riferimento in materia definiscono il rischio come "effetto dell'incertezza" (UNI EN ISO 9000) ovvero "effetto dell'incertezza sugli obiettivi" (UNI ISO 31000), dove l'effetto è uno scostamento da quanto atteso.

Il rischio è spesso espresso in termini di combinazione delle conseguenze di un evento e della verosimiglianza del suo verificarsi, dove per verosimiglianza (o possibilità) si intende la plausibilità di un accadimento ipotizzabile e, per conseguenze, si intendono gli esiti di un evento che influenza gli obiettivi.

La verosimiglianza può essere descritta come probabilità (o frequenza, con riferimento ad un dato intervallo di tempo). Le conseguenze di un evento possono avere effetti positivi o negativi sugli obiettivi.

Pertanto, la definizione di rischio contenuta nelle Linee-guida 17/EN WP 248 è sovrapponibile con queste definizioni: "scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di gravità e probabilità".

Pertanto, il rischio può essere espresso come funzione di G (*gravità delle conseguenze) e di* P (*probabilità di accadimento dell'evento), cioè:*

R= f (G, P)

ove:

R = *entità del rischio*

G = *gravità delle conseguenze*

P = *probabilità di accadimento dell'evento*

Si assume in particolare che la funzione per determinare il rischio sia espressa dal prodotto di probabilità e gravità/rilevanza delle conseguenze, ovvero:

R (rischio) = P (probabilità) x G (gravità/rilevanza)

La procedura di valutazione dei rischi può essere riassunta come definito di seguito.

Ogni possibile minaccia viene analizzata sotto i seguenti profili:

- ✓ valutazione intrinseca della **probabilità** di accadimento dell'evento, in una scala da 1 a 4;
- ✓ valutazione della **gravità** delle conseguenze, in una scala da 1 a 4.

Per ogni possibile rischio identificato, come indicato al paragrafo 2.4 della "Procedura per la valutazione di impatto sulla protezione dei dati", è effettuata la valutazione dell'entità del rischio.

La valutazione è corretta (ossia ricalcolata) in presenza di misure di prevenzione e opportunità identificate e adeguatamente attuate, in relazione ai diversi aspetti esaminati. Si valuta così il

rischio residuo, ossia il rischio che residua a seguito del trattamento del rischio stesso.

Per valutare la gravità, si tengono in considerazione il danno per la reputazione, la discriminazione, il furto d'identità, le perdite finanziarie, i danni fisici o psicologici, la perdita di controllo dei dati, altri svantaggi economici o sociali e, infine, l'impossibilità di esercitare diritti, servizi o opportunità.

Criteri di attribuzione dei livelli di Probabilità e Gravità.

R (entità del rischio)	**Probabilità**	Alta	**4**	Esiste una correlazione diretta tra la situazione rilevata ed il verificarsi dell'evento. Si sono già verificati eventi per la stessa situazione rilevata nel medesimo luogo, in ambienti simili o in situazioni simili. Il verificarsi dell'evento non susciterebbe alcuno stupore nell'organizzazione.
		Media	**3**	La situazione rilevata può provocare l'evento anche se non in modo automatico o diretto. È noto qualche episodio in cui si è verificato l'evento. Il verificarsi dell'evento susciterebbe una moderata sorpresa nell'organizzazione.
		Bassa	**2**	La situazione rilevata può provocare l'evento al contemporaneo verificarsi di particolari condizioni. Sono noti rari episodi già verificatisi. Il verificarsi dell'evento susciterebbe una discreta sorpresa nell'organizzazione.
		Estremamente bassa/non rilevante	**1**	La situazione rilevata può provocare l'evento per concomitanza di più eventi poco probabili indipendenti. Non sono noti episodi già verificatisi. Il verificarsi dell'evento susciterebbe incredulità.

	Gravità	Alta	4	Seria violazione della privacy di un interessato. Alto impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione), con compromissione della fruizione. Conseguenze significative irreversibili o non eliminabili (minaccia per la vita, perdita o sospensione del rapporto di lavoro, danno finanziario ingente).
		Media	3	Violazione della privacy di un interessato con significativo disagio. Impatto su altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione, incolumità della vita) che, in concomitanza con altri elementi, potrebbe comprometterne la fruizione. Conseguenze ripristinabili con un certo dispendio di risorse.
		Bassa	2	Violazione della privacy di un interessato con basso impatto (es. la violazione comporta un disturbo/disagio facilmente ripristinabile). Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di coscienza e di religione).
		Estremamente bassa/non rilevante	1	Impatto irrilevante per la privacy di un interessato. Nessuna violazione di altri diritti fondamentali (es. libertà di espressione e di pensiero, libertà di movimento, divieto di discriminazioni, diritto alla libertà di

				coscienza e di religione).

Il titolare del trattamento ed i soggetti di cui sopra, a seguito della valutazione condotta, effettuano la ponderazione dei rischi.

La ponderazione del rischio è definita come il processo di comparazione dei risultati dell'analisi del rischio rispetto ai criteri di rischio, per determinare se il rischio e/o la sua espressione quantitativa sia accettabile o tollerabile. La ponderazione del rischio agevola la decisione circa il trattamento del rischio, ossia il processo per modificare il rischio. La decisione sugli interventi necessita di stabilire a priori quale sia il livello di **rischio accettabile Ra**, in modo che si individuino le situazioni di intervento prioritarie, che presentano, cioè, un livello di rischio superiore al valore ritenuto accettabile (R>Ra).

La quantificazione del **rischio accettabile R < Ra** avviene in base alla tabella sottostante.

Area del rischio accettabile

R = P X G

Probabilità (P)

Alta	4	4 (eccezione)	8	12	16
Media	3	3	6	9	12
Bassa	2	2	4	6	8
Estrem. bassa / non rilevante	1	1	2	3	4
		1	2	3	4
Gravità (G)		Estrem. bassa / non rilevante	Bassa	Media	Alta

La matrice in tabella individua graficamente quelli che si considerano rischi non accettabili, ovvero quelli per cui è richiesto un intervento di miglioramento tale da riportare la situazione al di sotto della soglia di accettabilità. In base alla matrice dei rischi si individuano come **non accettabili** tutti quei **rischi che risultano avere valori di P x G superiori a 4**, unica eccezione le situazioni che si

riferiscono ad un alto livello di probabilità (P = 4). Poiché non si considera accettabile alcun tipo di danno, neppure di lieve entità, qualora si ritenga il suo verificarsi estremamente probabile.

La tabella che segue riporta i giudizi attribuiti alle classi di rischio. In base a quanto sopra detto, risultano **non accettabili**[3] i rischi classificati come **medio o alto**, oltre a tutti i rischi con un alto livello di probabilità (P = 4).

R (entità del rischio) normalizzata	**I ≥ 6**	**RISCHIO ALTO**
	4 ≤ I ≤ 5	**RISCHIO MEDIO**
	2 ≤ I ≤ 3	**RISCHIO BASSO**
	I ≤ 1	**RISCHIO ESTREMAMENTE BASSO, NON RILEVANTE**

Le carenze eventualmente evidenziate sono oggetto di **misure tecniche e organizzative e/o programmi di miglioramento** definiti al fine di **ridurre il rischio ad un livello accettabile**, secondo il criterio di accettabilità enunciato.

Tali misure e programmi tengono conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento.

INDIVIDUAZIONE DEL TRATTAMENTO E DELLE MISURE DI SICUREZZA

Ai sensi dell'art. 30 del Regolamento UE 2016/679, il titolare del trattamento, insieme al DPO agli eventuali responsabili del trattamento e ad altre funzioni coinvolte provvedono a determinare le tipologie di trattamenti di dati personali effettuati dall'organizzazione o per conto di essa, mantenendo aggiornato un registro delle attività di trattamento svolte sotto la propria responsabilità.

Tale registro contiene tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento, e del responsabile della protezione dei dati;

b) le tipologie di trattamento;

c) le basi legali del trattamento;

[3] Il Regolamento (UE) 2016/679 considera non accettabile il rischio "elevato", che nella presente classificazione su quattro livelli accorpa anche il livello di rischio medio.

d) le finalità del trattamento;

e) una descrizione delle categorie di interessati e delle categorie di dati personali;

f) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

g) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;

h) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

i) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1, del Regolamento.

Tali informazioni saranno documentate nel "Registro delle attività del trattamento (approvato con Determinazione del Direttore Generale n. 73 del 15/06/2023), che sarà aggiornato a seguito dell'adozione della presente valutazione di impatto.

Il trattamento dei dati personali dei soggetti che, ai sensi del D.Lgs. 24/2023, possono effettuare segnalazioni o denunce nonché i facilitatori, la persona coinvolta e la persona menzionata nella segnalazione viene effettuato attraverso strumenti cartacei sia informatici.

L'utilizzazione cartacea e la dotazione di strumenti fisici di conservazione dei dati si rendono necessarie per la corretta gestione degli adempimenti e per l'attività dell'Ente, previa adozione delle seguenti misure di sicurezza:

- Limitazione al solo personale autorizzato (RPCT) dell'attività di trattamento dei dati;
- Limitazione dell'attività di trattamento dei dati connessi alla procedura di whistleblowing all'interno dei locali protetti dell'Ente;
- Nomina ed autorizzazione al trattamento dei dati del RPCT;
- Nomina del fornitore della piattaforma ex art. 28 GDPR;
- Formazione e sensibilizzazione del personale autorizzato all'attività di trattamento;
- Disciplinare per la gestione della segnalazione degli illeciti;
- dotazione di sistemi di allarme (con eventuale collegamento con le forze dell'ordine o servizi di vigilanza);
- dotazione di sistemi di videosorveglianza;
- chiusura delle porte di accesso degli edifici;
- chiusura delle porte di accesso dei locali/uffici;
- serrature agli arredi;
- adozione della tecnica dell'oscuramento dei dati personali e di ogni altra informazione dalla quale si possa dedurre direttamente o indirettamente l'identità del segnalante e di tutti gli altri soggetti la cui identità, ai sensi del D. Lgs. 24/2023, deve rimanere riservata, qualora per ragioni istruttorie anche altri soggetti debbano essere messi a conoscenza del

contenuto della segnalazione e/o della documentazione ad essa allegata;

- Nei casi espressamente previsti dal D.lgs. 24/2023 in cui sia necessario disvelare l'identità del segnalante, richiesta di rilascio del consenso espresso al segnalante e comunicazione per iscritto delle ragioni di tale rivelazione;
- Conservazione dei dati per il conseguimento delle finalità per le quali sono stati raccolti e per il periodo necessario all'espletamento del procedimento amministrativo correlato e in ogni caso saranno detenuti per 5 anni, decorrenti dalla data della comunicazione dell'esito finale della procedura di segnalazione.

La strumentazione informatica prevede l'utilizzo della piattaforma WHISTLEACTA di Actainfo che risulta pienamente conforme al D.lgs. n. 24/2023. Tale strumento, come previsto dalle Circolari AgID n. 2 (Servizi IaaS/PaaS) e n. 3 (Servizi SaaS) del 9 aprile 2018, utilizza il servizio SaaS cloud attraverso un server Cloud dedicato al servizio whistleblowing dell'ente. Il trattamento viene eseguito con l'adozione delle misure di sicurezza di seguito indicate:

1. ogni segnalazione ricevuta viene identificata mediante l'attribuzione di un codice univoco progressivo, registrando la data e l'ora di ricezione che vengono associate stabilmente alla segnalazione;
2. viene tutelata la riservatezza dell'identità del segnalante mediante l'impiego di strumenti di anonimizzazione dei dati di navigazione tramite il protocollo di trasporto https;
3. viene tutelata la riservatezza del contenuto della segnalazione, della documentazione ad essa allegata nonché dell'identità di eventuali soggetti segnalati, garantendo l'accesso a tali informazioni solo ai soggetti autorizzati e previsti nell'iter procedurale attraverso password assegnate dal RPCT. Tutti i dati della segnalazione sono criptati con algoritmo di cifratura a blocchi a chiave simmetrica (AES). Per decriptare i dati, quindi per accedervi, è necessario effettuare il login alla piattaforma. Il login è disponibile solo per l'RPCT e gli eventuali soggetti autorizzati con attivazione dell'autenticazione a due fattori per maggiore sicurezza;
4. viene separato il contenuto della segnalazione dall'identità del segnalante;
5. ai soggetti che gestiscono l'istruttoria, accreditati dal RPCT, viene reso disponibile il solo contenuto della segnalazione;
6. è previsto l'accesso sicuro e protetto all'applicazione Whistleacta per tutti gli utenti mediante l'adozione di sistemi di autenticazione che prevedono tecniche di strong authentication;
7. la piattaforma Whistleacta, per l'acquisizione e gestione delle segnalazioni, assicura l'accesso selettivo ai dati delle segnalazioni, da parte dei diversi soggetti autorizzati, esclusivamente dal RPCT al trattamento, prevedendo, una procedura per l'assegnazione, unicamente da parte del RPCT della trattazione di specifiche segnalazioni all'eventuale personale di supporto;
8. garanzia del divieto di tracciamento dei canali di segnalazione;

9. viene consentito al solo RPCT l'accesso all'identità del segnalante esclusivamente die-tro espresso consenso del "custode" virtuale dell'identità dal segnalante, una funzione, che il RPCT/ODV deve richiedere inserendo la sua password ogni volta che vuole accedere ai dati identitari del whistleblower;
10. nel corso dell'istruttoria, al fine di tutelare l'identità del segnalante, lo scambio di messaggi o documenti tra segnalante e istruttore avviene all'interno della piattaforma web Whistleacta;
11. è consentito in qualsiasi momento, tramite l'applicazione Whistleacta, la fruibilità della documentazione custodita, al fine di evitare il download o, soprattutto, la stampa della stessa che, ove indispensabile per fornirla ai soggetti esterni coinvolti nella segnalazione (ufficio procedimenti disciplinari, magistratura, ANAC, Corte dei Conti, Dipartimento della funzione pubblica) può essere eseguita dal solo RPCT reinserendo la sua password anche se già loggato;
12. vengono applicate politiche di tutela della riservatezza attraverso strumenti informatici (disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione che risiedono su DataBase separati e crittografati): tutti i dati e i documenti allegati o inseriti su Whistleacta sono crittografati.

Per ulteriori dettagli tecnici sul software si rinvia al documento " DOCUMENTAZIONE A SUPPORTO DEL TITOLARE DEL TRATTAMENTO PER LA VALUTAZIONE DI IMPATTO DEI DATI TRATTATI CON IL SOFTWARE" trasmesso da Actainfo srl il 15.01.2024 e assunto al protocollo dell'ente n. 239/2024.

VALUTAZIONE SULLA NECESSITÀ E LA PROPORZIONALITÀ DEL TRATTAMENTO

Sono state determinate le misure previste per garantire il rispetto del Regolamento, ai sensi e per gli effetti dell'articolo 35, paragrafo 7, lettera d) e del considerando 90):

- Resa ai possibili interessati di una informativa sul trattamento dei dati personali;
- Aggiornamento del registro delle attività di trattamento;
- Adozione di una procedura che illustra gli illeciti che si possono segnalare e le modalità per farlo;
- Adozione delle misure tecniche ed organizzative adeguate a proteggere i dati personali;
- Disciplina del rapporto con il fornitore della piattaforma whistleblowing ai sensi dell'art. 28 del GDPE 2016/679;
- Nomina e formazione del personale interno incarico della gestione della segnalazione;

- Sono state determinate le misure (di seguito elencate) che contribuiscono alla proporzionalità e alla necessità del trattamento:
  1. La segnalazione in forma scritta, attraverso il servizio postale, dovrà essere effettuata avendo cura di trasmettere la medesima e la documentazione allegata in due buste chiuse di cui la prima con i dati identificativi del segnalante e copia del documento di riconoscimento e la seconda con la segnalazione. Entrambe, poi, dovranno essere inserite in una terza busta chiusa priva dell'indicazione del mittente e recante l'indicazione "*riservata personale al RPCT*"; la segnalazione sarà protocollata in modalità riservata dal RCPT in autonomo registro; la documentazione cartacea sarà custodita e conservata, a cura del RPCT, in

armadio chiuso a chiave.

2. La segnalazione in forma orale, attraverso l'uso del telefono, sarà effettuata telefonando direttamente al numero telefonico istituzionale e chiedendo di parlare esclusivamente con RPCT. La telefonata non sarà oggetto di registrazione. La segnalazione, previo consenso del segnalante, sarà documentata per iscritto dal RPCT mediante redazione di un verbale. La persona segnalante potrà, verificare, rettificare e confermare il contenuto del verbale mediante sottoscrizione. La documentazione cartacea sarà custodita e conservata, a cura del RPCT, in armadio chiuso a chiave. Qualora il verbale venisse redatto con strumenti informatici, il medesimo sarà conservato in una cartella criptata salvata nella rete dell'Ente ed accessibile solo al RPCT.
3. La segnalazione effettuata mediante incontro diretto con il RPCT sarà, per quanto possibile, organizzata evitando l'appuntamento nell'orario di servizio e nei locali istituzionali dell'Ente. La segnalazione, previo consenso del segnalante, sarà documentata per iscritto dal RPCT mediante redazione di un verbale. La persona segnalante potrà, verificare, rettificare e confermare il contenuto del verbale mediante sottoscrizione. La documentazione cartacea sarà custodita e conservata, a cura del RPCT, in armadio chiuso a chiave.
4. La segnalazione attraverso l'utilizzo della piattaforma informatica presente sul sito istituzionale sarà effettuata con credenziali di accesso ed i file spediti dal segnalante saranno crittografati e quindi, accessibili in chiaro solo dal ricevente Responsabile della prevenzione della corruzione e Trasparenza (RPCT).
5. La segnalazione e la documentazione allegata saranno sottratte al diritto di accesso previsto dagli articoli 22 e seguenti della legge 241/1990 e s.m.i. ed altresì escluse dall'accesso civico generalizzato di cui all'art. 5, co. 2, del D.lgs. 33/2013;
6. Qualora per ragioni istruttorie anche altri soggetti debbano essere messi a conoscenza del contenuto della segnalazione e/o della documentazione ad essa allegata sarà compito del RPCT adottare la tecnica dell'oscuramento dei dati personali e di ogni altra informazione dalla quale si possa dedurre direttamente o indirettamente l'identità del segnalante e di tutti gli altri soggetti la cui identità, ai sensi del D. Lgs. 24/2023, deve rimanere riservata;
7. Nei casi espressamente previsti dal D.lgs. 24/2023 in cui sia necessario disvelare l'identità del segnalante, sarà compito del RPCT richiedere il rilascio del consenso espresso al segnalante e comunicare per iscritto le ragioni di tale rivelazione;
8. Consultazione preventiva del DPO qualora vi fossero dubbi relativamente al trattamento dei dati personali;
9. Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l'Autorità Giudiziaria, la Corte dei conti e l'ANAC.
10. I dati saranno conservati per il conseguimento delle finalità per le quali sono stati raccolti e per il periodo necessario all'espletamento del procedimento amministrativo correlato e in ogni caso saranno detenuti per 5 anni, decorrenti dalla data della comunicazione dell'esito finale della procedura di segnalazione;

- Sono stati disciplinati i rapporti con il Responsabile esterno del trattamento (articolo 28) attraverso l'atto di nomina; Sono state individuate finalità di trattamento determinate e legittime, esplicitate (articolo 5, paragrafo 1, lettera b)) attraverso la stesura dell'informativa

pubblicata sul sito web dell'Ente, ove sono riportati i diritti dell'interessato e le modalità per esercitarli;

- È stato rispettato il principio di liceità del trattamento (articolo 6), attraverso la valutazione delle finalità. Il trattamento, ai sensi del Regolamento UE 2016/679, è finalizzato ad adempiere ad un obbligo legale al quale è soggetto il titolare (art. 6 – par. 1 lett. c) e all'esecuzione di un compito di interesse pubblico (art. 6 par. 1 lett. e) in applicazione del D.Lgs. n. 24/2023;
- I dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c). I dati saranno trattati esclusivamente da personale autorizzato per la ricezione e gestione della segnalazione.
- Ai sensi dell'art. 39, comma 1, lett. c del Regolamento, in ordine alla presente valutazione di impatto il DPO, dietro richiesta dell'Ente, ha rilasciato un parere.

VALUTAZIONE DEI RISCHI PER I DIRITTI E LE LIBERTA' DEI SOGGETTI INTERESSATI

I rischi per i diritti e le libertà degli interessati (articolo 35, paragrafo 7 lettera c)) sono valutati ed indicati nella tabella di valutazione dei rischi. Tali rischi vengono così riassunti:

- rischio distruzione
- rischio perdita
- rischio modifica
- rischio divulgazione non autorizzata
- rischio accesso non consentito ai dati personali trasmessi, conservati o comunque trattati (art. 32, comma 2).

- L'origine, la natura, la particolarità e la gravità dei rischi (cfr. Considerando 84) vengono determinate, tenendo in considerazione le diverse prospettive degli interessati e l'impatto sui relativi diritti e libertà.

ORIGINE INTERNA ED ESTERNA

1) Vi sono rischi causati dal **comportamento degli operatori/dipendenti difforme o non consapevole** (per dolo o colpa) e concretantesi in (a titolo esemplificativo):

- Furto di credenziali di autentificazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;
- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati).

2) Vi sono rischi **causati dolosamente, ma anche fortuitamente, derivanti da eventi esterni che colpiscono gli strumenti di lavoro e la struttura**. Si pensi ad un:

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco *criptolocker* che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati.
- *Spamming*, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati. Il rischio *de quo* è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server, che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione.

3) Vi sono rischi causati da **eventi causali, prevedibili pur in astratto.**
In tal caso si fa riferimento al verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

NATURA DOLOSA E COLPOSA
I rischi sopra declinati possono essere ricondotti ad eventi di natura sia **dolosa** che **colposa**.

PARTICOLARITÀ RISCHI INFORMATICI E CARTACEI
Come evidenziato, si considerano come fonti di rischio, anche prevedibili (cfr. Considerando 90):

- l'errore umano del personale dipendente;
- i rischi provenienti dall'esterno (virus, *troianhorse*, *ramsomware*, intrusione informatica ecc.);
- accessi non autorizzati nei locali e nelle strutture di soggetti terzi non autorizzati, il cui unico scopo è quello di sottrarre, con intento doloso, hardware, software o dispositivi elettronici o documenti cartacei;
- eventi fortuiti

GRAVITÀ; TIPOLOGIA DI CONSEGUENZE (perdita, accesso, danno di immagine, ecc.)
Sono stati, come evidenziato, valutati gli impatti potenziali per i diritti e le libertà degli interessati al verificarsi di eventi, quali l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati; le conseguenze derivanti dagli stessi, astrattamente individuabili nella diffusione e conoscenza di informazioni riservate e di dati personali, determinano un rischio per i diritti e libertà degli interessati (diritto alla riservatezza e la dignità della persona).
Vengono stimate, dunque, la probabilità e la gravità per determinarne il livello di rischio (Considerando 90):

Trattamento dati personali procedura segnalazione di illeciti (whistleblowing)

VALUTAZIONE SUI DATI INFORMATICI E CARTACEI (con applicazione delle misure tecniche ed organizzative sopra riportate)					
	Gravità distruzione **2**	Gravità perdita **2**	Gravità modifica **2**	Gravità divulgazione non autorizzata **2**	Gravità accesso non consentito **2**
Probabilità distruzione **1**	Rischio distruzione **2**				
Probabilità perdita **1**		Rischio perdita **2**			
Probabilità modifica **1**			Rischio modifica **2**		
Probabilità divulgazione non autorizzata **1**				Rischio divulgazione non autorizzata **2**	
Probabilità accesso non consentito **1**					Rischio accesso non consentito **2**

MISURE PREVISTE PER CONTRASTARE I RISCHI

Le altre misure ritenute adeguate a contrastare i rischi individuati sono le seguenti:

- Controlli interni del DPO;
- Regole scritte circa il trattamento dei dati per i soggetti autorizzati;
- Nomine scritte e responsabilizzazione dei responsabili esterni

- Si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2): questo viene sempre coinvolto nelle decisioni dell'Ente e viene richiesto il suo parere su singole questioni o quesiti che hanno a che fare con il trattamento dei dati personali.
  Anche il presente documento verrà sottoposto al suo vaglio finale.

CONCLUSIONI

Considerato il livello di rischio basso, si ritiene superflua, in accordo con il DPO, la consultazione

preventiva dell'Autorità Garante, ai sensi e per gli effetti dell'art. 36 Regolamento UE 679/2016.

Il Direttore Generale
Ing. Enzo Tacconi (*)

(*) Documento informatico sottoscritto con firma digitale
ai sensi del D.Lgs. 82/2005

REGISTRO DI TRATTAMENTO DEI DATI PERSONALI

Dati identificativi e di contatto del Titolare del Trattamento	
Denominazione	**Autorità per il Servizio di Gestione integrata dei Rifiuti urbani ATO Toscana Sud**
Indirizzo/Sede legale	**Via della Pace n. 37 - int. 9 - Loc. Renaccio - 53100 SIENA**
P.IVA/C.F.	**92058220523**
Codice iPA	
N. telefono / N. fax	**0577/247075**
Email	**segreteria@atotoscanasud.it**
PEC	**segreteria@pec.atotoscanasud.it**

Responsabile della Protezione dei Dati (DPO)	
Denominazione	**Avv. Marco Giuri**
Indirizzo	**Via Cosseria n. 28**
P.IVA/C.F.	**050571190489**
N. telefono	**3389642439**
PEC	**marco.giuri@firenze.pecavvocati.it**

Data di creazione:	giugno 2023
Data di aggiornamento:	gennaio 2024
Data di aggiornamento:	
Data di aggiornamento:	

SCHEDA REGISTRO DEI TRATTAMENTI

	AREA/SERVIZIO	TIPOLOGIA DI TRATTAMENTO	BASI LEGALI DEL TRATTAMENTO	FINALITA'	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CONSERVAZIONE	CATEGORIE DI DESTINATARI A CUI I DATI VENGONO COMUNICATI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
SCHEDA N. 1	**Servizio Adempimenti contabili**	Gestione spese ed entrate compreso il fondo economale	Art. 6, comma 1, lett. b), c) ed e); Art. 9 comma 2 lett. b), (trattamento autorizzato dal contratto collettivo);	Gestione delle entrate e delle spese del bilancio dell'Ente	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (Dati anagrafici; iban); Solo per il personale dipendente: categorie particolari di dati (appartenenza sindacale; salute)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno) House Connected (Resp. Esterno) Server dell'Ente	Tesoriere (Resp. Esterno) Revisore	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**Servizio Sistemi Informatici e Generali**	Gestione Protocollo	Art. 6, comma 1, lett. e), ; Art. 10 (trattamento autorizzato dal D.Lgs. 50/2016 e dal 1 luglio 2023 dal D.Lgs. 36/2023 e dal contratto collettivo nazionale di lavoro)	Registrazione documenti in entrata ed in uscita.	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici; iban); Solo per il personale dipendente: categorie particolari di dati (salute, appartenenza sindacale); Dati giudiziari;	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente	Dipendenti	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; chiusura a chiave armadi;Nomine di Responsabili e autorizzati;Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 2	**Servizio Sistemi Informatici e Generali**	Acquisti e forniture	Art. 6, comma 1, lett. b), c), e) ed f), (quet'ultimo per l'esercizio dei diritti del titolare in sede giudiziaria e la gestione di eventuali contenzioni); Art. 10 (trattamento autorizzato dal D.Lgs. 50/2016 e dal 1 luglio 2023 dal D.Lgs. 36/2023)	acquisto di beni e servizi per le esigenze dell'Ente	Operatori economici	Dati personali comuni; Dati giudiziari;	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente	ANAC, Agenzia delle Entrate, INPS INAIL, Procedura della Repubblica, Camera di Commercio, Tesoriere (Resp. Esterno), Ufficio territoriale del Lavoro, Prefettura, consulenti esterni per servizio supporto procedure di affidamento beni e servizi	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 3	**Servizio Sistemi Informatici e Generali**	Centralino e servizio posta elettronica	Art. 6, comma 1, lett. b) ed e);	gestione servizio centralino e posta elettronica	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici);	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente	NO	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 4	**Servizio Sistemi Informatici e Generali**	Pubblicazione atti	Art. 6, comma 1, lett. c) (trattamento autorizzato dal D.Lgs. 33/2013 e sm.i. e Legge 190/2012)	Trasparenza e pubblicità legale	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici);	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno)	NO	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 5	**Servizio Sistemi Informatici e Generali**	Gestione informatica	Art. 6, comma 1, lett. b) ed e);	Amministrare, gestire e assistere i processi informatici, le attrezzature informatiche, gli applicativi, la sicurezza informatica.	Dipendenti	Dati personali comuni (dati anagrafici);	n.a.	n.a.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; diffusione delle Linee Guida del Garante in materia di pubblicazione on line dei dati; utilizzo di screen saver dotati di password (cambiata di frequente), da attivare a tempo e tutte le volte che ci si allontana dalla postazione, protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 6	**Servizio Sistemi Informatici e Generali**	Gestione archivi dell'Ente	Art. 6, comma 1, lett. c) Art. 9, comma 2, lett. b), (trattamento autorizzato dal contratto collettivo) Art. 10 (trattamento autorizzato dal codice dei contratti e dal contratto collettivo)	gestione documenti di archivio dell'Ente	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici); Solo per il personale dipendente: categorie particolari di dati (salute, appartenenza sindacale); Dati giudiziari;	n.a.	n.a.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; armadi chiusi a chiave; accesso da parte del personale autorizzato;
SCHEDA N. 7	**Servizio Sistemi Informatici e Generali**	Conservazione digitale	Art. 6, comma 1, lett. c) ed e); Art. 9, comma 2, lett. b), (trattamento autorizzato dal contratto collettivo) Art. 10 (trattamento autorizzato dal codice dei contratti e dal contratto collettivo)	conservare i documenti in formato digitale	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici); Solo per il personale dipendente: categorie particolari di dati (salute, appartenenza sindacale); Dati giudiziari;	Unimatica (Resp. Esterno);	N.A.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 8	**Servizio Sistemi Informatici e Generali**	Gestione sito web istituzionale	Art. 6, comma 1, lett. c) ed e);	gestione delle sezioni del sito web istituzionale	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici)	House Connected (Resp. Esterno)	n.a.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 9	**Servizio Sistemi Informatici e Generali**	sistema di videosorveglianza	Art. 6, comma 1, lett. f)	protezione del patrimonio dell'Ente	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (immagini)	Server dell'Ente	Forze dell'ordine (eventuale)	NO	Le immagini vengono cancellate dopo un giorno	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 10	**Servizio Sistemi Informatici e Generali**	Gestione documentazione accesso agli atti per conto del responsabile	Art. 6, comma 1, lett. c)	gestione delle richieste di accesso agli atti	Operatori economici; Personale dipendente; utenti; collaboratori; Gestore Servizio;	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente	Controinteressati	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**Servizio Progettazione e Monitoraggio**	Esecuzione del contratto di servizio-analisi del progetto annuale dei servizi esecutivo (PSE)	Art. 6, comma 1, lett. b)	Analisi dei progetti per metterli a disposizione delle amministrazioni comunali	Utenti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	Amministrazioni comunali	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 2	**Servizio Progettazione e Monitoraggio**	Esecuzione del contratto di servizio - monitoraggio dei disservizi	Art. 6, comma 1, lett. b)	Monitorare i disservizi sulla base di quanto previsto dal regolamento di controllo e gestione elaborato sulla base di quanto prescritto dal contratto di servizio con il Gestore	Utenti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	Gestore del servizio	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**Servizio Pianificazione e Regolazione**	Predisposizione del corrispettivo di ambito/Piani economici finanziari (PEF)	Art. 6, comma 1, lett. b) e c)	Predisposizione dei piani economici e finanziari ai sensi di legge	Utenti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	ARERA e Amministrazioni comunali	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 2	**Servizio Pianificazione e Regolazione**	Esecuzione del contratto di servizio 6 Toscana-Regolamenti e strumenti di controllo del Gestore Unico (Regolamento per la gestione ed il controllo)	Art. 6, comma 1, lett. b)	Predisporre e monitorare i regolamenti di gestione e controllo sulla base del contratto di servizio	Utenti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	Amministrazioni comunali	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**Servizio Regolazione impianti e filiere del recupero**	Programmazione e regolazione flussi da conferire presso gli impianti di ambito e regolazione delle tariffe di conferimento ai gestori impianti (Predisposizione del corrispettivo impianti)	Art. 6, comma 1, lett. b) e c)	predisposizione tariffa legata alla gestione degli impianti	Legale rapp. Gestore impianti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	ARERA	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 2	**Servizio Regolazione impianti e filiere del recupero**	Gestore rinnovo e modifica delle convenzioni con i Gestori Impianti	Art. 6, comma 1, lett. b)	rinnovo e aggiornamento delle convenzioni con i Gestori degli impianti	Legale rapp. Gestore impianti	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	n.a.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 3	**Servizio Regolazione impianti e filiere del recupero**	Rendicontazione tecnica per finanziamenti per progetti legati all'incremento della raccolta differenziata	Art. 6, comma 1, lett. b)	erogazione dei finanziamenti ai soggetti destinatari	Firmatari delle convenzioni	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente; Google Drive (Resp. Esterno)	n.a.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**Servizi Generali**	Reclutamento e gestione del personale	Art. 6, comma 1, lett. b) e c); Art 9, comma 2, lett. b); Art. 10 (per gli artt. 9 e 10 il trattamento è autorizzato dal D.Lgs. 165/2001, dal D.Lgs. 81/2008 dalla normativa sul trattamento economico e normativo del personale e dai	reclutamento del personale e gestione del medesimo	Candidati procedure di reclutamento, Personale dipendente e coniuge, figli e parenti	Dati personali comuni (dati anagrafici, dati curriculum vitae e professionale) Categorie particolari di dati (appartenenza sindacale, salute) Dati giudiziari;	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	INPS, INAIL, CENTRI PER L'IMPIEGO, TESORIERE	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;

SCHEDA REGISTRO DEI TRATTAMENTI

	AREA/SERVIZIO	TIPOLOGIA DI TRATTAMENTO	BASI LEGALI DEL TRATTAMENTO	FINALITA'	CATEGORIE DI INTERSSATI	CATEGORIE DI DATI PERSONALI	CONSERVAZIONE	CATEGORIE DI DESTINATARI A CUI I DATI VENGONO COMUNICATI *[indicare eventuali responsabili del trattamento o altri titolari cui i dati siano comunicati]*	TRASFERIMENTO DATI VERSO PAESI TERZI O ORGANIZZAZIONI INTERNAZIONALI *[indicare il Paese terzo o l'organizzazione internazionale cui i dati sono trasferiti e le "garanzie" adottate ai sensi del capo V del RGPD]*	TERMINI ULTIMI DI CANCELLAZIONE PREVISTI	MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE
SCHEDA N. 2	**Servizi Generali**	Conferimento incarichi esterni (studio, ricerca, consulenza, collaborazione)	Art. 6, comma 1, lett. b);	conferimento incarichi	Candidati delle procedure di individuazione del soggetto incaricato; Soggetti a cui è conferito l'incarico	Dati personali comuni (dati anagrafici, dati curriculum vitae e professionale, dati titolarità altre incarichi e cariche, dati cause inconferibilità e incompatibilità conferimento incarico)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	INPS; AGENZIA DELLE ENTRATE	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 3	**Servizi Generali**	Gestione attività Organi	Art. 6, comma 1, lett. e);	gestione delle attività degli organi dell'Ente	componenti organi Ente	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	N.A.	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 4	**Servizi Generali**	Affari legali e contenzioso	Art. 6, comma 1, lett. e);	gestione del contenzioso dell'Ente	parti contenziosi	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	avvocati esterni, organi giurisdizionali	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 1	**RPCT**	Verifica attuazione PTPCT e Codici di comportamento	Art. 6, comma 1, lett. c) Art. 10 (trattamento autorizzato dal DPR 62/2013)	ricognizione adempimento degli obblighi derivanti dal codice di comportamento	dipendenti, collaboratori	Dati personali comuni (dati anagrafici) Dati giudiziari	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	RPCT, dirigenti, OIV, Direttore Generale,	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 2	**RPCT**	raccolta dati e istruttoria casi di conflitti d'interesse	Art. 6, comma 1, lett. c)	istruttoria casi di possibile conflitto di interesse	dipendenti, collaboratori	Dati personali comuni (dati anagrafici)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	RPCT, dirigenti, OIV, Direttore Generale,	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 3	**RPCT**	Adempimenti in materia di anticorruzione e trasparenza	Art. 6, comma 1, lett. c) Art. 10 (trattamento autorizzato dal DPR 62/2013)	svolgimento attività dirette a garantire la trasparenza dell'attività amministrativa e prevenire il fenomeno corruttivo	dipendenti, collaboratori	Dati personali comuni (dati anagrafici) Dati giudiziari	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno) Server dell'Ente;	RPCT, dirigenti, OIV, Direttore Generale,	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;
SCHEDA N. 4	**RPCT**	gestione delle segnalazioni interne (whistleblowing)	Art. 6, comma 1, lett. b) e c); Art 9, comma 2, lett. b); Art. 10 (per gli artt. 9 e 10 il trattamento è autorizzato dal D.Lgs. 24/2023)	raccolta e gestione segnalazioni di illecito	dipendenti, collaboratori	dati personali comuni particolari categorie di dati dati giudiziari	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno); Actainfo (Resp. Esterno)	Autorità giudiziaria, Corte dei Conti, Ufficio provvedimenti disciplinari, ANAC	NO	I dati saranno conservati per il conseguimento delle finalità per le quali sono stati raccolti e per il periodo necessario all'espletamento del procedimento amministrativo correlato e in ogni caso saranno detenuti per 5 anni, decorrenti dalla data della comunicazione dell'esito finale della procedura di segnalazione. La conservazione dei dati trattati in maniera elettronica avviene tramite sistema a norma fornito dalla Società Unimatica, nominata Responsabile esterno del trattamento dei dati personali ai sensi dell'art. 28 del GDPR	Segnalazione visibile solo al RPCT, password di accesso solo al RPCT; Attivazione canale informatico di segnalazione interno; Valutazione di impatto sulla protezione dei dati sulla quale il DPO ha espresso parere favorevole e dove sono contenute, nel dettaglio, le misure di sicurezza da adottare; informativa sul trattamento dei dati personali; Adozione del disciplinare per la gestione della segnalazione di illeciti; Nomina ai sensi dell'art. 28 del GDPR 2016/679 della Società fornitrice della piattaforma; nomina e formazione del personale interno incarico della gestione della segnalazione
SCHEDA N. 1	**CUG**	Segnalazioni del personale dipendente riguardante le materia di competenza del Comitato	Art. 6, comma 1, lett. c) ed e)	assicurare il rispetto dei principi di parità e pari opportunità di genere a garantire l'assenza di forma di violenza, anche morale o psicologica, e di discriminazione	dipendenti	dati personali comuni (dati anagrafici e dati relativi all'oggetto della segnalazione)	Halley Informatica (Resp. Esterno) Unimatica (Resp. Esterno); House Connected (Resp. Esterno)	RPCT, Direttore Generale, Ufficio procedimenti disciplinari	NO	V. Piano di conservazione	Formazione sulla normativa relativa al trattamento dei dati personali (reg. UE 2016/679, D.Lgs. 196/2003 come modificato dal D.Lgs. 101/2018); sensibilizzazione del personale dipendente alle problemaiche connesse al trattamento dei dati personali ed alle relative conseguenze derivanti dall'inosservanza delle norme; protezione della rete dell'Ente da accessi esterni non autorizzati mediante Firewall; Controllo delle IP; backup, antivirus; controllo degli accessi alle risorse di rete; Nomine di Responsabili e autorizzati; Differenzazione degli accessi al server;Aggiornamento costante sistemi operativi; Costante manutenzione dei sistemi hardware;

Da "Consolve Srl" <consolve@pec.it>
A "segreteria@pec.atotoscanasud.it" <segreteria@pec.atotoscanasud.it>
Cc "marcogiuri" <marcogiuri@studiogiuri.it>
Data martedì 7 novembre 2023 - 20:55

Re:Prot. N.3797 del 13-10-2023 - ATS - DPO TRASMISSIONE DPIA PER PARERE

Spett.le ATO Toscana Sud,
la presente per esprimere un positivo parere rispetto alla Valutazione di impatto in oggetto.
Cordiali saluti,
Il DPO
Avv. Marco Giuri

> Da "PEC Ato Toscana Sud" segreteria@pec.atotoscanasud.it
> A consolve@pec.it
> Cc
> Data Fri, 13 Oct 2023 13:13:19 +0200
> Oggetto Prot. N.3797 del 13-10-2023 - ATS - DPO TRASMISSIONE DPIA PER PARERE

DOCUMENTAZIONE A SUPPORTO DEL TITOLARE DEL TRATTAMENTO PER LA VALUTAZIONE DI IMPATTO DEI DATI TRATTATI CON IL SOFTWARE

WHISTLEACTA

TRATTAMENTO DATI RELATIVI ALLE SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)

Documento aggiornato il 15 gennaio 2024

Actainfo srl - 64026 Roseto degli Abruzzi - Sede Operativa: Via Nazionale, 39 – Sede legale: Via Boccaccio 4 - P.I.: 01901750677
Internet: www.actainfo.it - Posta certificata: info@actapec.it - Email: info@actainfo.it - Tel-Fax: +39 0852194581 – 0852015591

Sommario

Actainfo srl - 64026 Roseto degli Abruzzi - Sede Operativa: Via Nazionale, 39 – Sede legale: Via Boccaccio 4 - P.I.: 01901750677
Internet: www.actainfo.it - Posta certificata: info@actapec.it - Email: info@actainfo.it - Tel-Fax: +39 0852194581 – 0852015591

PREMESSA

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Actainfo s.r.l., nel suo ruolo di Responsabile del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.

DESCRIZIONE DELLA PIATTAFORMA WHISTLEACTA

Actainfo s.r.l., in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

Architettura di sistema

L'architettura di sistema è principalmente composta da:

- Infrastruttura virtuale Cloud di Aruba basata su architettura vCloud Director
- Spazio Storage Virtuale Ridondato gestito da Aruba
- VM su vCloud Director

Software impiegato

Vengono primariamente utilizzate le tecnologie open source:

- Sistema operativo Ubuntu Linux 20.04 x86_64 LTS

- Docker
- Mariadb 10.6
- PHP 8.2
- Apache 2.4
- OpenVPN (vpn).

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- Vmware: software di virtualizzazione (gestito dal Cloud Provider)
- Veeam: software di backup (gestito dal Cloud Provider)

Predisposizione dei sistemi virtualizzati:

- Le macchine virtuali sono create all'interno del tenant Actainfo nell'infrastruttura Cloud di Aruba. La gestione dell'HA e del bilanciamento del carico è effettuata in maniera automatica dal Cloud Provider, senza possibilità di intervento da parte dell'utente;
- Le macchine virtuali sono create sulla base di un template di Ubuntu 20.04 LTS, che viene aggiornato periodicamente quando viene creata una nuova VM.
- E' previsto un aggiornamento programmato delle VM, in base agli applicativi installati e al fermo macchina necessario.
- La VM su cui gira OpenVPN è una pfSense (sistema operativo FreeBSD), aggiornata periodicamente.

Architettura di rete

- L'architettura di rete prevede la presenza del firewall di vCloud Director che fornisce funzionalità di NAT, Firewalling e NLB (Network Load Balancer) per esporre i servizi minimi necessari.
- E' prevista la segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente.
- La VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema.
- Ogni connessione di rete implementa TLS 1.2 o superiore.
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità.

Actainfo srl - 64026 Roseto degli Abruzzi - Sede Operativa: Via Nazionale, 39 – Sede legale: Via Boccaccio 4 - P.I.: 01901750677
Internet: www.actainfo.it - Posta certificata: info@actapec.it - Email: info@actainfo.it - Tel-Fax: +39 0852194581 – 0852015591

- Gli accessi amministrativi via SSH sono previsti solo tramite VPN e le VM sono esposte solo per le porte 80,443 .

DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento

PA, Ente o Organizzazione > Titolare del trattamento

Actainfo s.r.l. > Responsabile del trattamento per la fornitura e la gestione di WhistleActa

Aruba > Sub-Responsabile del trattamento, nominato da Actainfo s.r.l., per la gestione dell'infrastruttura (IaaS)

Standard applicabili

Conformità normativa:

- Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)" emanate da ANAC, delibera n. 311 del 12/07/2023.
- ISO27001 "Erogazione di Servizi SaaS di Sportello Digitale"
- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica ACN
- Certificazione CSA Star

Dati e operazioni di trattamento

Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti.

Dati di registrazione

Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio WhisleActa (es. Responsabile Anticorruzione).

Categorie particolari di dati

Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

Dati relativi a condanne penali e reati

Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento e dei dati

1. Attivazione della piattaforma
2. Configurazione della piattaforma

Actainfo srl - 64026 Roseto degli Abruzzi - Sede Operativa: Via Nazionale, 39 – Sede legale: Via Boccaccio 4 - P.I.: 01901750677
Internet: www.actainfo.it - Posta certificata: info@actapec.it - Email: info@actainfo.it - Tel-Fax: +39 0852194581 – 0852015591

3. Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti
4. Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore

Risorse a supporto delle attività di trattamento

Software WhistleActa professionale

Infrastruttura IaaS e SaaS privata basata su tecnologie:

- Sistema operativo Ubuntu Linux 20.04 x86_64 LTS
- Docker
- Mysql 8
- PHP 8.2
- Apache 2.4
- OpenVPN (vpn).
- Vmware: software di virtualizzazione (gestito dal Cloud Provider)
- Veeam: software di backup (gestito dal Cloud Provider)

Actainfo srl - 64026 Roseto degli Abruzzi - Sede Operativa: Via Nazionale, 39 – Sede legale: Via Boccaccio 4 - P.I.: 01901750677
Internet: www.actainfo.it - Posta certificata: info@actapec.it - Email: info@actainfo.it - Tel-Fax: +39 0852194581 – 0852015591