



# MODELLO ORGANIZZATIVO GDPR 2018

ADOTTATO DAL L'AU IL ..... 2018



# **Modello Organizzativo sulla Riservatezza dei Dati Personali**

## **Normativa di Riferimento**

Dal 25 maggio 2018 è diventato operativo il **Regolamento Europeo per La Protezione dei Dati Personali EU 2016/679**, (in seguito **GDPR**), pubblicato sulla Gazzetta Ufficiale Europea il 4 maggio 2016 e avente valore di legge per tutti i paesi europei.

Il GDPR stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati.

Il GDPR protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.

Alla base del nuovo regolamento è il principio di responsabilità (Accountability) che informa tutta la struttura del GDPR.

Il nuovo regolamento abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

**AAMPS** spa si è dotata, ed è effettivo da tale data, di un modello organizzativo, tecnologico e di processo che soddisfa quanto richiesto dal GDPR. Sulla base di tali sistemi di gestione AAMPS spa ha messo in atto controlli, procedure, informative, meccanismi di miglioramento continui atti a rendere i trattamenti dei dati personali effettuati da essa e da eventuali Responsabili dei Trattamenti che, in suo nome e per suo conto, dovessero eseguirli, in linea con quanto previsto dal regolamento europeo.

**AAMPS** promuove il rispetto, da parte dei propri dipendenti e collaboratori, di alti valori morali e di integrità di condotta, imponendo il corretto utilizzo delle informazioni personali di cui entrano in possesso nello svolgimento della propria attività lavorativa.

**Utenti dei servizi, Fornitori, Dipendenti**, di AAMPS a seguito delle loro attività e delle loro richieste possono fornire dati personali che vengono trattati per lo svolgimento delle attività correlate.

Il **titolare per il loro trattamento** è:

AAMPS S.p.A. che ha sede in Via dell'artigianato, 39/B 57121 LIVORNO

## **Chi Siamo?**

AAMPS, **Azienda Ambientale di Pubblico Servizio SpA**, è la società in house che eroga i servizi connessi alla gestione del ciclo integrato dei rifiuti e alla pulizia stradale per il Comune di Livorno.

AAMPS svolge la propria attività nel rispetto dei principi di eguaglianza, imparzialità, continuità, partecipazione, efficienza, efficacia ed economicità.

Si impegna inoltre ad ascoltare le esigenze di istituzioni, aziende e cittadini, a confrontarsi con loro e a fornire informazioni aggiornate sui servizi e sui comportamenti ambientali virtuosi.

Il nostro Responsabile della Protezione dei Dati (DPO) può essere contattato direttamente:

- ([aamps@aamps.livorno.it](mailto:aamps@aamps.livorno.it))
- ([0586.416111](tel:0586416111))
- ([dpo@aamps.livorno.it](mailto:dpo@aamps.livorno.it))

## **Definizioni (Art. 4 GDPR)**

- **Dati personali**: 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;

- **Categorie particolari di dati personali** - dati personali che rivelano l'origine razziale o etnica, opinioni politiche, convinzioni religiose o filosofiche, o appartenenza sindacale e il trattamento di dati genetici, dati biometrici al fine di identificare in modo univoco una persona fisica, dati riguardanti la salute o dati riguardanti la vita sessuale o l'orientamento sessuale di una persona fisica.
- **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. Titolare del trattamento Organo Amministrativo di AAMPS spa

**DPO**: Il Responsabile della Protezione dei Dati, (di seguito solo "Data Protection Officer" o, in breve, "DPO") è la persona fisica nominata dal Titolare che ha il compito di supportare, coordinare e collaborare con tutte le strutture organizzative aziendali nella gestione di tematiche data protection e di sorvegliare l'osservanza dei requisiti normativi applicabili e delle politiche del Titolare. Il DPO svolge una funzione informativa e di consulenza sui principali adempimenti derivanti dal Regolamento, fornendo, se richiesto, pareri ed indicazioni in merito alla conduzione, valutazione e follow up conseguenza di valutazione d'impatto (o DPIA). Il DPO coopera con il Garante nel caso di verifiche ispettive e funge da punto di contatto per le richieste dei soggetti interessati nell'esercizio dei loro diritti. La Responsabile area Legale

- **Responsabile dell'Osservanza**: la persona fisica, munita di necessari poteri conferiti dal Titolare ha il compito di garantire che i trattamenti

effettuati dall'azienda siano svolti in conformità con il Regolamento e con la vigente normativa in materia di protezione dei dati personali.

Inoltre, il Responsabile dell'Osservanza è chiamato a supportare il Titolare nella definizione delle politiche aziendali in materia di data protection e assicura la conformità della documentazione aziendale ai requisiti del Regolamento, monitorando costantemente in coordinamento con il DPO, e con il supporto operativo della Funzione Legale, l'evoluzione del quadro normativo di riferimento. Il responsabile Area Progettazione e Servizi

- **Amministratore di sistema**: l'Amministratore di Sistema ricopre un ruolo estremamente delicato: progetta, sviluppa e gestisce l'infrastruttura di rete, i server, il software ed i servizi applicativi di base occupandosi spesso della sicurezza e della protezione dei dati e delle risorse. Responsabile CED
- **Responsabili dei dati**: Responsabili dei dati sono le persone fisiche preposte alla **conduzione delle strutture organizzative aziendali** coinvolte nelle operazioni di trattamento e hanno il **compito di supervisionare** lo svolgimento delle operazioni che vengono effettuate dai Referenti e dagli Incaricati che operano nell'ambito della propria struttura organizzativa e di assicurare il rispetto delle normative in materia di trattamento dei dati personali. Responsabili di Area Aziendale
- **Referenti di linea**: sono le persone fisiche che svolgono una funzione di supporto e raccordo, coadiuvando il Responsabile Dati nello svolgimento delle operazioni di trattamento di dati personali. La funzione Organizzazione, in accordo con i Responsabili dei dati, elabora/aggiorna l'elenco contenente i nominativi dei Referenti di Linea e lo rende disponibile sulla intranet aziendale. Tale elenco è comunque conservato presso la Funzione Organizzazione e reso tempestivamente disponibile, in caso di necessità, al DPO.
- **Incaricati del Trattamento**: le persone fisiche preposte alle operazioni di trattamento sotto la responsabilità dei Responsabili dei dati. Gli Incaricati svolgono le attività di trattamento in conformità alle istruzioni ricevute e alle politiche aziendali. Effettuano materialmente le operazioni di trattamento di dati personali contenuti in banche dati e negli archivi cartacei aziendali, nell'esercizio delle mansioni agli stessi affidate.

- **Interessato** - qualsiasi persona fisica vivente che è oggetto di dati personali detenuti da un'organizzazione.
  
- **Trattamento**  
qualsiasi operazione o insieme di operazioni eseguite su dati personali o su serie di dati personali, anche con strumenti automatizzati, quali raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o alterazione, reperimento, consultazione, uso, divulgazione mediante trasmissione, diffusione o altrimenti messa a disposizione, allineamento o combinazione, restrizione, cancellazione o distruzione.
  
- **Liceità (Art. 6 GDPR)**  
I Trattamenti effettuati da AAMPS avvengono esclusivamente nel rispetto dei criteri di liceità contenuti nel GDPR (ex art. 6) ed in particolare solo dietro consenso dell'interessato o per l'esecuzione di un obbligo contrattuale o di legge. Per i dati particolari sarà inoltre richiesto un consenso espresso in modo chiaro ed esplicito.
  
- **Consenso**  
Nei casi in cui il trattamento sia basato sul consenso dovrà essere concesso in forma scritta oppure in forma digitale attraverso il sito istituzionale o comunque in forma dimostrabile e solo dopo aver letto attentamente la relativa informativa. In caso di dati particolari per i quali si applicano le eccezioni di cui al par. 2 ex art. 9 del GDPR verrà richiesto un consenso esplicito  
In caso di minori di anni 16 sarà necessario il consenso dell'autorità genitoriale (ex. art.8)  
È possibile revocare il consenso in qualsiasi momento
  
- **Cessione dei Dati a Terzi**  
AAMPS spa non trasferirà i suoi dati personali a terze parti senza aver ottenuto preventivamente il suo consenso.
  
- **Periodo di conservazione**

AAMPS spa tratterà i dati personali per saranno trattati esclusivamente per le finalità connesse alle attività aziendali con strumenti automatizzati per il tempo strettamente necessario a conseguire gli scopi per cui sono stati raccolti. Specifiche misure di sicurezza sono osservate per prevenire la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati. AAMPS archiverà i dati personali per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali sono stati raccolti o successivamente trattati, conformemente a quanto previsto dagli obblighi di legge.

### **Cookies**

Nessun dato personale degli utenti viene in proposito acquisito dal sito di AAMPS`www.aamps.livorno.it.

Non viene fatto uso di *cookies* per la trasmissione di informazioni di carattere personale, né vengono utilizzati c.d. *cookies* persistenti di alcun tipo, ovvero sistemi per il tracciamento degli utenti.

L'uso di c.d. *cookies* di sessione (che non vengono memorizzati in modo persistente sul computer dell'utente e svaniscono con la chiusura del browser) è strettamente limitato alla trasmissione di identificativi di sessione (costituiti da numeri casuali generati dal *server*) necessari per consentire l'esplorazione sicura ed efficiente del sito.

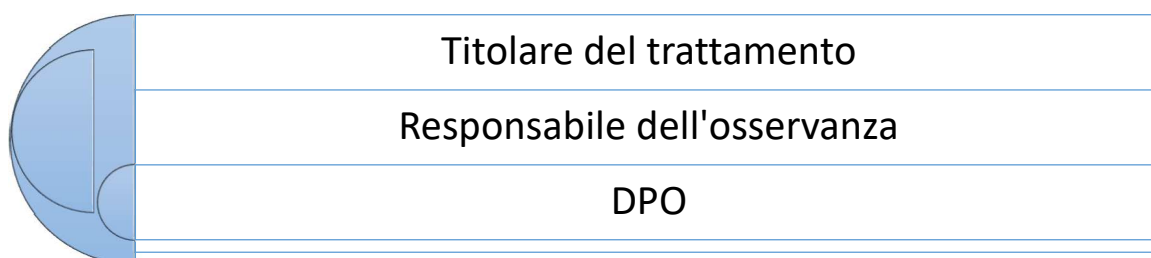
I c.d. *cookies* di sessione utilizzati in questo sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

Il modello organizzativo di AAMPS si articola su tre livelli:

- **Governo:** i ruoli coinvolti in questa attività determinano il sistema di Governance applicabile ai trattamenti effettuati dall'azienda e definiscono le decisioni strategiche e le linee guida in materia di Data Protection applicabili sia alla capogruppo sia alle controllate.
- **Sorveglianza:** il DPO è deputato alla verifica della conformità del sistema di gestione dei dati alla normativa.

- Attuazione e Gestione: le figure coinvolte in queste attività danno attuazione alle decisioni aziendali e hanno cura di effettuare i trattamenti nel rispetto delle linee guida elaborate e dettagliate dal titolare e dai ruoli deputati alla Governance.

#### GOVERNO



#### ATTUAZIONE e GESTIONE

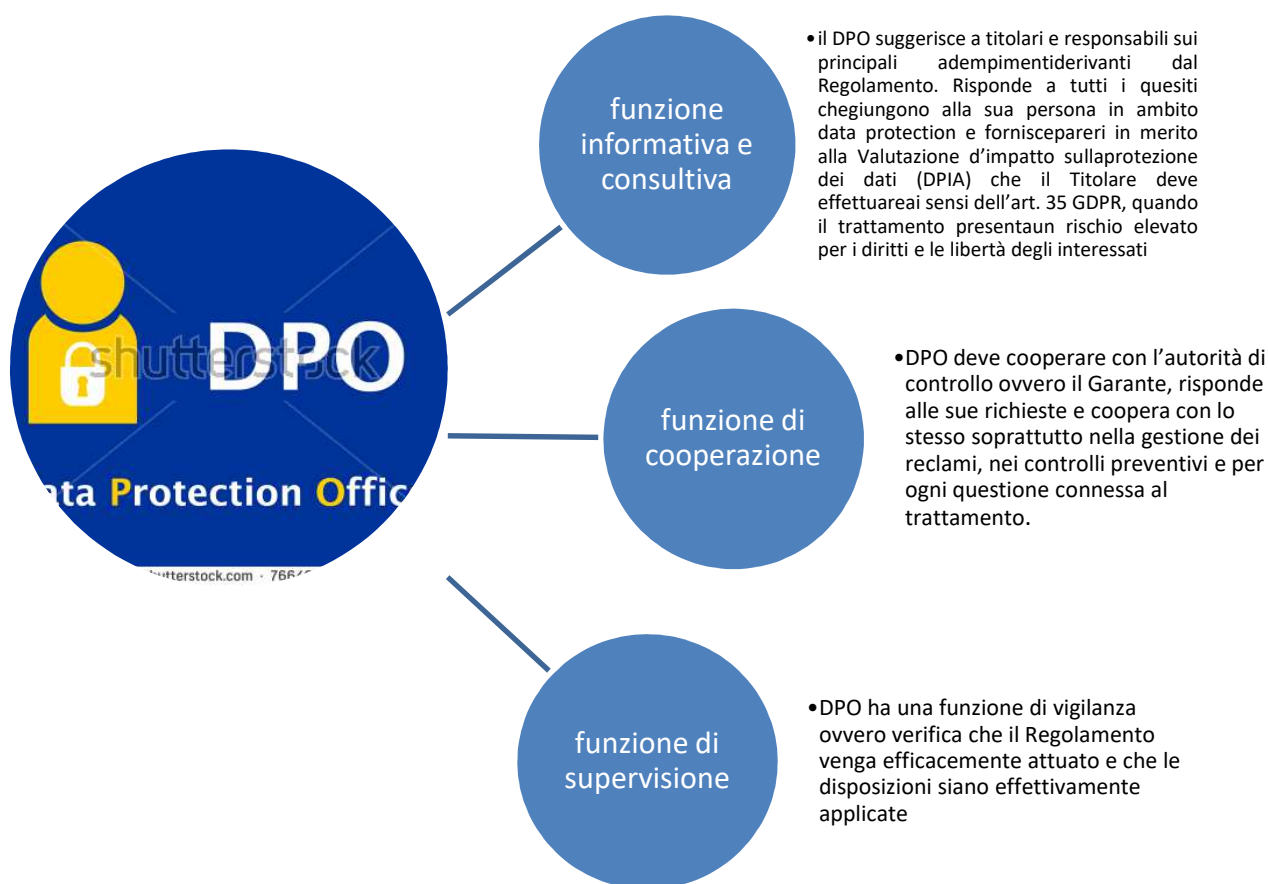


#### IL DPO

È la persona fisica nominata dal Titolare avente il compito di controllo,



informazione e consulenza in merito alla normativa in materia di Data Protection (art. 37 GDPR ) le principali funzioni sono rappresentate nello schema che segue:



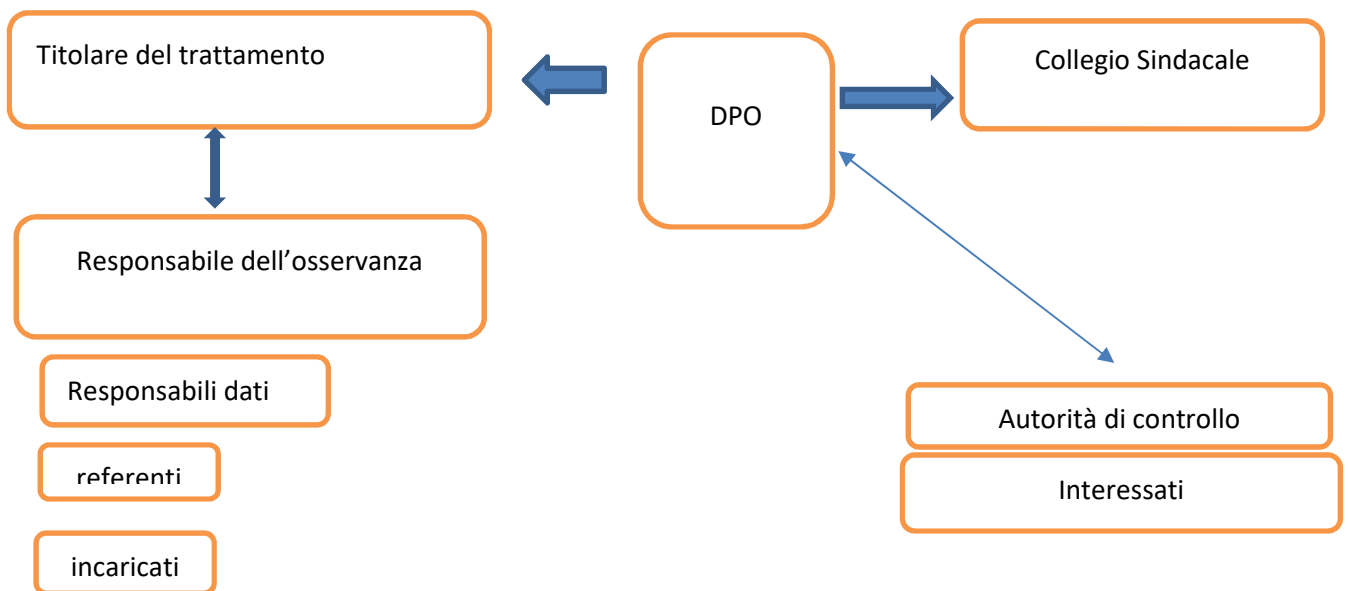
Il DPO riferisce almeno una volta all'anno all'Organo Amministrativo e agli Organi di Controllo in merito al livello di conformità al Regolamento, all'osservanza della normativa e delle politiche aziendali in materia di data protection, all'attuazione del Modello Organizzativo Data Protection, agli esiti dell'attività di vigilanza svolta e formula suggerimenti per il miglioramento del modello.

In particolare, il DPO riporta

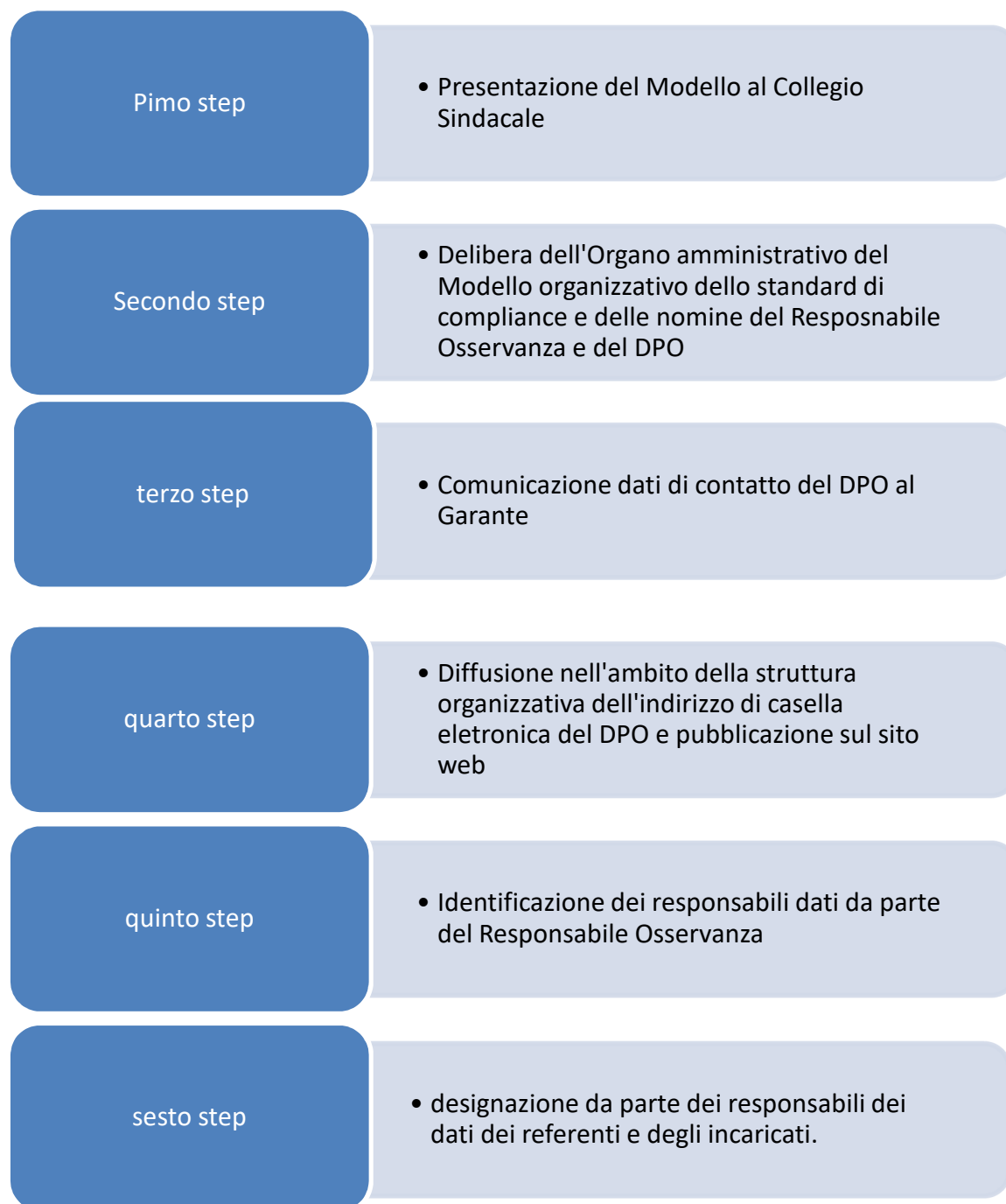
- in maniera continuativa al Consiglio di Amministrazione e agli Organi di Controllo, in ogni circostanza in cui lo ritenga necessario e/o opportuno per l'attuazione degli obblighi previsti dal Regolamento, fornendo ogni informazione rilevante e/o utile per il corretto adempimento delle prescrizioni del Regolamento;
- attraverso una relazione scritta al Consiglio di Amministrazione con periodicità almeno annuale, sulle attività svolte, sulle richieste degli interessati, sulle richieste dell'autorità di controllo, sui suggerimenti in

merito agli interventi correttivi da adottare per rimuovere eventuali disallineamenti riscontrati.

### **Flussi informativi del Modello Organizzativo**



## **Ruoli e responsabilità**



AAMPS ha descritto nello standard di compliance i punti cardine su cui si fonda il modello organizzativo le responsabilità e le figure chiave dell'Organigramma privacy.

Lo standard di compliance costituisce, pertanto elemento essenziale del Modello

Le figure chiave del modello sono quelle riportate nelle pagine iniziali del presente documento di seguito riassunte.

