atac

*Rev. x del / /*

# Politica per la tutela del trattamento dei dati personali

atac

## VERIFICHE:

| Struttura | Responsabile | Firma |
|---|---|---|
| | | |
| | | |
| | | |

atac

# SOMMARIO



## Indice delle figure

## 1. Premessa

Il presente documento costituisce la politica aziendale per il trattamento dei dati personali di ATAC S.p.A.

## *Scopo e Campo di Applicazione*

Lo scopo del presente documento è quello di fornire indirizzi di livello generale in merito alla tutela dei trattamenti dei dati personali posti in essere in ATAC. S.p.A.

I principi e gli indirizzi espressi nel presente documento si applicano a tutte le entità organizzative, ai dipendenti, alle risorse esterne e a chiunque abbia accesso e/o tratti i dati personali di ATAC S.p.A.

ATAC S.p.A., in qualità sia di Titolare del Trattamento che di Responsabile del trattamento, ha definito la presente politica tenendo in considerazione:

- l'insieme delle normative di riferimento vigenti in materia di tutela del trattamento dei dati personali
- gli obblighi determinati dalla contrattualistica relativa al trattamento dei dati personali
- gli standard di riferimento in materia di tutela del trattamento dei Dati Personali
- l'approccio basato sulla valutazione dei rischi rispetto ai diritti ed alle libertà delle persone fisiche.

La Politica per la tutela del trattamento dei dati personali è valida sia per i trattamenti attualmente posti in essere dall'azienda, sia per quelli futuri: l'obiettivo rimane quello di garantire che i trattamenti dei dati personali siano eseguiti in linea con quanto previsto dalla normativa, dagli obblighi contrattuali e dagli standard di riferimento e poterlo dimostrare.

Il presente documento si pone al vertice di una struttura documentale che prevede l'emissione di documentazione di maggior dettaglio al fine di attuare in azienda la tutela del trattamento dei dati personali in linea con i principi enunciati nella presente politica.

La documentazione di maggior dettaglio, costituita da processi, documenti di indirizzo tecnico e metodologico, procedure e modulistica a supporto, contiene le regole specifiche ed i passi operativi da attuare in relazione alla misure tecniche ed organizzative che consentono ai trattamenti dei dati personali di ATAC S.p.A. di essere conformi ai requisiti normativi, contrattuali e agli standard, e consentono ad ATAC S.p.A. di dimostrarne la conformità.

## *Responsabilità per la gestione del documento*

Il presente documento deve essere:

- redatto, revisionato e approvato dal Privacy Manager, funzione aziendale deputata ad assicurare gli adempimenti normativi in materia di Privacy finalizzati al trattamento dei dati personali in conformità alla normativa vigente, assicurando al Titolare il necessario supporto giuridico e curando il cooordinamento delle attività in materia di Privacy delle strutture aziendali interessate;

- approvato, in via definitiva, dal Titolare del trattamento;
- distribuito a tutte le figure professionali coinvolte all'interno dell'ambito di applicazione del Sistema di Gestione della Privacy ed ivi operanti a qualsiasi titolo, sia esso riconducibile ad un rapporto di lavoro dipendente ovvero a qualsiasi altra forma di collaborazione o prestazione professionale.

La Politica per la tutela del trattamento dei dati personali è periodicamente aggiornata al fine di gestire nel tempo l'efficacia dei principi da essa espressi e l'ottimizzazione del rapporto costi/benefici delle misure tecniche ed organizzative adeguate implementate.

La Politica per la tutela del trattamento dei dati personali viene sottoposta a revisione a fronte di eventuali modifiche od aggiornamenti dei presupposti di natura normativa, contrattuale e standard.

L'aggiornamento del presente documento deve essere inoltre valutato ed eventualmente implementato anche a fronte delle evidenze risultanti dall'attività periodica di analisi del rischio privacy e, comunque, con cadenza non superiore all'anno.

Il DPO ha il ruolo di monitorare il costante aggiornamento del documento di Politica ed il suo allineamento alla strategia Privacy a livello aziendale.

Per qualsiasi informazione aggiuntiva o supporto in merito alla implementazione dei principi espressi all'interno della presente politica, si deve far riferimento al Privacy Manager di ATAC S.p.A.

## *Struttura del documento*

Il documento è strutturato come segue:

Capitolo 1 – Premessa, è il presente capitolo che descrive caratteristiche e scopo del documento.

Capitolo 2 – Principi generali per il trattamento dei dati personali, descrivono il contesto relativo alla tutela del trattamento dei dati personali ed ai relativi rischi da gestire e stabiliscono i criteri generali che caratterizzano il trattamento dei dati personali in ATAC S.p.A.

Capitolo 3 – Sistema di Gestione per il trattamento dei dati personali, descrive le modalita organizzative definite da ATAC S.p.A. per pianificare, sviluppare, implementare, gestire, monitorare e migliorare le misure tecniche ed organizzative adeguate relative al trattamento dei dati personali, e poterne dimostrare la conformità alle normative vigenti.

Capitolo 4 – Misure tecniche ed organizzative per il trattamento dei dati personali, descrive gli indirizzi attuativi delle specifiche misure tecniche ed organizzative individuate da ATAC S.p.A, quali adeguate al fine di conferire la conformità ai trattamenti dei dati personali ed essere in grado di dimostrarla.

## *Documentazione di riferimento*

Viene di seguito elencata la documentazione di riferimento per il presente documento.

- *REGOLAMENTO GENERALE SULLA PROTEZIONE DEI DATI - Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016*
- *Decreto Legislativo 30 giugno 2003 n. 196 così come integrato dalle modifiche introdotte dal Decreto*

*Legislativo 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)"*

- *Standard ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements*
- *Standard ISO/IEC 27002 - Information technology — Security techniques — Code of practice for information security controls*
- *Standard ISO/IEC 27701 – Security Techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and Guidelines*
- *Standard ISO/IEC 29100 – Privacy Framework*
- *Standard ISO/IEC 29134 - Information technology — Security techniques — Guidelines for privacy impact assessment*
- *Codice Etico di ATAC S.p.A.*
- *Ordine di Servizio n. 25 del 17.05.2018*
- *Ordine di Servizio n. 44 del 18.09.2018*
- *Ordine di Servizio n. 30 del 23.07.2019*
- *Ordine di Servizio n. 45 del 05.12.2019*
- *Ordine di Servizio n. 1 del 01.02.2021*
- *Ordine di Servizio n. 3 del 01.03.2021*
- *Ordine di Servizio n. 15 del 19.03.2021*
- *Ordine di Servizio n. 17 del 02.04.2021*
- *Disposizione Organizzativa n. 3 del 12.04.2021*

## *Principali acronimi e definizioni*

Nel presente documento valgono i seguenti acronimi e definizioni.

| Acronimo/Termine | Definizione |
|---|---|
| Accountability | Il titolare del trattamento è competente per ed è in grado di comprovare il rispetto dei [principi applicabili al trattamento dei dati personali] («responsabilizzazione») (Art. 5(2)). |
| Archivio | Qualsiasi insieme strutturato di dati personali informatici o cartacei, accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico. |

| | |
|---|---|
| Autorità di controllo | L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; L 119/34 IT Gazzetta ufficiale dell'Unione europea 4.5.2016. |
| Autorità di controllo interessata | Un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo. |
| Categorie particolari di dati personali | Dati personali che rivelano 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 (art. 9 GDPR). |
| Consenso dell'interessato | Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento. |
| Dati biometrici | I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. |
| Dati genetici | I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione. |
| Dati relativi alla salute | I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute. |
| 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. |
| 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 4.5.2016 IT Gazzetta ufficiale dell'Unione europea L 119/33 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. |
| Diritto di Accesso | Diritto riconosciuto all'interessato di poter chiedere ulteriori informazioni sul trattamento ed eventualmente estrarne copia |

| | |
|---|---|
| Diritto di rettifica | Diritto riconosciuto all'interessato di ottenere dal titolare la rettifica o l'aggiornamento dei propri dati quando errati |
| Diritto di cancellazione | Diritto riconosciuto all'interessato di ottenere dal titolare la cancellazione dei propri dati quando trattati in violazione di Legge, |
| Diritto di limitazione | Diritto riconosciuto all'interessato di ottenere dal titolare che i propri dati non vengano trattati se non per gli scopi concessi dalla Legge, quando il trattamento va' oltre i termini stabiliti, i dati siano inesatti o quando l'interruzione sia necessaria all'interessato allo scopo di poter tutelare un proprio diritto in sede giudiziaria |
| Diritto di opposizione | Diritto riconosciuto all'interessato di pretendere che il titolare interrompa i trattamenti basati sull'interesse leggittimo, |
| Diritto di portabilità | Diritto riconosciuto all'interessato di chiedere al titolare del trattamento che i dati vengano trasferiti, in formato strutturato, ad un altro titolare del trattamento |
| Diritto a non esser sottoposto a processo decisionale automatizzato e\o profilazione | Diritto riconosciuto all'interessato di non essere sottoposto a trattamenti che comportino un processo decisionale automatizzato o di non essere soggetto a profilazione |
| DPIA | Data Protection Impact Assessment (art. 35 del GDPR): Valutazione d'impatto sulla protezione dei dati |
| DPO | Data Protection Officer. |
| Evidenza privacy | Registrazioni, tracce evidenti che possono essere utilizzate per comprovare la conformità alla normativa privacy vigente, quali ad esempio: documentazione di processo, e-mail, documento che comprova la realizzazione di un adempimento, registrazioni e log in applicazioni informatiche. |
| GDPR | Regolamento Generale per la Protezione dei Dati. |
| GDPR Roadmap | Programma di adeguamento al GDPR costituito da interventi progettuali di natura organizzativa, tecnologica e procedurale, declinati in modalità integrata per gli aspetti di Privacy e di Sicurezza |
| Gruppo imprenditoriale | Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate. |
| Impresa | La persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica. |
| Impatto sugli interessati | Previsione delle conseguenze cui può andare incontro l'interessato a causa del trattamento posto in essere o causa di un data breach. |
| Limitazione di trattamento | Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro. |
| Misure tecniche ed organizzative / misure di mitigazione | Misure intraprese dal Titolare del trattamento volte ad ottenere una mitigazione del livello di rischio o della possibilità che il trattamento possa avere impatti non dovuti sugli interessati |
| Norme vincolanti d'impresa | Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro. |

| | |
|---|---|
| Organizzazione internazionale | Un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati. |
| Profilazione | Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica. |
| Pseudonimizzazione | Il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile. |
| Rappresentante | La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento. |
| Rischio Privacy | Sono i rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale. |
| Rischio inerente Privacy | Misura del livello di rischio che tiene conto della probabilità dell'accadimento di un evento nefasto e delle conseguenze che, potenzialmente, possono determinarsi sugli interessati (Impatto), senza tener conto delle misure di mitigazione che possono essere intraprese dal Titolare del trattamento |
| Rischio residuo Privacy | Misura del livello di rischio che tiene conto della probabilità dell'accadimento di un evento nefasto e delle conseguenze che, potenzialmente, possono determinarsi sugli interessati (Impatto) al netto dell'efficacia delle misure di mitigazione intraprese dal Titolare del trattamento |
| RPD | Responsabile della Protezione dei Dati Personali (equivale a DPO) |
| 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. |
| Repository delle evidenze privacy | Archivio delle evidenze gestite per dimostrare la conformità alle Normative Privacy Vigenti |
| Sistema di Gestione della Privacy | Il Sistema di Gestione della Privacy è l'insieme delle attività di tutela del trattamento dei dati personali aventi come obiettivi:<br>• la protezione delle persone fisiche ripetto ai rischi per i diritti e le libertà delle persone<br>• la possibilità di dimostrare di aver ottemperato alle normative vigenti in materia di protezione di dati personali. |
| 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. |
| 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. |
| Trattamento di dati personali | 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. |
| Trattamento di dati personali transfrontaliero | a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure<br>b) Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro. |
| Trattamento del rischio Privacy | Adozione di misure di mitigazione / misure tecniche organizzative, volte a contenere la probabilità di accadimento di una violazione dei diritti e delle libertà individuali delle persone fisiche. |
| Violazione dei dati personali | La violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati. |
| Videosorveglianza | E' il trattamento che contempla la raccolta, la registrazione, la conservazione ed in generale l'utilizzo di immagini video. |

## 2. Principi generali per la tutela del trattamento dei dati personali

Il presente capitolo illustra il contesto specifico di riferimento della presente politica, relativo ai trattamenti dei dati personali, alla tutela del trattamento dei dati personali ed alla relativa gestione dei rischi, ed enuncia i principi generali adottati da ATAC S.p.A. in merito alla tutela del trattamento dei dati personali.

### *Trattamento dei Dati Personali*

Il presente documento di politica si applica a tutti i trattamenti dei dati personali posti in essere da ATAC S.p.A. sia in qualità di Titolare del Trattamento che in qualità di Responsabile del Trattamento. Per trattameno di dato personale si intende, ai fini del presente documento, 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. Nel contesto di ATAC S.p.A. i trattamenti dei dati personali sono svolti sia con che senza l'ausilio di processi automatizzati, ed hanno come oggetto principalmente i dati di natura personale comune, particolare e giudiziaria[1].

## *Tutela del trattamento dei dati personali*

Per tutela dei trattamenti dei dati personali si intende, ai fini del presente documento, la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, cosi' come disposto dalle normative vigenti in materia di Privacy.

La tutela delle persone fisiche con riguardo al trattamento dei dati di carattere personale ("dati personali") rispetta i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta [2], sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica.

La protezione delle persone fisiche si applica sia al trattamento automatizzato che al trattamento manuale dei dati personali, se i dati personali sono contenuti o destinati a essere contenuti in un archivio.

## *I rischi per i diritti e le libertà delle persone fisiche*

I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:

- se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;
- se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;
- se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori;
- se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.

---

[1] Cfr elenco categorie dei dati personali di cui al Capitolo 4 del presente documento "Classificazione dei dati personali"

[2] Rif. Considerando (1) del GDPR: L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.

Nella valutazione del rischio sono tenuti in considerazione i rischi presentati dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale[3].

## *I principi generali adottati da ATAC per la tutela del trattamento dei dati personali*

ATAC SpA ha quale finalità statutaria l'attività di erogazione di servizi di trasporto pubblico di persone per Roma Capitale. Al centro di tale attività vi sono tre fondamentali direttrici, che rappresentano il risultato interpretativo che ATAC ha ritenuto di dare all'attuale assetto normativo nazionale ed internazionale. Il riferimento è in particolare a[4]:

- **rispetto dei diritti umani**, sia all'interno (dipendenti,collaboratori) che all'esterno della Società (fornitori, clienti, utenza), nella sua più ampia declinazione, che comprende la tutela della salute e sicurezza nei luoghi di lavoro e la promozione di comportamenti fattivi e concreti di non discriminazione;
- **responsabilità sociale, rispetto dell'ambiente e contribuzione all'equilibrato sviluppo** delle condizioni di vita del territorio;
- **legalità e corretta gestione dei rapporti con i soggetti terzi**, siano essi parte della PA o appartenenti al contesto privatistico.

In tale contesto, ed in osservanza del proprio Codice Etico, ATAC S.p.A. tratta i dati personali nel rispetto della normativa applicabile e, in particolare, del Regolamento (UE) 2016/679 (GDPR), nonché nel rispetto dei diritti e delle libertà fondamentali delle persone fisiche con particolare riferimento alla riservatezza e alla protezione dei dati personali.
I principi generali per il trattamento dei dati personali adottati da ATAC Sp.A. sono di seguito elencati.

**Principio di Accountability**

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, ATAC S.p.A. mette in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, e ne gestisce le relative evidenze, al fine di essere in grado di dimostrare, che i trattamenti sono effettuati conformemente alla normativa Privacy vigente.

**Principio del livello di protezione adeguato**

ATAC S.p.A. si impegna a proteggere i dati personali adottando, sulla base dell'esecuzione dell'analisi dei rischi che impattano sui diritti e le libertà fondamentali delle persona fisiche, le misure tecniche ed organizzative adeguate.

**Principio del miglioramento continuo**

[3] Rif Considerando 75 del GDPR
[4] Rif. Codice Etico ATAC S.p.A.

La tutela del trattamento dei dati personali ATAC S.p.A. è attuata attraverso un processo continuo e ciclico di controllo e di aggiornamento delle misure tecniche ed organizzative per adeguarle all'evoluzione della normativa di riferimento, delle tecnologie disponibili e dei rischi emergenti.

**Principio della responsabilità collettiva**

La tutela del trattamento dei dati personali è un impegno collettivo e non un'attività demandata a specifiche unità organizzative: tutti coloro i quali, a vario titolo, sono coinvolti nei trattamenti dei dati personali di ATAC S.p.A. contribuiscono a proteggere e a salvaguardare il trattamento dei dati personali posti in essere.

**Principio di liceità, correttezza e trasparenza del trattamento**

ATAC S.p.A. pone in essere trattamenti per i quali è verificata la liceità, ovvero per i quali è individuata la base giuridica per il trattamento, ed in linea con le esigenze di correttezza e trasparenza, fornisce le opportune informazioni agli interessati.

**Principio di Limitazione delle finalità**

ATAC S.p.A. assicura di trattare i dati personali limitandone la raccolta e l'elaborazione al minimo indispensabile per l'esecuzione delle specifiche finalità del trattamento. La limitazione riguarda sia la quantità dei dati personali che la diversa tipologia.

**Principio di Minimizzazione dei dati**

ATAC S.p.A. assicura la minimizzazione dei dati elaborati con strumenti informatici non solo in funzione delle finalità del trattamento, ma anche in relazione alle modalità di elaborazione dei medesimi dati nel trattamento, limitandone la possibilità di elaborazione in chiaro quando possibile e quindi limitando la osservabilità e la collegabilità dei medesimi dati.

**Principio di esattezza**

ATAC S.p.A. assicura l'esattezza dei dati personali trattati verificando periodicamente l'aggiornamento e operando se del caso la rettifica dei medesimi.

**Principio della limitazione della conservazione**

ATAC S.p.A. assicura che la conservazione dei dati personali è eseguita per il minimo tempo necessario a perseguire le finalità del trattamento e a soddisfare eventuali diritti ad esso correlati.

**Principio di integrità e riservatezza**

ATAC S.p.A. assicura la protezione dei dati personali relativi ai propri dipendenti e ai Terzi, generati o acquisiti all'interno e nelle relazioni d'affari, e ad evitarne ogni uso improprio. ATAC S.p.A. assicura i requisiti di integrità, riservatezza e disponibilità dei dati personali rispetto a trattamenti non autorizzati o illeciti e rispetto alla perdita, alla distruzione o al danno accidentali attuando un approccio basato sull'analisi e la gestione dei rischi che impattano sui diritti e le libertà fondamentali delle persona fisiche.

**Principio della protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita - Privacy by Design e Privacy by Default**

ATAC S.p.A. assicura che i trattamenti dei dati personali, progettati e sviluppati direttamente da ATAC S.p.A o, per suo conto, da terze parti, considerano, fin dalle prime fasi e per tutto il ciclo di vita, i principi e i requisiti di Privacy definiti nelle normative vigenti in materia di protezione dei dati personali. Inoltre ATAC S.p.A. assicura l'adozione di adeguate misure tecniche ed organizzative per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

## 3. Sistema di Gestione per la tutela del trattamento dei dati personali

Dal punto di vista organizzativo e operativo, il contesto nel quale si inquadrano le attività di ATAC S.p.A. è in continua evoluzione per rispondere alle mutevoli esigenze della collettività e delle normative e al progresso tecnologico, e l'Azienda ha da tempo adottato come punto di riferimento il modello organizzativo dei sistemi di gestione[5].

Con l'evoluzione normativa in materia di protezione dati personali, e in particolare con l'avvento del Regolamento europeo n. 679/2016 GDPR (General Data Protection Regulation) ATAC S.p.A ha individuato nel Sistema di Gestione della Protezione dei Dati Personali, o Sistema di Gestione della Privacy (SGP), lo strumento organizzativo atto a soddisfare il principio di accountability[6] in quanto rappresenta la capacità di dimostrare o meglio "rendicontare" le azioni di responsabilizzazione adottate dall'Azienda nel governare la Tutela del Trattamento dei Dati Personali e di migliorarle nel tempo.

Al fine di adempiere agli obblighi di tutela del trattamento dei dati personali e poter domostrare la conformità alle normative vigenti in materia di Privacy, ATAC S.p.A. si dota di un Sistema di Gestione della Privacy.

### *Obiettivi ed ambito del Sistema di Gestione della Privacy*

ATAC S.p.A adotta il Sistema di Gestione della Privacy per la corretta esecuzione delle attività connesse alla pianificazione, sviluppo, implementazione, monitoraggio e miglioramento continuo delle misure tecniche ed organizzative atte a conferire, e poter dimostrare, la conformità dei trattamenti dei dati personali alle normative privacy vigenti e a tutelare i diritti e le libertà fondamentali delle persone fisiche.

Il Sistema di Gestione della Privacy disciplina gli aspetti necessari a:

- fornire gli obiettivi e la strategia relativi alla tutela del trattamento dei dati personali
- adottare un modello organizzativo in cui ruoli e responsabilità, per la gestione della tutela del trattamento dei dati personali, siano definiti in maniera puntuale
- garantire la protezione dei dati personali in modo commisurato agli impatti sui diritti e le libertà delle persone fisiche e in funzione dei risultati dell'analisi dei rischi
- recepire e verificare l'applicabilità di leggi, regolamenti, standard generali e specifici per le proprie attività
- prevedere la formazione idonea del personale sul tema della Privacy in funzione dei ruoli e delle responsabilità ad esso assegnate.

L'ambito del Sistema di Gestione della Privacy è costituito dai trattamenti di dati personali posti in essere da ATAC S.p.A. sia in qualità di Titolare che in qualità di Responsabile del Trattamento dei Dati Personali.

ATAC S.p.A. ha definito il proprio Sistema di Gestione della Privacy sulla base delle esigenze e dei requisiti di tutela del trattamento dei Dati Personali espressi:

- dalle parti interessate;

[5] Rif. Codice Etico
[6] Rif art 24 GDPR

- nella legislazione di riferimento applicabile;
- negli standard di riferimento;

La parti interessate, ovvero gli stakeholder del SGP di ATAC. S.p.A. ed i relativi ambiti di aspettativa e interesse sono elencati nell'Allegato A.

## *Modello del Sistema di Gestione della Privacy*

Il Sistema di Gestione della Privacy è l'insieme delle attività di tutela del trattamento dei dati personali aventi come obiettivi:

- la protezione delle persone fisiche ripetto ai rischi per i diritti e le libertà delle persone
- la possibilità di dimostrare di aver ottemperato alle normative vigenti in materia di protezione di dati personali.

Il Sistema di Gestione della Privacy (SGP) di ATAC S.p.A. è rappresentato da un insieme di processi, documentabili sotto forma di procedure, volti a garantire gli adempimenti normativi nei confronti degli stakeholder in linea con il Ciclo di Deming, noto anche come modello "Plan-Do-Check-Act" (PDCA).

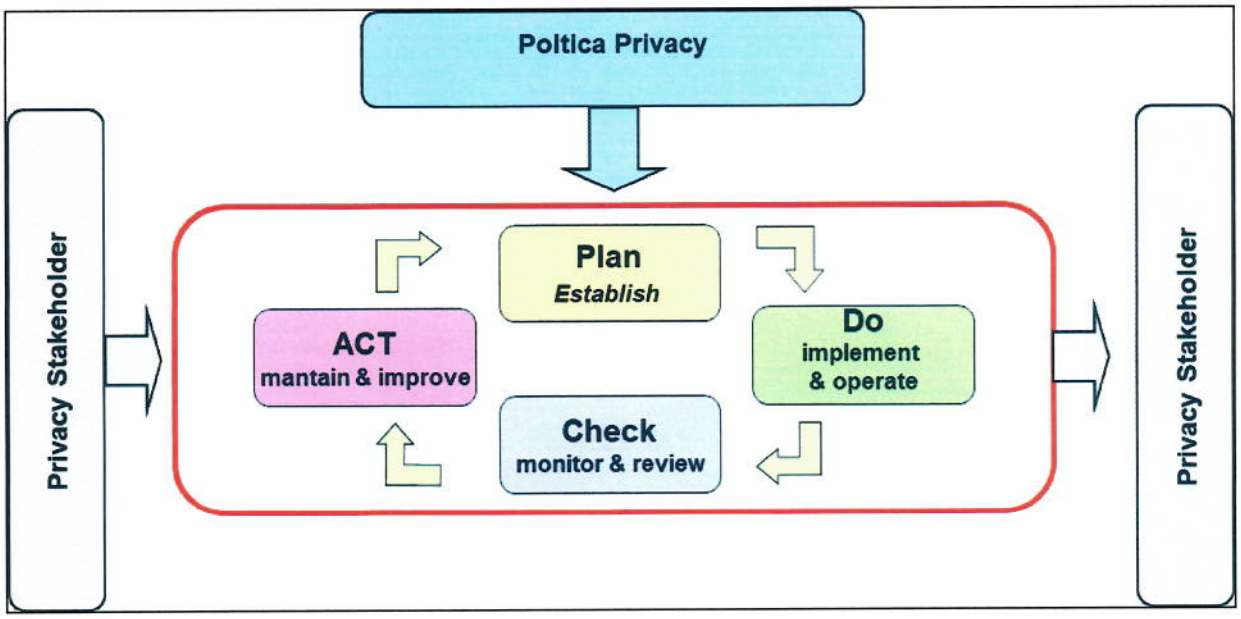


**Figura 1 – Il Sistema di Gestione della Privacy**

I processi del Sistema di gestione della Privacy adottati da ATAC S.p.A. fanno riferimento a quanto di seguito definito.

### PLAN - Processo di Pianificazione

In questo processo sono poste in essere le attività di pianificazione delle misure tecniche ed organizzative adeguate, eseguendo le attività di:

- Definire ed aggiornare la Politica di Privacy aziendale (il presente documento)
- Presidiare l'emergere di nuove normative e provvedimenti che possono potenzialmente impattare l'Azienda
- Definire un approccio sistematico per l'analisi dei rischi Privacy, che sia integrato in ogni nuovo Trattamento di dato personale fin dalle fasi di progettazione, valutando l'adozione di specifica metodologia, processi e tool a supporto
- Eseguire la valutazione dei rischi di conformità Privacy
- Identificare e valutare le opzioni per il trattamento (eliminazione, cessione, riduzione) dei rischi di conformità Privacy
- Identificare gli adempimenti attuabili per gestire I rischi privacy: la Misure Organizzative, Procedurali, Tecnologiche, Logistiche adeguate ed il relativo ciclo di vita
- Identificare le evidenze da gestire per ciascun adempimento o misura tecnica ed organizzativa adeguata
- Identificare le esigenze di monitoraggio degli adempimenti e delle relative evidenze
- Redigere il Piano degli Interventi per gestire il ciclo di vita degli adempimenti e delle relative evidenze (GDPR Roadmap) e ottenerne l'approvazione del management

**DO – Implementare e gestire**

In questo processo sono implementate e gestite le misure tecniche ed organizzative adeguate individuate in fase di Pianificazione, eseguendo le attività di:

- Implementare gli interventi della GDPR Roadmap tramite sviluppo e/o acquisizione di Skill (competenze professionali), Processi, Tecnologie, Documentazione a supporto
- Implementare e gestire gli adempimenti e le Misure Organizzative e Tecniche
- Implementare e gestire le evidenze di ciascun adempimento
- Svolgere programmi di informazione e formazione in materia di Privacy

**CHECK – Monitorare**

In questo processo sono effettuate le attività di monitoraggio sulle misure tecniche ed organizzative adeguate (adempimenti) e sulla gestione delle relative evidenze, eseguendo le attività di:

- Condurre test, monioraggio e revisione di prima parte del Sistema di Gestione della Privacy per verificare l'efficacia degli adempimenti, delle Misure Tecniche ed Organizzative e delle relative evidenze implementate e per verificare che siano soddisfatti gli obiettivi di gestione del Rischio di Privacy ed i requisiti per l'accountability
- Aggiornare i piani degli adempimenti e delle evidenze al fine di tenere conto dei risultati delle attività di monitoraggio e revisione
- Registrare le azioni e gli eventi che potrebbero avere impatti sugli adempimenti, sulle evidenze o sulle prestazioni del Sistema di Gestione della Privacy, al fine di poter indirizzare azioni di migliormento preventive e correttive

atac

**ACT – Migliorare**

In questo processo sono effettuate le attività di miglioramento delle misure tecniche ed organizzative adeguate (adempimenti) e della gestione delle relative evidenze, eseguendo le attività di:

- Implementare le azioni migliorative, correttive e preventive del Sistema di Gestione della Privacy identificate in fase di monitoraggio
- Comunicare le azioni eseguite e i miglioramenti ottenuti alle parti interessate
- Assicurarsi che le azioni migliorative raggiungano gli obiettivi identificati.

## *Ruoli e Responsabilità in ambito Privacy*

In attuazione del Sistema di Gestione della Privacy ATAC S.p.A. ha puntualmente definito ruoli e responsabilità specifiche di privacy in modo trasversale in tutta l'Azienda.
Il modello organizzativo dei ruoli Privacy in ATAC S.p.A. è illustrato nella figura che segue.

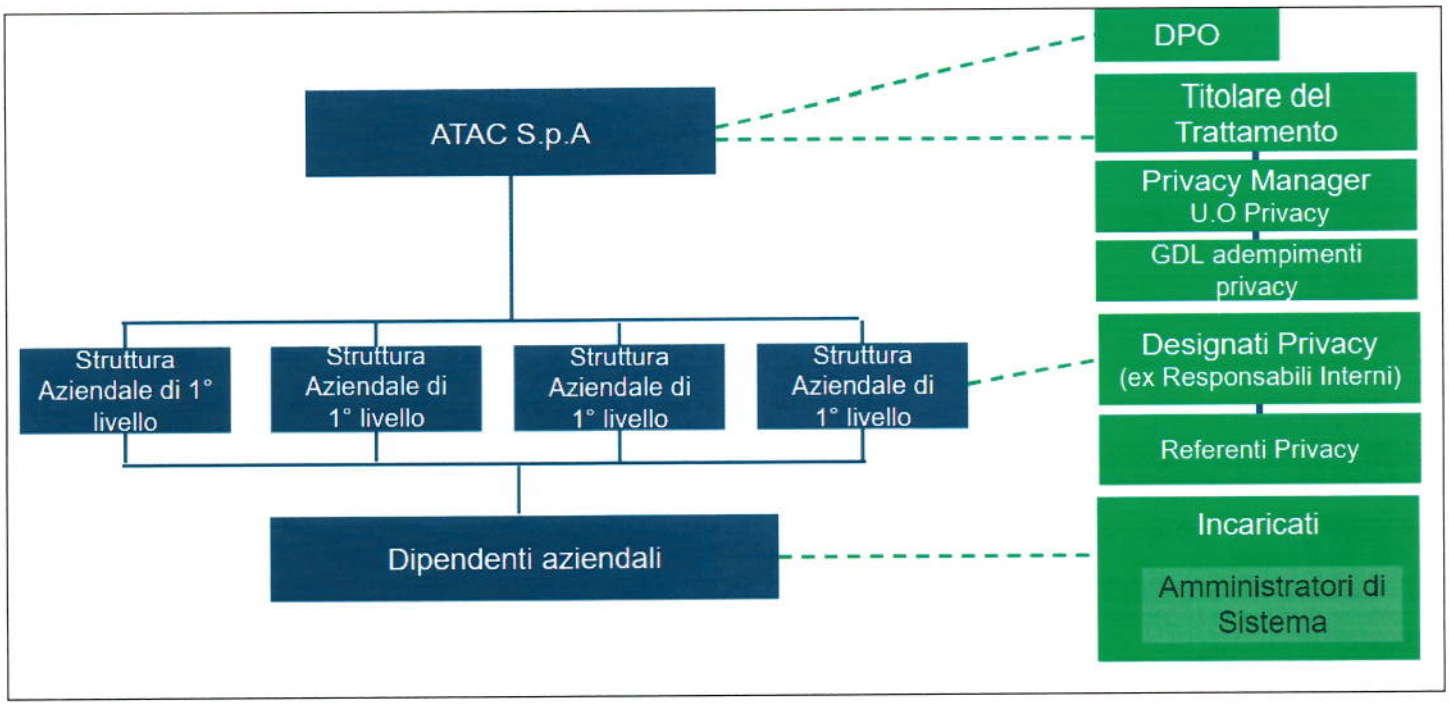


**Figura 2 – I ruoli Privacy in azienda**

Vengono di seguito descritti i ruoli e le responsabilità in materia di tutela del trattamento dei dati personali adottati in ATAC S.p.A.

### Titolare del Trattamento

Il Titolare dei Trattamenti dei dati personali e' ATAC S.p.A.
Le funzioni e le competenze di Titolare sono attribuite al Direttore Generale.
Al Titolare competono le decisioni riguardanti le finalità, i mezzi del trattamento, la messa in atto di misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Regolamento GDPR. Dette misure sono riesaminate e aggiornate qualora necessario.
Per adempiere agli obblighi di legge e per garantire il corretto trattamento dei dati personali ATAC S.p.A., in qualità di Titolare del Trattamento, si avvale dei seguenti «soggetti» privacy:

- DPO,
- Privacy Manager,
- Designati Privacy (Ex Responsabili Interni)

- Referenti Privacy,
- Incaricati del trattamento dei dati personali,
- Amministratori di Sistema.

**DPO – Responsabile della Protezione dei dati Personali**

Con ordine di Servizio n. 17 del 12.04.2021, ATAC S.p.A ha nominato il Responsabile della Protezione dei Dati (DPO) ai sensi degli Artt 37, 38 e 39 del Regolamento Europeo UE 216/679, già previsto con Ordine di Servizio n. 25 del 17.05.2018.

IL DPO, fatte salve le competenze in materia di Privacy attribuite al Privacy Manager nell'ambito della Struttura Organizzativa Privacy, nell'esercizio delle sue funzioni risponde direttamente al Titolare del trattamento ed è incaricato di svolgere, in piena autonomia e indipendenza ed attraverso un approccio strutturato, i seguenti compiti e funzioni:

- Informare e fornire consulenza al Titolare, al Responsabile del Trattamento, e al personale aziendale coinvolto nei trattamenti, in merito al contesto normativo Privacy complessivo vigente di riferimento
- Sorvegliare l'osservanza delle normative vigenti in materia di tutela dei trattamenti dei dati personali, delle politiche del Titolare o del Responsabile, inclusa l'attribuzione delle responsabilità, la sensibilizzazione e formazione del personale coinvolto nei trattamenti
- Fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'Art 35 del GDPR
- Cooperare con il Garante per la Protezione dei Dati Personali
- Fungere da punto di contatto con l'Autorità di controllo per la protezione dei dati personali per questioni connesse al trattamento, tra cui la consultazione preventive di cui all'Art 36 del GDPR, ed effettuare, se del caso, consultazioni relativamente a qualsiasi altra questione.

**Privacy Manager**

Con Disposizione Organizzativa n. 3 del 12.04.2021 la Unità Organizzativa Privacy, che cura le attività inerenti gli adempimenti normativi europei e nazionali in materia di Privacy (cfr D.lgs 196/03 e s.m.i. e il Regolamento Europeo 2016/679), è stata posta a diretto riporto del Direttore Generale

La Struttura Organizzativa Privacy, la cui responsabilità è affidata al Privacy Manager, assicura gli adempimenti normativi in materia di Privacy finalizzati al trattamento dei dati personali in conformità alla normativa vigente, assicurando al Titolare del Trattamento il necessario supporto giuridico e curando il cooordinamento delle attività in materia di Privacy delle strutture aziendali interessate.

In tale ambito è attribuito anche il coordinamento degli interventi di adeguamento individuati dal Gruppo di Lavoro «Adempimenti Privacy a seguito del nuovo Regolamento Europeo UE 2016/679».

**Gruppo di lavoro «Adempimenti Privacy a seguito del nuovo Regolamento Europeo UE 2016/679»**

Con ordine di Servizio n. 30 del 23.07.2019, ATAC S.p.A ha costituito il Gruppo di Lavoro che ha il compito di rendere operativi gli adempimenti normativi privacy nell'ambito di tutta l'azienda.

Il Gruppo di lavoro è composto da:

- Comitato Guida: Direttore del Personale, Direttore ICT, Responsabile della struttura Affari Societari, DPO, Direttore Commerciale e Marketing
- Project Leader: Privacy Manager
- Program Manager: Affari Societari
- Team Operativo: Direzione del Personale, Commerciale e Marketing, Audit, Sicurezza, Ambiente e Qualità, Security, Affari Societari, Legale, Direzione ICT, Atti e Provvedimenti.

Il gruppo di lavoro opera in base ad un cronoprogramma di progetto che è aggiornato annualmente.

**Designato Privacy**

I Designati Privacy, (ex Responsabili Interni) sono individuati nei Responsabili delle Strutture Aziendali di primo livello e vengono nominati con atto formale da parte del Titolare ATAC S.p.A.

I Designati Privacy hanno il compito di realizzare, in linea con le indicazioni fornite dal Titolare, gli adempimenti previsti dalla normative vigente in materia di tutela del trattamento dei dati personali, tra i quali, a titolo esemplificativo e non esaustivo:

- Censire i trattamenti dei dati personali pertinenti alla propria struttura organizzativa e aggiornare il Registro dei Trattamenti quando richiesto
- Individuare e nominare gli Incaricati al trattamento e provvedere alla relativa istruzione e formazione
- Individuare e nominare gli Amministratori di Sistema laddove presenti nella propria Struttura organizzativa
- Individuare e nominare in forma scritta il Referente Privacy e, se nel caso, i Co-Referenti Privacy
- Provvedere alla revoca delle nomine assegnate quando necessario
- Eseguire l'analisi dei rischi dei trattamenti di propria pertinenza ed individuare le Misure tecniche ed organizzative adeguate di propria pertinenza
- Eseguire la valutazione di impatto (DPIA) su nuovi trattamenti di propria pertinenza
- Adottare gli adempimenti, le misure tecniche ed organizzative adeguate, nell'ambito della propria struttura organizzativa, inclusa la contrattazione e la nomina a responsabile esterno di eventuali fornitori

Il Designato Privacy è responsabile rispetto ai compiti assegnati e fornisce al Titolare evidenze in merito agli adempimenti attuati nell'ambito della propria struttura organizzativa.

I Presidenti delle Commissioni interne previste dalla normativa di legge, dai regolamenti e/o dalla normativa interna aziendale rivestono il ruolo di Designati Privacy per le attività di competenza e per tutta la durata della Commissione. In questo contesto, i Presidenti realizzeranno, in linea con le indicazioni fornite dal Titolare, gli adempimenti previsti dalla normative vigente in materia di tutela del trattamento dei dati personali, tra i quali, a titolo esemplificativo e non esaustivo quelli sopra riportati.

**Referente Privacy**

Il Referente Privacy è il dipendente, individuato a diretto riporto del Designato Privacy tra le risorse idonee e nominato dal medesimo al fine di supportarlo negli adempimenti di pertinenza della Struttura Organizzativa di riferimento, dandone contestuale comunicazione al Titolare ed al Privacy Manager.

Qualora le dimensioni e le attività di una Struttura Organizzativa fossero complesse e significative da un punto di vista Privacy, ossia le sotto-strutture riportate in Macrostruttura in cui è suddivisa la singola Struttura

Organizzativa sviluppassero diversi trattamenti di dati personali, il Designato Privacy può avvalersi di ulteriori (Co-)Referenti in ragione della numerosità/diversità dei trattamenti effettuati dalle sotto-strutture. In questo caso i Co-Referenti dovranno coordinarsi con il Referente Privacy di Struttura per le attività di riporto e di comunicazione.

Il Referente Privacy riporta le proprie attività al Designato Privacy, interagendo in caso di esigenza, con il Privacy Manager.

**Incaricato al Trattamento**

Sono incaricati al trattamento dei dati personali le persone fisiche che, per ruolo o attività svolte, effettuano operazioni di trattamento dei dati personali nell'ambito della propria struttura organizzativa.

Per lo svolgimento di tali operazioni l'Incaricato deve essere autorizzato dal Designato Privacy e deve ricevere specifico atto di Nomina ed istruzioni da parte di quest'ultimo.

**Amministratore di Sistema**

Sono Amministratori di Sistema le persone fisiche che compiono attività tecniche finalizzate alla gestione ed alla manutenzione di un impianto di elaborazione dati personali o di sue componenti su sistemi informatici e/o elettronici, di apparati di rete e/o di sicurezza, con specifiche capacità di accessibilità e/o intervento nella gestione, modifica, assegnazione di utenze, credenziali di identificazione e di autenticazione.

Sono considerati Amministratori di Sistema le figure che amministrano tecnicamente i sistemi operativi, i data base, gli apparati di rete, gli apparati di sicurezza e i sistemi software complessi.

L'Amministratore di Sistema deve essere autorizzato con atto di Nomina dal Designato Privacy nella cui struttura organizzativa sono svolte attività tecniche di gestione e manutenzione di un impianto di elaborazione dati personali o di sue componenti su sistemi informatici e/o elettronici.

**ATAC Responsabile del Trattamento**

ATAC S.p.A opera in qualità di Responsabile del Trattamento ogni qualvolta si configura come fornitore di servizi di trattamento di dati personali per conto di entità esterne che a loro volta sono individuate quali Titolari del Trattamento.

Al fine di gestire gli adempimenti di ATAC S.p.A in qualità di Responsabile del Trattamento sono coinvolti i ruoli del Modello Organizzativo Privacy, alcuni dei quali con le seguenti specificità:

- Privacy Manager, che assicura gli adempimenti normativi in materia di Privacy finalizzati al trattamento dei Dati Personali posti in essere da ATAC S.p.A in qualità di Responsabile del Trattamento in conformità alla normativa vigente assicurando il necessario supporto giuridico e curando il coordinamento delle attività in materia di Privacy delle strutture aziendali interessate.
- Designato Privacy della struttura organizzativa che gestisce la fornitura dei servizi di trattamento dei dati personali, che ha il compito di governare tutti gli adempimenti previsti dalla legge e contrattualmente nei confronti del Titolare del Trattamento (committente esterno).
- Referente Privacy che supporta direttamente il Designato Privacy nell'attuazione degli adempimenti rispetto al ruolo di ATAC Responsabile.

Tutto il personale di ATAC S.p.A. e le parti interessate sono coinvolti nelle attività necessarie ad assicurare un atteggiamento proattivo alla tutela del trattamento dei dati personali.

## *La documentazione del Sistema di Gestione della Privacy*

In attuazione del Sistema di Gestione della Privacy ATAC S.p.A. ha definito il modello dell'architettura documentale a supporto, ovvero l'insieme dei documenti ed il loro grado "gerarchico" per poter eseguire le attività previste.

Il modello gerarchico di riferimento della documentazione del SGP è illustrato nella figura che segue.

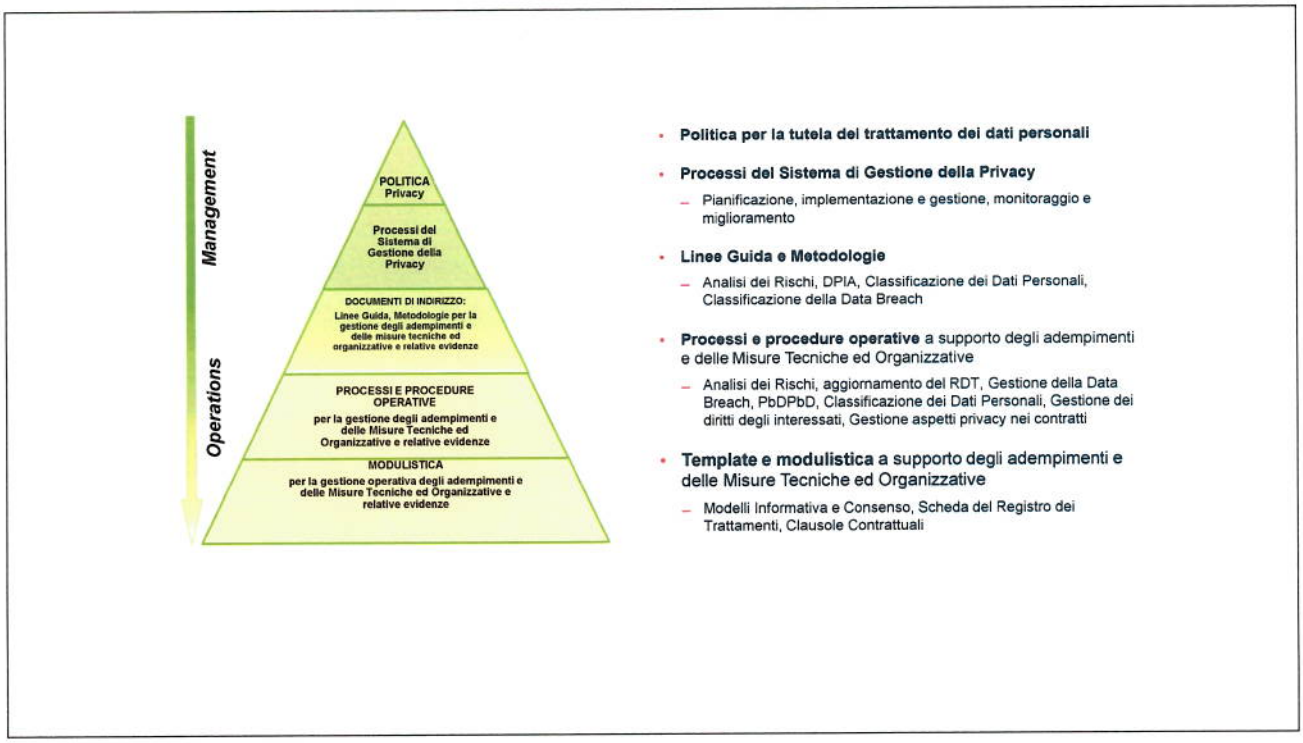


**Figura 3 – La documentazione per il Sistema di Gestione della Privacy**

### Politica per la tutela dei trattamenti dei dati personali

E' il presente documento con cui ATAC S.p.A., in qualità di Titolare e Responsabile del Trattamento dei Dati Personali, definisce i principi, le modalità organizzative e gli indirizzi in materia di Tutela del Trattamento dei Dati Personali da attuare in azienda. Il presente documento si pone al vertice di una struttura documentale che prevede l'emissione di documentazione di maggior dettaglio al fine di attuare in azienda la tutela del trattamento dei dati personali in linea con i principi e gli indirizzi enunciati nella presente politica.

### Processi del Sistema di Gestione della Privacy

Sono i documenti che descrivono i processi posti in essere nell'ambito del Sistema di Gestione della Privacy relativamente al ciclo PDCA: Pianificazione, Implementazione e Gestione, Monitoraggio e Miglioramento continuo.

**Linee Guida e Metodologie**

Sono i documenti che illustrano le linee guida di riferimento e le specifiche metodologie adottate per l'attuazione di alcuni adempimenti o misure di sicurezza tecniche ed organizzative, quali ad esempio, a titolo illustrativo e non esaustivo: l'aggiornamento del Registro dei Trattamenti, l'analisi dei rischi Privacy, la valutazione di impatto (DPIA), la gestione della Data Breach, la Privacy by Design e by Default, la classificazione dei dati personali, la gestione dei diritti degli interessati, la gestione della Privacy nei contratti.

**Processi e procedure operative**

Sono i documenti relativi ai processi ed alle procedure adottate da ATAC S.p.A. per la gestione degli adempimenti e delle Misure Tecniche ed Organizzative adeguate , quali ad esempio, a titolo illustrativo e non esaustivo: l'aggiornamento del Registro dei Trattamenti, l'analisi dei rischi Privacy, la valutazione di impatto (DPIA), la gestione della Data Breach, la Privacy by Design e by Default, la classificazione dei dati personali, la gestione dei diritti degli interessati, la gestione della Privacy nei contratti.
I processi e le procedure operative attuano i principi e gli indirizzi delle misure tecniche ed organizzative adeguate illustrati nel presente documento di politica.

**Template e Modulistica**

Sono i documenti di vario tipo e formato utilizzati nelle procedure operative per la gestione degli adempimenti privacy e delle misure tecniche ed organizzative adeguate, quali ad esempio, a titolo illustrativo e non esaustivo: il form per redigere il Registro dei Trattamenti, il template per la nomina degli Incaricati e degli Amministratori di Sistema, il template per la redazione delle informative e dei consensi, il template per rispondere alle richieste degli interessati, il Template per la redazione delle clausole Privacy nei contratti di fornitura.

La documentazione del Sistema di Gestione della Privacy è disponibile nella intranet aziendale.

## 4. Indirizzi generali delle misure tecniche ed organizzative per la Tutela del Trattamento dei Dati Personali

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità dei trattamenti, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, ATAC S.p.A mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che i trattamenti sono effettuati conformemente alla normativa vigente.
Vengono di seguito evidenziati, per ciascuna misura tecnica ed organizzativa, gli indirizzi adottati da ATAC S.p.A. per raggiungere gli obiettivi ed i principi correlati alla tutela del trattamento dei dati personali e poterne dimostrare la conformità alle normative vigenti.

Le specifiche modalità operative relative a ciascuna misura tecnica ed organizzativa di seguito decritta sono fornite nell'ambito della documentazione relativa a processi, linee guida, metodologie, procedure e modulistica del Sistema di Gestione della Privacy.

## Organizzazione della Privacy

Al fine di perseguire una corretta tutela del trattamento dei dati personali ATAC S.p.A. si è dotata di un modello organizzativo che garantisce una gestione efficace ed efficiente degli adempimenti in tema di Tutela del Trattamento dei Dati Personali, in coerenza con le norme vigenti e con la definizione del Sistema di Gestione della Privacy.

Il Modello organizzativo ed i relativi ruoli e compiti sono descritti nel capitolo 3.

Nell'ambito di tale modello organizzativo i soggetti coinvolti nel trattamento dei Dati personali sono designati individualmente con atto formale e vengono, contestualmente, informati circa le competenze, le responsabilità e le limitazioni che l'incarico comporta.

Il Designato Privacy cura la conservazione delle evidenze relative agli atti di nomina eseguiti presso la propria struttura aziendale ed alimenta lo specifico repository (archivio).

Tutto il personale di ATAC S.p.A. e le parti interessate sono coinvolti nelle attività necessarie ad assicurare un atteggiamento proattivo alla gestione della tutela del trattamento dei dati personali.

La modellistica relativa alla nomina / designazione del personale aziendale è disponibile nella intranet aziendale.

## Registro dei Trattamenti

Al fine di dimostrare la conformità alla normativa Privacy vigente, ATAC S.p.A. ha definito i modelli per redigere il registro dei trattamenti dei dati personali, in linea con quanto previsto all'art 30 del GDPR, e redige ed aggiorna regolarmente:

- il registro dei trattamenti di ATAC S.p.A Titolare
- il registro dei trattamenti di ATAC S.p.A Responsabile

L'attività di aggiornamento periodico dei Registri dei Trattamenti dei Dati personali coinvolge le diverse strutture organizzative aziendali di primo livello ed è realizzata in linea con il Modello del Registro dei Trattamenti e le relative Istruzioni di aggiornamento disponibili nella intranet aziendale.

I registri sono tenuti in forma scritta, anche in formato elettronico, ciascun registro costituisce l'evidenza dell'adempimento ed è conservato a cura del Privacy Manager. I Registri sono messi a disposizione del Titolare, del DPO e dell'Autorità di controllo.

## Analisi dei Rischi Privacy

ATAC S.p.A. esegue periodicamente e comunque per ogni nuovo trattamento, la valutazione dei rischi inerenti il trattamento dei dati personali al fine di individuare e attuare misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio (Art 32 del GDPR).

A tal fine ATAC S.p.A. adotta una metodologia ed un processo per eseguire l'analisi dei rischi privacy, in linea con quanto dettato dalla normativa vigente e dagli standard e best practice di riferimento.

La metodologia per la valutazione dei rischi tiene conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e

gravità per i diritti e le libertà delle persone fisiche che possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale agli interessati.

Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi 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. Sono tenuti pertanto in considerazione i rischi determinati dalla violazione dei requisiti di Riservatezza, Integrità e Disponibilità (RID) dei Dati Personali.

Il rischio è considerato in base a una valutazione oggettiva mediante cui si stabilisce se i trattamenti di dati personali comportano un rischio o un rischio elevato in relazione ai diritti ed alle libertà fondamentali degli interessati. Laddove il trattamento presenti un rischio elevato, questo deve essere attenuato atrraverso l'adozione di Misure Tecniche ed Organizzative adeguate.[7]

Il processo per l'analisi dei rischi privacy prevede che le attività di Analisi dei Rischi Privacy siano condotte in fase di pianificazione del trattamento per consentire l'individuazione delle misure tecniche ed organizzative adeguate. Il processo è attivato dalla Struttura organizzativa owner del trattamento ed eseguito in collaborazione con le strutture aziendali in perimetro, quali ad esempio, Direzione ICT, Risk Management, CERT, Privacy.

Il Processo di gestione del rischio assicura una costante misurazione delle minacce e degli impatti derivanti dagli scenari di rischio, fornendo gli elementi necessari per adeguare e migliorare le misure tecniche ed organizzative atte a ridurre/mitigare i rischi individuati.

Le attività decisionali in merito alla determinazione ed alla gestione dei rischi Privacy che risultano elevati è di competenza del Titolare del Trattamento.

Il report delle attività di Analisi dei Rischi costituisce l'evidenza del relativo adempimento ed è custodito centralmente a livello aziendale presso il Privacy Manager.

## *Valutazione di impatto (DPIA)*

ATAC S.p.A. svolge una valutazione d'impatto sulla protezione dei dati personali qualora un trattamento possa presentare, considerati la natura, l'oggetto, il contesto e le finalità, un rischio elevato per i diritti e le libertà delle persone fisiche, in particolare se prevede l'uso di nuove tecnologie.

A tal fine ATAC S.p.A. definisce ed adotta una metodologia ed un processo per eseguire la valutazione di impatto in linea con quanto dettato dalla normativa vigente e dagli standard e best practice di riferimento.

La valutazione di impatto è redatta, in linea con quanto previsto all'art 35 del GDPR, secondo lo schema documentale ed il processo definiti nella documentazione aziendale, e si avvale della metodologia di Analisi dei Rischi Privacy per le specifiche valutazioni di Impatto.

La valutazione di impatto è condotta dalla Struttura organizzativa aziendale owner del trattamento, in collaborazione con la Direzione ICT, Risk Management e Privacy.

[7] Vedasi GDPR Considerando 76

Il DPO fornisce, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e ne sorveglia lo svolgimento.

L'esito della valutazione è preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta la normativa Privacy vigente.

Laddove la valutazione d'impatto sulla protezione dei dati indichi che i trattamenti presentano un rischio elevato che ATAC S.p.A. non può attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento è consultata l'Autorità di controllo.

Il report della valutazione di impatto costituisce l'evidenza del relativo adempimento ed è custodito centralmente a livello aziendale presso il Privacy Manager.

## *Classificazione dei dati personali*

ATAC S.p.A. ha definito ed attribuito ai dati personali le seguenti classificazioni:

| **Categoria di Dato Personale** | **Esempi** |
|---|---|
| Dato personale comune | Qualsiasi informazione riguardante una persona fisica identificata o identificabile, ad esempio dati identificativi, dati anagrafici, identificativi online |
| Dato personale particolare | Qualsiasi informazione che riveli l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (Art. 9 del GDPR) |
| Dato Personale Giudiziario | Qualsiasi informazione relativa alle condanne penali e ai reati o a connesse misure di sicurezza (Art 10 del GDPR) |
| Dati genetici (categoria di Dati particolari) | Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione; |
| Dati biometrici (categoria di Dati particolari) | Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici |

Il trattamento dei dati personali è eseguito tenendo in considerazione la classificazione dei Dati Personali sopra riportati e applicando quanto specificamente previsto nelle normative vigenti di riferimento per ciascuna specifica categoria.

L'attribuzione della classificazione del dato personale è condotta in fase di censimento dei trattamenti dei dati personali e formalizzata nel medesimo registro dei trattamenti.

ATAC S.p.A. definisce le linee guida per la gestione dei dati personali classificati.

## *Applicazione dei principi del trattamento dei dati personali*

Il trattamento dei dati personali, in linea con i principi espressi nella presente Politica al capitolo 2, è attuato come di seguito specificato.

**Liceità, correttezza e trasparenza**

ATAC S.p.A. assicura la liceità dei trattamenti posti in essere attuando verifiche in merito alle finalità del trattamento ed alle normative applicabili, in particolare determinando la base giuridica del trattamento e documentandola nel Registro dei Trattamenti. La correttezza dei dati raccolti è gestita tramite verifiche di aggiornamento dei dati personali e la trasparenza è realizzata mediante le Informative rilasciate agli interessati.

**Limitazione delle finalità**

ATAC S.p.A. assicura di trattare i dati personali limitandone la raccolta e l'elaborazione al minimo indispensabile per l'esecuzione delle specifiche finalità del trattamento. La limitazione riguarda sia la quantità dei dati personali che la diversa tipologia.

L'impostazione sulla limitazione dei dati trattati è eseguita in fase di progettazione del trattamento da parte della Struttura Organizzativa owner del trattamento in collaborazione con la Direzione ICT e il Privacy Manager, e documentata nelle relative specifiche funzionali.

Le specifiche funzionali di limitazione delle finalità ed i relativi test funzionali costituiscono l'evidenza dell'adempimento e sono custoditi a cura del Designato Privacy della Struttura organizzativa owner del trattamento.

**Minimizzazione dei Dati**

ATAC S.p.A. assicura la minimizzazione dei dati elaborati con strumenti informatici non solo in funzione delle finalità del trattamento, ma anche in relazione alle modalità di elaborazione dei medesimi dati nel trattamento, limitandone la possibilità di elaborazione in chiaro quando possibile e quindi limitando la osservabilità e la collegabilità (linkability) dei medesimi dati.

L'impostazione relativa alla minimizzazione dei dati è eseguita in fase di progettazione tecnica di applicazioni, infrastrutture ICT e sistemi al fine di tenere in considerazione di eseguire per default interazioni o transazioni che utilizzino dati non identificabili (pseudoanonimi o anonimi). La Struttura Organizzativa owner del trattamento si rivolge alla Direzione ICT richiedendo la definizione delle specifiche tecniche per la realizzazione della minimizzazione dei dati e la relativa implementazione.

Le specifiche tecniche della minimizzazione ed i relativi test costituiscono l'evidenza dell'adempimento e sono custoditi a cura del Designato Privacy della Struttura organizzativa owner del trattamento.

**Esattezza**

ATAC S.p.A. assicura l'esattezza dei dati personali trattati verificando periodicamente l'aggiornamento e operando se del caso la rettifica dei medesimi.

Le verifiche per l'esattezza dei dati elaborati tramite strumenti informatici prevedono l'esecuzione delle seguenti attività a carico della Direzione ICT: la revisione dei dati raccolti rispetto alle limitazioni delle finalità, la verifica delle fonti di raccolta del dato, l'aggiornamento delle procedure con cui vengono raccolti ed eleborati i dati, il monitoraggio sulla qualità dei dati.

I report di monitoraggio sulla qualità dei dati costituiscono l'evidenza dell'adempimento e sono custoditi a cura del Designato Privacy della Struttura organizzativa owner del trattamento.

**Limitazione della conservazione**

ATAC S.p.A. assicura la limitazione della conservazione dei dati personali:

- Curandone l'elaborazione per il periodo strettamente necessario a soddisfare le finalità per le quali sono stati raccolti e provvedendo alla successive anonimizzazione o distruzione
- Conservandoli in modalità sicura (archiviandoli ed evitandone possibili utilizzi) anche allo scadere della finalità per la quale erano stati raccolti, laddove sussistano obblighi di legge o esigenze di diritti da tutelare.

La conservazione, la distruzione o l'eventuale anonimizzazione dei dati personali è definita a cura del Designato Privacy della Struttura organizzativa owner del trattamento in linea con le procedure aziendali di riferimento.

**Integrità e riservatezza**

ATAC S.p.A. assicura i requisiti di integrità, riservatezza e disponibilità dei dati personali rispetto a trattamenti non autorizzati o illeciti e rispetto alla perdita, alla distruzione o al danno accidentali, attuando:

- l'esecuzione dell'analisi dei rischi Privacy e individuando le misure tecniche ed organizzative adeguate
- l'implementazione, il monitoraggio ed il migliormanto continuo delle misure di sicurezza tecniche ed organizzative adeguate
- il riesame periodico dei rischi e delle misure a contrasto.

Le attività sopra descritte, connesse alla individuazione delle Misure di Sicurezza, nonchè le attività di sviluppo, gestione e monitoraggio delle misure di sicurezza dei trattamenti dei dati personali, sono condotte dal Designato Privacy della Struttura organizzativa owner del trattamento in collaborazione con Privacy, Risk Management e la Direzione ICT.

## *Privacy by Design e by Default*

ATAC S.p.A., ogni qualvolta viene progettato (Privacy by Design) un nuovo trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, mette in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, e ad integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della normativa nazionale Privacy vigente e tutelare i diritti degli

interessati. Le misure tecniche ed organizzative adeguate sono individuate, sulla base dell'analisi dei rischi Privacy, attraverso il processo di Privacy by Design, utilizzando specifiche procedure e metodologie in linea con gli standard e le best practice di riferimento.

ATAC S.p.A. mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita (Privacy by Default), solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza il consenso dell'interessato. Le misure tecniche ed organizzative adeguate sono individuate attraverso il processo di Privacy by Default, utilizzando specifiche procedure e metodologie in linea con gli standard e le best practice di riferimento.

I processi di Privacy by Design e di Privacy by Deafult sono attivati dalla Struttura organizzativa owner del trattamento ed eseguiti in collaborazione con le strutture aziendali in perimetro, in particolare con la collaborazione della Direzione ICT ed integrati:

- nell'ambito del più ampio Processo di Sviluppo / Acquisizione del Software
- con il Processo di Analisi dei Rischi Privacy
- con le procedure di implementazione dei principi del trattamentonell'ambito del processo di sviluppo del software.

La documentazione di progetto costituisce l'evidenza dell'adempimento ed è custodita a cura del Designato Privacy della Struttura organizzativa owner del trattamento.

## *Sensibilizzazione e formazione per la tutela del trattamento dei dati personali*

ATAC S.p.A., consapevole che la tutela del trattamento dei dati personali è una responsabilità collettiva a livello aziendale, assicura la pianificazione e l'erogazione di regolari interventi di informazione e formazione in materia di Tutela del Trattamento dei Dati Personali.

In particolare ATAC S.p.A. cura:

- lo sviluppo e l'attuazione di programmi di sensibilizzazione in materia di tutela dl trattamento dei dati personali indirizzati al personale aziendale coinvolto nel trattamento dei dati personali
- lo sviluppo e l'attuazione di programmi di formazione specifica Privacy indirizzati al personale coinvolto nelle attività del Sistema di Gestione della Privacy aziendale.

Lo sviluppo dei programmi di formazione e la relativa erogazione sono sviluppati a cura dell'Unità Organizzativa Formazione della Direzione del Personale in collaborazione con Privacy.

Il programma di formazione, il materiale didattico oggetto della formazione e le registrazioni delle presenze ai corsi costituiscono evidenze dell'adempimento e sono custodite a cura di Formazione.

## Misure di Sicurezza

ATAC S.p.A. mette in atto misure di sicurezza tecniche ed organizzative adeguate a tutelare il trattamento dei dati personali individuandole tramite specifica attività di valutazione dei rischi in termini di impatti per i diritti e le liberta individuali degli interessati.

L'individuazione delle misure di sicurezza adeguate a contrastare i rischi determinati dalla perdita di riservatezza, integrità e disponibilità dei dati personali è condotta dalla Struttura organizzativa owner del trattamento in collaborazione con la Direzione ICT, ed eventualmente con CERT, Sicurezza sul Lavoro, Security e con Privacy. Le misure di sicurezza adeguate a contrastare i rischi privacy sono individuate in linea con quanto definito negli standard ISO/IEC 27001 ed ISO/IEC 27002 già adottati a livello aziendale. Inoltre ATAC S.p.A. adotta le Misure Minime di Sicurezza definite da AGID[8].

Lo sviluppo, l'adozione, il monitoraggio ed il miglioramento continuo delle misure di sicurezza individuate quali adeguate a contrastare i rischi Privacy sono assicurati dalla Direzione ICT, in allineamento con Privacy e con la Struttura Organizzativa owner del trattamento.

La Direzione ICT individua, registra e conserva le evidenze relative alla implementazione e gestione delle Misure di Sicurezza adeguate a contrastare i rischi Privacy.

## Gestione della Data Breach

Ai fini del presente documento si definisce la Data Breach come un incidente di Sicurezza che puo' comportare impatti di natura fisica, economica o morale agli interessati a causa di violazione della riservatezza, integrità o disponibilità dei dati personali.

ATAC S.p.A. assicura la gestione della Data Breach adottando uno specifico processo, integrato con il processo di gestione degli incidenti di sicurezza, basato su:

- Identificazione e classificazione di un evento di data breach
- Analisi degli impatti Privacy
- Escalation e risoluzione interna della Data Breach
- Gestione delle comunicazioni nei confronti degli interessati e dell'Autorità Garante
- Registrazione di tutte le azioni compiute nel Registro della Data Breach.

Privacy cura il disegno, lo sviluppo e l'attuazione del processo di gestione della Data Breach in collaborazione con la Direzione ICT, CERT e Security, e individua, registra e conserva le evidenze relative alla gestione della Data Breach, incluso il Registro delle Evidenze della Data Breach.

Tutto il personale di ATAC S.p.A. e le parti interessate sono coinvolti nelle attività necessarie ad assicurare un atteggiamento proattivo alla gestione degli eventi/incidenti di Privacy (Data Breach).

[8] Agenzia per l'Italia Digitale - Circolare 17 marzo 2017, n. 1/2017 e Circolare 18 aprile 2017, n. 2/2017. Misure minime di sicurezza ICT per le pubbliche amministrazioni.

## *Informative*

ATAC S.p.A. assicura il principio della trasparenza nel trattamento dei dati personali fornendo agli interessati, per ciascun trattamento, una dettagliata informativa contenente tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 del GDPR.

Le informative sono rese in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, prima di iniziare il trattamento. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Le informazioni possono essere fornite anche oralmente.

La responsabilità di rendere disponibile l'Informativa Privacy per ciascun trattamento è della Struttura Organizzativa owner del medesimo trattamento.

I testi da utilizzare per la redazione di una Informativa sono curati da Privacy e sono resi disponibili nella Intranet aziendale.

Il documento di Informativa associato a ciascun trattamento costituisce evidenza dell'adepimento ed è gestito a cura della Struttura Organizzativa owner del medesimo trattamento.

## *Consensi*

ATAC S.p.A. assicura ed è in grado di dimostrare che, qualora il trattamento sia basato sul consenso, l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

ATAC S.p.A. fornisce agli interessati la richiesta di consenso in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro e tiene traccia dei consensi forniti dall'interessato prima di avviare il trattamento.

ATAC S.p.A. informa gli interessati sulle modalità per revocare il proprio consenso e tiene traccia delle modifiche al consenso prestate dagli interessati.

La responsabilità di rendere disponibile il documento del Consenso per ciascun trattamento è della Struttura Organizzativa owner del medesimo trattamento.

I testi da utilizzare per la redazione del documento di consenso sono curati da Privacy e sono resi disponibili nella Intranet aziendale.

Il documento di consenso associato a ciascun trattamento e la relativa registrazione costituiscono evidenza dell'adepimento e sono custoditi a cura della Struttura Organizzativa owner del medesimo trattamento in caso di consenso fornito su supporto cartaceo. In caso il consenso sia registrato tramite applicazioni SW, la custodia delle registrazioni è eseguita, su richiesta della struttura owner del trattamento, da parte di ICT.

## *Gestione dei Diritti degli Interessati*

ATAC S.p.A. assicura agli interessati di esercitare, ai sensi degli articoli dal 15 al 22 del Regolamento UE n. 2016/679, il diritto di:

a) chiedere la conferma dell´esistenza o meno di propri dati personali;

b) ottenere le indicazioni circa le finalità del trattamento, le categorie dei dati personali, i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati e, quando possibile, il periodo di conservazione;

c) ottenere la rettifica e la cancellazione dei dati;

d) ottenere la limitazione del trattamento;

e) ottenere la portabilità dei dati, ossia riceverli da un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e trasmetterli ad un altro titolare del trattamento senza impedimenti;

f) opporsi al trattamento in qualsiasi momento ed anche nel caso di trattamento per finalità di marketing diretto;

g) opporsi ad un processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione;

h) chiedere al titolare del trattamento l´accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;

i) revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;

j) proporre reclamo all'Autorità di controllo

ATAC S.p.A. attua un processo per assicurare che le richieste degli interessati abbiano risposta entro i tempi previsti dalle normative nazionali vigenti[9] e mantiene traccia di tutte le comunicazioni intercorse a fronte di ciascuna richiesta di accesso da parte degli interessati.

Le richieste di esercizio dei diritti dovranno essere inviate al Titolare del Trattamento dei dati personali via e-mail alla casella di posta elettronica (email/ PEC) di ATAC S.p.A. protocollo@cert2.atac.roma.it e/o al Responsabile della protezione dei dati (DPO) di ATAC all'indirizzo PEC segreteria.societaria@cert2.atac.roma.it, ovvero all'indirizzo email responsabileprotezionedati@atac.roma.it, cui va allegato l´apposito modulo - scaricabile dal sito aziendale all'indirizzo https://www.atac.roma.it/files/doc.asp?r=717 - compilato e copia del documento di riconoscimento. Le richieste possono essere inviate anche via posta ordinaria con raccomandata A/R all'indirizzo Via Prenestina 45 00176 ROMA.

La responsabilità di gestire le richieste degli Interessati è di Privacy in collaborazione con le Strutture Organizzative owner dei trattamenti dei dati personali e la Direzione ICT, in linea con le procedure aziendali definite.

Le comunicazioni intercorse per la gestione del diritto dell'interessato e le registrazioni a supporto dei sistemi informatici costituiscono evidenza dell'adepimento e sono custoditi a cura di Privacy, della Struttura Organizzativa owner del trattamento e della Direzione ICT, in linea con le procedure aziendali definite.

[9] Rif. GDPR Art 12 c3. Il titolare del trattamento fornisce all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste.

## *Trasferimento all'estero dei dati*

ATAC S.p.A. assicura che, in caso di trasferimento all'estero dei dati personali, questo si svolge solo in presenza delle garanzie adeguate previste dalle vigenti normative in materia di tutela del trattamento dei dati personali.

A tal fine ATAC S.p.A. adotta un processo che prevede di verificare e formalizzare, nell'ambito di ciascun trasferimento all'estero dei dati personali, le specifiche garanzie di adeguatezza.

## *Gestione della Privacy nei contratti*

ATAC S.p.A. assicura la gestione dei requisiti di conformità alle normative vigenti Privacy nell'ambito della contrattualistica e della gestione dei fornitori attuando:

- la redazione di specifiche clausole e misure di sicurezza nell'ambito degli accordi di protezione dei Dati (Data Protection Agreement) dei contratti di fornitura
- l'attuazione di processi strutturati preposti alla gestione degli obblighi privacy derivanti dalla sottoscrizione dei contratti di ATAC S.p.A. come Titolare e come Responsabile, obblighi relativi ad esempio a Misure di Sicurezza, Gestione Data Breach, Gestione Diritti degli Interessati, Registro dei Trattamenti, Auditing, Nomina di subfornitori,...).

La responsabilità della redazione delle specifiche clausole privacy direttamente nel contratto e/o degli Accordi di Protezione dei Dati Personali è del Privacy Manager.

La responsabilità di inserire gli accordi di Protezione dei Dati Personali nei contratti di Fornitura di ATAC S.p.A Titolare del trattamento è della Struttura Organizzativa owner del trattamento.

Il contratto sottoscritto con le clausole o con gli accordi di Protezione dei Dati Personali firmati costituiscono evidenza dell'adempimento e sono custoditi a cura della Struttura Organizzativa owner del trattamento e a cura di Acquisti.

## *Monitoraggio e Audit delle misure tecniche ed organizzative Privacy*

ATAC S.p.A. assicura il monitoraggio delle misure tecniche ed organizzative adeguate attuando:

- il Processo di Monitoraggio dell'efficacia delle Misure Organizzative e Tecniche di Privacy, con la definizione ed implementazione degli indicatori di monitoraggio, frequenza del monitoraggio, esecuzione delle attività di monitoraggio, gestione delle evidenze e reporting dei risultati
- Il Processo di Auditing delle Misure Organizzative e Tecniche di Privacy con la definizione ed implementazione della Pianificazione di AUDIT PRIVACY, frequenza, esecuzione delle attività di auditing e reporting dei risultati.

Il Processo di monitoraggio dell'efficiacia delle misure tecniche ed organizzative Privacy è a cura di Privacy, che conserva i report di monitoraggio quali evidenze dell'adempimento.

Il Processo di di Auditing delle Misure Organizzative e Tecniche di Privacy è a cura della Struttura Organizzativa di Internal Audit, che conserva i report di audit quali evidenze dell'adempimento.

## *La gestione delle evidenze per dimostrare la conformità*

ATAC Sp.A., in linea con il principio di accountability, attua la gestione delle evidenze per dimostrare la conformità alle normative Privacy vigenti adottando uno specifico processo, il "Processo per la gestione delle evidenze", e adottando specifici strumenti: il "Repository delle evidenze Privacy" ed il "Registro delle Evidenze Privacy",

Il Processo per la gestione delle evidenze ha l'obiettivo di garantire che le evidenze di ciascun adempimento privacy siano individuate, tracciate e conservate al fine di poter essere esibite in caso di attività di monitoraggio, auditing e controlli esterni anche da parte dell'Autorità Garante Privacy.

Le evidenze di ciascun adempimento sono individuate, registrate e conservate in linea con quanto previsto dallo specifico processo e sono custodite a cura dal soggetto ivi individuato nell'ambito di uno specifico repository. Il Repository delle evidenze Privacy gestito da ciascun Designato Privacy, sarà costituito, a seconda delle modalità del trattamento, da archivi elettronici che contengono mail, documenti o registrazioni applicative e di log, o da faldoni che contengono documenti cartacei.

Il Registro delle evidenze è lo strumento di controllo adottato da ATAC S.p.A. con l'obiettivo di consentire di individuare e reperire in caso di necessità ciascuna evidenza.

Il Registro riporta, per ciascuna evidenza:

- Denominazione dell'Evidenza (cosa è: es Consenso)
- Identificativo dell'evidenza (nome doc, nome file, ...)
- Formato della evidenza cartaceo/elettronico
- Struttura / contenuto dell'evidenza
- Eventuale scadenza della documentazione che costituisce evidenza
- Ownership di produzione/ raccolta/ gestione/ conservazione evidenza
- Archivio Evidenza: è la denominazione del repository delle evidenze che contiene l'evidenze da poter esibire
- Localizzazione fisica o logica dell'evidenza per finalità di esibizione: Coordinate di localizzazione fisica o logica dell'evidenza da poter esibire
- Modalità di accesso all'evidenza: chi, perchè, come e quando e modalità con cui accedere: link diretti nella intranet, o link a processi/procedure, o istruzioni operative, forms, altri repository aziendali informatizzati e non.

Il Registro delle evidenze è curato, aggiornato e custodito a cura della Struttura Organizzativa Privacy.

## 5. Gestione delle violazioni della Politica per la Tutela del Trattamento dei Dati Personali

E' fatto obbligo ai destinatari della presente politica di osservare scrupolosamente le prescrizioni della presente Politica.

Il mancato rispetto delle regole qui contenute, comporta per i destinatari, previa contestazione dei fatti, l'applicazione di sanzioni proporzionali alla gravità dell'inadempimento.

Il seguente allegato costituisce parte integrante del presente documento di Politica per la Tutela del Trattamento dei Dati Personali.

**ALLEGATO A – Stakeholder del Sistema di Gestione della Privacy**

Per il Titolare del Trattamento dei dati personali
Il Direttore Generale
*Dott. Franco Giampaoletti*

……

*Data, ……*

## ALLEGATO A – Stakeholder Privacy

Nell'ambito del SGP definiamo gli Stakeholder Privacy qualsiasi soggetto, persona o struttura organizzativa, interna o esterna all'azienda, che ha delle aspettative/interessi rispetto alle attività di Gestione della Privacy di ATAC S.p.A.

Gli Stakeholder sono soggetti che possono avere interazioni di diversa natura rispetto alle attività di Privacy Compliance di ATAC, quali ad esempio:

- Facoltà decisionale rispetto alle scelte strategiche che confomano le attività di Privacy Compliance
- Esigenze di informazioni per poter indirizzare adeguatamente le proprie attività aziendali
- Esigenze di controllo rispetto ad obiettivi correlati agli aspetti di Privacy Compliance

Gli Stakeholder Privacy sono individuati come:

- Stakeholder Interni – ovvero quei soggetti che internamente ad ATAC S.p.A. possono esprimere aspettative o interessi correlati alle attività di Conformità Privacy
- Stakeholder esterni – ovvero quei soggetti che pur essendo esterni all'azienda possono esprimere aspettative o interessi correlati alle attività di di Conformità Privacy

Di seguito gli stakeholder interni ed esterni del SGP di ATAC S.p.A. ed indicazioni in merito al relativo ambito di aspettativa o interesse.

| **Stakeholder interni** | **Ambito di aspettativa / interesse** |
|---|---|
| Titolare Direttore Generale | Governo dell'Accountability verso il GDPR |
| Collegio Sindacale | Valutare l'adeguatezza delle strutture organizzative al raggiungimento degli obiettivi aziendali, in questo caso gli obiettivi di conformità alle normative Privacy. |
| DPO Responsabile della Protezione dei Dati Personali | Funzioni di controllo e verifica in merito alla tutela del trattamento dei dati personali in azienda |
| Privacy – Privacy Manager | Attività inerenti gli adempimenti normativi europei e nazionali in materia di Privacy |
| Risk Management | Gestione del rischio di Privacy in allineamento ai processi aziendali di gestione del rischio |
| Amministratore Unico | Budget per attuare la Privacy in azienda |
| Relazioni industriali - Rapporti con Organizzazioni Sindacali | Gestione degli impatti Conformità Privacy sui lavoratori |

| | |
|---|---|
| Formazione – Direzione Personale | Awareness, Formazione e sviluppo skill specifici in ambito Privacy Compliance |
| Procurement – Acquisti | Gestione contrattualistica con i fornitori a norma Privacy |
| Direzione del Personale – Organizzazione | Integrazione della Privacy nei processi e procedure aziendali |
| Qualità | Integrazione del Sistema di Gestione della Privacy con il Sistema Qualità |
| Internal Audit | Controlli di conformità a Procedure, Best Practices e Politiche di Privacy aziendale |
| Direzione ICT | Misure di Sicurezza a supporto dei trattamenti dei dati personali, Gestione della Data Breach |
| Strutture aziendali: Designati Privacy e Referenti Privacy | Realizzazione e gestione dei requisiti di Privacy Compliance nell'ambito dei trattamenti eseguiti nella propria struttura organizzativa. |
| Dipendenti: interessati | Tutela dei Diritti e Riscontri rispetto all'esercizio dei diritti degli interessati |
| Incaricati al trattamento e Amministratori di Sistema | Nomine, Istruzioni e relativi compiti |

| Stakeholder esterni | Ambito di aspettativa / interesse |
|---|---|
| Azionista – Roma Capitale | Interesse di natura generale dell'azionista rispetto alla conformità della partecipata. |
| Cliente: Roma Capitale contraente (in relazione a quanto erogato da ATAC S.p.A. in qualità di Fornitore di Servizi) | Rispetto del contratto di servizio e degli obblighi privacy in esso definiti. |
| Cliente: Regione Lazio | Rispetto del contratto di servizio e degli obblighi privacy in esso definiti. |
| Fornitori esterni | Eseguono le attività contrattualizzate in linea con gli obblighi privacy sottoscritti in qualità di Responsabile o Sub-responsabile del Trattamento. |
| Fornitori e/o destinatari esterni che operano in qualità di Titolari Autonomi | Riconoscono reciprocamente il ruolo di Titolare Autonomo ed operano in autonomia. |
| Contitolari | Partecipano alle attività di individuazione delle finalità e dei mezzi del trattamento definendo la ripartizione delle responsabilità |
| INTERESSATI ai sensi Privacy: Utenti dei Servizi erogati da ATAC S.p.A. | Tutela dei Diritti e Riscontri rispetto all'esercizio dei diritti degli interessati |
| Autorità Garante "Privacy" | Verifica la conformità con la normativa vigente in materia di Tutela del Trattamento dei Dati Personali |