REGOLAMENTO DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Approvato dal Consiglio di Amministrazione con deliberazione del 31.03.2023

INDICE

1. Premessa 3
2. Titolare del Trattamento dei dati 3
3. Designato del Trattamento 6
4. Persone autorizzate al trattamento 7
5. Responsabile del Trattamento 8
6. Responsabile della Protezione Dati 10
7. Amministratore di Sistema, di Rete e di Base Dati 16
8. Finalità del trattamento dei dati di AMET 17
9. Sicurezza del trattamento 18
10. Registro delle attività di trattamento 19
11. Registro delle categorie di attività trattate dai Responsabili del trattamento 20
12. Valutazioni d'impatto sulla protezione dei dati 21
13. Violazione dei dati personali 24
14. Diritto di accesso dell'interessato ai dati personali 26
15. Glossario 27
16. Allegati 29

1. Premessa

Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento Europeo (UE) 2016/679 (Regolamento Generale sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali, di seguito "Regolamento" o "GDPR" ossia *General Data Protection Regulation*), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, dell'AMET S.p.A. (di seguito "AMET" oppure "Società") con sede in Via Barletta 156, 76125 Trani.

2. Titolare del Trattamento dei dati

1. L'AMET S.p.A. rappresentata ai fini previsti dal GDPR dal Presidente, è il Titolare del trattamento dei dati personali (di seguito indicato con "Titolare") raccolti o meno in banche dati automatizzate o archivi cartacei, come definiti dall'art. 4 par. 1, n. 6 del GDPR. Il Presidente può delegare le relative funzioni al Dirigente in possesso di adeguate competenze, quale Designato al trattamento dati § art. 4.

2. Il Titolare del trattamento è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare del trattamento mette in atto misure tecniche ed organizzative adeguate a garantire ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR (art. 24 GDPR). Tali misure sono riesaminate e aggiornate se necessario.

4. Adotta le misure tecniche e organizzative, quali la pseudonimizzazione e la minimizzazione, fin dalla fase di progettazione (privacy by design) per garantire che siano trattati per impostazione predefinita (privacy by default) solo i dati necessari per ogni specifica finalità di trattamento;

5. Le misure definite sono messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

6. Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa, di bilancio e di Piano esecutivo di Gestione, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

7. Il Titolare del trattamento adotta misure appropriate per fornire all'interessato, ovverosia la persona fisica identificata o identificabile, le seguenti informazioni:

   a. le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;

   b. le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non stati ottenuti presso lo stesso interessato.

   c. le informazioni per agevolare l'esercizio dei diritti ai sensi degli articoli da 15 a22 GDPR;

   d. ogni comunicazione relativa ad eventuali violazione dei dati personali (data breach) ai sensi dell'art. 34 del RGPD.

8. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA", "Data Protection Impact Assessment"), ai sensi dell'art. 35, GDPR, considerando la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

9. Il Titolare, inoltre, provvede:

   a. alla tenuta del registro delle attività di trattamento (art. 30, paragrafo 1, GDPR) svolte sotto la propria responsabilità;

   b. designare con atto formale di nomina il *Responsabile della Protezione dei Dati* (di seguito indicata con "RPD");

c. ad attribuire specifici compiti e funzioni connessi al trattamento dei dati, nominando con atto formale, i *Designati al trattamento dei dati con funzioni di responsabilità* (ai sensi del comma 1 e 2 dell'art. 2 quaterdecies del D.lgs. 10 agosto 2018 n.101, del Regolamento UE 2016/679), le figure si riferimento delle singole strutture in cui si articola la Società, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza.

   Il Designato al trattamento, connesso all'espletamento dei compiti istituzionali della Società, deve svolgerli sotto la diretta sorveglianza e secondo le istruzioni di questa, che conserva la qualità di "titolare del trattamento", non deve comportare decisioni di fondo sulle finalità e sulle modalità di utilizzazione dei dati, ma limitati margini di autonomia in ordine al concreto svolgimento del servizio ed a scelte tecnico-operative dettagliatamente specificato nell'atto formale di incarico.

d. designare con atto formale di nomina, direttamente o indirettamente tramite specifiche deleghe di funzioni ai designati, le *Persone Autorizzate al trattamento dei dati,* (ai sensi del Considerando 29 e art. 28.3 lett. b) del Regolamento UE 2016/679) ossia il personale interno afferente alle singole strutture in cui si articola la Società che sono preposti al trattamento dei dati contenuti negli archivi esistenti nelle articolazioni organizzative di loro competenza.

e. designare con atto formale di nomina, direttamente o indirettamente tramite specifiche deleghe di funzioni ai designati, i *Responsabili del trattamento dei dati,* (ai sensi dell'art. 28 del Regolamento UE 2016/679) ossia quei soggetti pubblici o privati affidatari di attività e servizi per conto dell'AMET, relativamente alle banche dati gestite da soggetti esterni alla stessa in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

f. predisporre l'elenco dei, Designati, Persone Autorizzate e dei Responsabili del trattamento delle strutture in cui si articola la Società;

10. L'AMET favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

3. Designato del Trattamento

1. L'Amministratore Delegato, i Consiglieri del Consiglio di Amministrazione ed i Dirigenti in cui si articola la Società, sono nominati *Designati del trattamento con specifiche funzione di responsabilità* (articolo 2-quaterdecies D.lgs. 101/08), di tutte le banche dati personali esistenti nell'articolazione organizzativa dell'area di rispettiva competenza. Il Designato deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

2. Il Designato del trattamento dei dati provvede, relativamente all'articolazione organizzativa di rispettiva competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare a seconda della soggettiva nomina può provvedere:

   a) alla designazione con atto formale di nomina, delle Persone Autorizzate al trattamento dei dati, ossia il personale interno afferente alle singole strutture in cui si articola la Società che sono preposti al trattamento dei dati contenuti negli archivi esistenti nelle Aree Organizzative di propria competenza.
   b) alla tenuta del registro delle attività di trattamento svolte per conto del Titolare (art. 30, paragrafo 1, GDPR) sotto la propria responsabilità;
   c) all'adozione di idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti (art. 32 GDPR);
   d) alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo (art. 29 GDPR);
   e) ad assistere il Titolare e l'RPD nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso (artt. 35-36 GDPR);
   f) ad informare il Titolare e l'RPD, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati (art. 33 GDPR).

3. Il Designato del trattamento dei dati è nominato, mediante atto formale sottoscritto dal Presidente, nel quale sono tassativamente disciplinati:

   - le specifiche deleghe di funzione (esempio nominare le Persone autorizzate, etc.)
   - l'ambito del trattamento al quale si è autorizzati, consentendo, in ottica di "accountability", di dare seguito agli adempimenti organizzativi interni alla struttura

del Titolare che può conferire autorizzazioni/istruzioni privacy alle figure organizzative di vario livello ed essere in grado di dimostrare che il trattamento è effettuato conformemente al GDPR.

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

4. Il Designato del trattamento dei dati deve essere in possesso di apposita formazione ed istruzione ed è sottoposto ad obbligo legale di riservatezza

5. Il Designato del trattamento dei dati di ciascuna struttura organizzativa della Società, per l'esecuzione di specifiche attività di trattamento per conto del Titolare (elaborando o utilizzando materialmente i dati personali) deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, individuato per iscritto e che opera sotto la diretta autorità del Titolare, attuandone le istruzioni.

4. Persone autorizzate al trattamento

1. Le Persone Autorizzate al trattamento dei dati personali (all'art. 28 co.3 lettera b), Considerando 29 del Regolamento) sono le persone fisiche (non anche le entità personificate), con diversi livelli di delega, effettuano materialmente le operazioni di trattamento sui dati personali e pertanto autorizzate a compiere le operazioni di trattamento sotto la direzione e vigilanza del Titolare o del Designato che li ha nominati tali, relativi all'articolazione organizzativa di rispettiva competenza. In particolare, le operazioni di trattamento possono essere effettuate solo da Persone Autorizzate che operano sotto la diretta autorità del Titolare o del Designato che li ha nominati tali, attenendosi alle istruzioni impartite e impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza.

2. Spetta, inoltre, al Titolare con il supporto del Designato del trattamento dei dati:

- organizzare le Persone Autorizzate nei loro compiti in maniera che le singole operazioni di trattamento risultino coerenti con le disposizioni legislative in materia e, facendo in modo che, sulla base delle istruzioni operative impartite, i trattamenti non si discostino dalle finalità istituzionali per cui i dati stessi sono stati raccolti;
- vigilare sulle Persone Autorizzate per la corretta applicazione delle istruzioni impartite;
- svolgere un'opera di sensibilizzazione nei confronti delle Persone Autorizzate,

orientata agli aspetti normativi e procedurali inerenti al trattamento dei dati personali, avendo specifico riguardo alle tipologie di dati e trattamenti effettuati nello svolgimento delle rispettive mansioni.

3. Le Persone Autorizzate sono nominate, dal Presidente o dal Designato, mediante atto formale, nel quale sono tassativamente disciplinati:

   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;

   Inoltre, la nomina individua puntualmente l'ambito del trattamento consentito. Si considera tale anche la documentata preposizione della persona fisica ad un'unità per la quale è individuato, per iscritto, l'ambito del trattamento consentito agli addetti all'unità medesima. Tale designazione è, infatti, indispensabile, in quanto permette di considerare legittimo il flusso delle informazioni personali nell'ambito degli uffici e tra i dipendenti della Società Titolare del trattamento.

4. In assenza di una formale designazione come incaricati del trattamento, i dipendenti della Società che, per lo svolgimento dei propri compiti, vengono a conoscenza di dati personali, devono essere considerati come soggetti terzi rispetto alla Società stesso, con conseguenti rilevanti limiti per la comunicazione e l'utilizzazione dei dati e quindi per la liceità del trattamento.

5. Le Persone Autorizzate devono essere in possesso di apposita formazione ed istruzione e sono sottoposte ad obbligo legale di riservatezza.

6. Le Persone Autorizzata della struttura organizzativa della Società, per l'esecuzione di specifiche attività di trattamento per conto del Titolare (elaborando o utilizzando materialmente i dati personali) devono essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, individuato per iscritto e che opera sotto la diretta autorità del titolare, attuandone le istruzioni.

5. Responsabile del Trattamento

1. Il *Responsabile del Trattamento* è indicato come (art. 4 del GDPR) "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento"

2. Il Titolare può avvalersi, per il trattamento di dati personali, anche particolari ai sensi dell'art. 9 del GDPR, di persone fisiche o giuridiche, autorità pubbliche, servizi o altri organismi nonché soggetti esterni all'AMET, che, in qualità di Responsabili del trattamento ai sensi dell'art. 28 e 29 del GDPR, forniscano garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

7. Il Responsabile del Trattamento è nominato, mediante atto formale sottoscritto dal Presidente, nel quale sono tassativamente disciplinati:

   - riferimento per relationem al contratto stipulato con la specifica Area Organizzativa;
   - la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
   - il tipo di dati personali oggetto di trattamento e le categorie di interessati;

   Pertanto, le Aree Organizzative collaborano con il Titolare del trattamento, individuando puntualmente l'ambito del trattamento consentito contestualizzato con i contratti.

3. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, paragrafo 3, del GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

4. E' consentita, ex art. 28, paragrafi 2 e 4 GDPR, la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali, ex art. 28, paragrafo 3 GDPR, che legano il Titolare ed il Responsabile primario previa autorizzazione scritta, specifica o generale del Titolare stesso; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito. Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia

impegnato alla riservatezza o abbia un adeguato obbligo legale di riservatezza (art.29 GDPR).

6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:
   - alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare (art. 30, paragrafo 2, GDPR);
   - all'adozione di idonee misure tecniche e organizzative adeguate a garantire la sicurezza dei trattamenti (art. 32 GDPR);
   - alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo (art. 29 GDPR);
   - alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare ai sensi dell'art. 37 GDPR;
   - ad assistere il Titolare e l'RPD nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso (artt. 35-36 GDPR);
   - ad informare il Titolare e l'RPD, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati (art. 33 GDPR).

6. Responsabile della Protezione Dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") ai sensi dell'art. 37 GDPR, è designato dal Titolare, con apposito atto formale, in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati personali.

2. Il RPD è incaricato dei seguenti compiti ex art. 39 del GDPR:

   a. informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati. In tal senso, il RPD può indicare al Titolare e/o al Responsabile del trattamento:

- i settori funzionali ai quali riservare un audit interno o esterno in tema di protezione dei dati,
- le attività di formazione interna per i dipendenti che trattano dati personali,
- i trattamenti ai quali dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b. sorvegliare sull'osservanza e sull'attuazione del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.

   Fanno parte di questi compiti, la raccolta di informazioni per individuare i trattamenti svolti:

   - l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c. sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d. fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento ai sensi dell'art. 35 del GDPR. Il Titolare, in particolare, si consulta con il RPD sulle seguenti questioni:

   - valutare la necessarietà di redigere di una DPIA;
   - quale metodologia adottare nel condurre una DPIA;
   - se condurre la DPIA con le risorse interne ovvero esternalizzandola;
   - quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i
   - rischi delle persone interessate;
   - se la DPIA sia stata condotta correttamente o meno,
   - se le conclusioni raggiunte (procedere o meno con il trattamento e quali salvaguardie applicare) siano conformi al GDPR;

e. cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per l'Autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso,

consultazioni relativamente a qualunque altra questione. A tali fini, il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f. eseguire i propri compiti considerando debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento stesso.

g. riferire al vertice gerarchico del Titolare del trattamento o del Responsabile del trattamento.

h. altri compiti e funzioni, a condizione che il Titolare o il Responsabile del trattamento si siano assicurati che non venga dato adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

3. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

   - il RPD è invitato a partecipare alle riunioni di coordinamento dell'AMET, che abbiano per oggetto questioni inerenti alla protezione dei dati personali;
   - il RPD deve disporre tempestivamente di tutte le informazioni pertinenti alle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
   - il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio, ma non vincolante. Nel caso in cui la decisione assunta dal Titolare determini condotte difformi da quelle raccomandate dal RPD, è necessario che essa sia specificamente motivata;
   - il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio della Società.

5. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti, da parte del Dirigente e dei relativi Responsabili, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa di bilancio;
- tempo sufficiente per l'espletamento dei suoi compiti;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno della Società;
- accesso garantito ai settori funzionali della Società, così da fornirgli supporto, informazioni e input essenziali.

6. Il RPD supporta la Società nella realizzazione degli adempimenti necessari ad adeguarsi al Regolamento Europeo nella prima fase di applicazione, in particolare:

a. Promuove aggiornamenti e modifiche al Regolamento per la gestione della privacy, secondo le indicazioni cogenti del Garante della protezione dei dati personali ed in caso di modifiche strutturali e/o organizzative della Società.

b. Fornisce consulenza circa la predisposizione ed aggiornamento da parte di ciascuna Società del Registro delle attività di trattamento, di cui all'art. 30 del GDPR, per una ricognizione dettagliata dei trattamenti di dati personali svolti dalla Società e verifica che questi avvengono nel rispetto dei principi fondamentali, del principio di liceità e abbiano un fondamento giuridico.

All'interno del registro, da predisporre in formato elettronico e/o cartaceo, saranno specificati nome e contatti di riferimento del titolare del trattamento e del RPD, i trattamenti svolti e le loro principali caratteristiche specificando per ognuno:

- finalità del trattamento;
- categorie di dati personali coinvolti;
- descrizione soggetti interessati;
- categorie di destinatari cui è prevista la comunicazione di tali dati;
- eventuali trasferimenti di dati a paesi terzi;
- misure di sicurezza tecniche/organizzative previste dall'art. 32 del Regolamento al fine di garantire un livello di sicurezza dei trattamenti adeguato al rischio;
- tempi di conservazione dati;
- ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte.

c. Fornisce un parere sui trattamenti dei dati che potrebbero generare un elevato rischio per la libertà e i diritti della persona fisica ai fini della redazione da parte dei Titolari della Valutazione d'impatto sulla protezione dei dati (art. 35 del regolamento europeo). La valutazione è svolta dalle Società, in particolare nei casi seguenti:

- aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'art. 9, par. 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione d'impatto contiene ai sensi del paragrafo 7 dell'articolo 35 del GDPR:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 dell'articolo 35 del GDPR:
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

d. Sorveglia e fornisce consulenza ai Titolari sull'attuazione ovvero aggiornamento delle misure tecniche ed organizzative e sugli atti e documenti per garantire che le operazioni di trattamento vengano effettuate in conformità alla nuova disciplina.

e. Fornisce supporto al Titolare, in accordo con le Figure competenti, circa le azioni necessarie per l'adeguamento alle disposizioni AGID in materia di misure idonee per la sicurezza informatica.

f. Fornisce consulenza sulle problematiche relative alla tutela dei dati personali e alla sicurezza informatica.

g. Programma almeno due giornate all'anno di supporto e formazione interna, dedicate ai dipendenti dell'AMET. Resta inteso che in caso di modifiche normative sostanziali si programmerà un intervento formativo ad hoc.

7. Le attività descritte al punto 2 costituiscono altresì oggetto del servizio.

8. Al fine di poter espletare al meglio il servizio, è riconosciuta al RPD la possibilità di accedere agli archivi, di assumere informazioni dagli autorizzati al trattamento, chiedere informazioni e documenti su circostanze specifiche ed eventi accaduti, segnalando eventuali inosservanze al Titolare del trattamento.

9. Nello svolgimento dei compiti affidatigli il RPD dovrà:

   a. svolgere i compiti che gli spettano secondo quanto previsto dal presente Regolamento osservando le norme in materia di segreto, riservatezza e confidenzialità, la normativa nazionale ed europea vigente in materia;

   b. utilizzare le eventuali risorse che il Titolare e i Responsabili del trattamento gli forniscano al fine di assolvere al meglio ai compiti attribuitigli dalla legge, accedere ai dati personali e ai trattamenti nonché di rafforzare la propria conoscenza specialistica;

   c. operare in modo indipendente;

   d. riferire direttamente al Presidente dell'AMET, qualora ritenga che il Responsabile e/o il Titolare del trattamento assumano decisioni incompatibili con il GDPR;

   e. informare immediatamente il Presidente dell'AMET, qualora sia destinatario di qualsiasi atto di intimidazione nel corso del proprio servizio che abbia l'obiettivo di condizionarne la regolare e corretta esecuzione;

   f. mettere a disposizione un recapito postale, telefonico fisso e/o mobile ed un indirizzo di posta elettronica utili alla reperibilità.

10. Durante lo svolgimento del servizio, il Titolare del Trattamento dovrà:

   a. Coinvolgere tempestivamente ed adeguatamente il RPD per mezzo del Designato in qualsiasi questione inerente la protezione dei dati personali.

b. Mettere a disposizione del RPD le risorse necessarie all'esecuzione dei propri compiti, il Referente ed eventualmente un gruppo di lavoro, formato dai Responsabili del Trattamento, in possesso delle competenze tecniche e informatiche e della necessaria conoscenza dei procedimenti e dei processi di lavoro delle Società.

c. Garantire che il RPD eserciti le proprie funzioni in autonomia e indipendenza e, in particolare, non assegnando allo stesso attività o compiti che risultino in contrasto o conflitto d'interesse.

11. Il Titolare ed il Designato forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare, è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti, da parte del Designato e dei relativi Responsabili, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa di bilancio;
- comunicazione tempestiva al fine di espletare in maniera regolare i suoi compiti;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno della Società;
- accesso garantito ai settori funzionali della Società, così da fornirgli supporto, informazioni e input essenziali.

7. Amministratore di Sistema, di Rete e di Base Dati

L'amministratore di sistema è nominato dal Presidente, mediante atto formale sottoscritto con l'attribuzione delle funzioni che deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto nominato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

La designazione quale amministratore di sistema deve essere in ogni caso individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.

Con la definizione di "amministratore di sistema" si individuano generalmente, in ambito informatico, figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti. Ai fini del presente provvedimento vengono però

considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli amministratori di basi di dati, gli amministratori di reti e di apparati di sicurezza e gli amministratori di sistemi software complessi.

Gli amministratori di sistema così ampiamente individuati, pur non essendo preposti ordinariamente a operazioni che implicano una comprensione del dominio, nelle loro consuete attività sono, in molti casi, concretamente "responsabili" di specifiche fasi lavorative che possono comportare elevate criticità rispetto alla protezione dei dati.

Attività tecniche quali il salvataggio dei dati (backup/recovery), l'organizzazione dei flussi di rete, la gestione dei supporti di memorizzazione e la manutenzione hardware comportano infatti, in molti casi, un'effettiva capacità di azione su informazioni che va considerata a tutti gli effetti alla stregua di un trattamento di dati personali; ciò, anche quando l'amministratore non consulti "in chiaro" le informazioni medesime.

8. Finalità del trattamento dei dati di AMET

L'AMET raccoglie i dati personali per finalità determinate, esplicite e legittime. I trattamenti dei dati personali operati dal Titolare sono compiuti per le seguenti finalità inerenti all'oggetto sociale. In particolare, provvede:

a) all'acquisto, all'approvvigionamento di energia elettrica all'ingrosso e dei connessi servizi di dispacciamento, dei servizi di trasmissione, distribuzione e misura per la consegna dell'energia elettrica al punto di prelievo dei clienti finali in maggior tutela, nonché le operazioni svolte per la gestione del rapporto commerciale con il cliente come la fatturazione e la gestione dei pagamenti, inclusi il recupero e la cessione dei crediti.

b) distribuzione Reti Trani gestisce il servizio di distribuzione di energia elettrica nel comune di Trani.

c) gestisce la darsena che può ospitare circa 400 imbarcazioni di lunghezza comprese tra i 4 e i 40 metri.

d) gestisce Trasporto Pubblico Urbano.

e) Gestisce Trasporto Scolastico.

f) Gestione i parcheggi urbani.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.

a. l'adempimento di un obbligo legale al quale è soggetta l'AMET La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina.;

b. l'esecuzione di un contratto con soggetti interessati;

c. il perseguimento del legittimo interesse del titolare;

d. per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

9. Sicurezza del trattamento

1. Il Titolare, il Designato al trattamento e/o Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate a garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono ai sensi dell'art. 32 GDPR: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Designato:

   a. sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);

   b. misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di

archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Titolare, il Designato al trattamento e/o Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi).

10. Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca le seguenti informazioni:

   a. il nome ed i dati di contatto dell'AMET, del Presidente, del RPD, del soggetto delegato dal Titolare alla tenuta ed aggiornamento del Registro;

   b. le finalità del trattamento;

   c. la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

   d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

   e. l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

   f. ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

   g. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art. 8.

2. Il Registro è tenuto ed aggiornato dal Titolare ovvero del soggetto delegato, nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative della Società.

3. Il Titolare tiene un Registro dei trattamenti che contiene le informazioni di cui ai commi precedenti nonché le categorie di trattamenti effettuati dal Designato nonché Responsabile del trattamento: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali.

4. Il Designato al trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

11. Registro delle categorie di attività trattate dai Responsabili del trattamento

1. Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento di cui al precedente art. 10, per conto dell'AMET reca le seguenti informazioni:

   a. il nome ed i dati di contatto del Responsabile del trattamento, di ogni titolare del trattamento per conto del quale agisce e del DPO;

   b. le categorie di trattamenti effettuati: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;

   c. l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

   d. il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.8;

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema allegato alla nomina del Responsabile del trattamento.

12. Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, GDPR.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

   a. trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

   b. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

   c. monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

   d. trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, GDPR;

   e. trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di

trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f. combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g. dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti della Società, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i. tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno all'AMET. Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA. Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria. Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale. Il responsabile della sicurezza dei sistemi informativi aziendale può proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

   - se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
   - se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
   - se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;
   - se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

   Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RPD e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

   a. descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

   b. valutazione della necessità e proporzionalità dei trattamenti, sulla base:

      - delle finalità specifiche, esplicite e legittime;
      - della liceità del trattamento;
      - dei dati adeguati, pertinenti e limitati a quanto necessario;
      - del periodo limitato di conservazione;
      - delle informazioni fornite agli interessati;
      - del diritto di accesso e portabilità dei dati;
      - del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
      - dei rapporti con i responsabili del trattamento;
      - delle garanzie per i trasferimenti internazionali di dati;

- della consultazione preventiva del Garante privacy;

c. valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d. individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

13. Violazione dei dati personali

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'AMET.

2. Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Designato e/o il Responsabile del trattamento a conoscenza della violazione, è obbligato ad informare tempestivamente il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

   - danni fisici, materiali o immateriali alle persone fisiche;
   - perdita del controllo dei dati personali;
   - limitazione dei diritti, discriminazione;
   - furto o usurpazione d'identità;
   - perdite finanziarie, danno economico o sociale.
   - decifratura non autorizzata della pseudonimizzazione;
   - pregiudizio alla reputazione;
   - perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

   - coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
   - riguardare categorie particolari di dati personali;
   - comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
   - comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
   - impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33 del GDPR come da allegato 1 al presente Regolamento

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

14. Diritto di accesso dell'interessato ai dati personali

In applicazione dell'art. 15 del GDPR (Diritto di accesso dell'interessato), l'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali e alle seguenti informazioni:

a) le finalità del trattamento;
b) le categorie di dati personali in questione;
c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
f) il diritto di proporre reclamo a un'autorità di controllo;
g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Nel caso in cui intenda presentare ricorso per fatti inerenti al trattamento dei propri dati personali, egli dovrà rivolgere istanza scritta come da modello allegato 2 al presente regolamento, inviandola a:

- Piazza Plebiscito, 20, 76125 Trani BT

L'interessato, nell'esercizio dei diritti sopra riportati, può conferire, per iscritto, delega o procura a persone fisiche o ad associazioni.

15. Glossario

Ai fini del presente Regolamento, si intende per:

- **Titolare del trattamento:** la Società giuridica, la persona fisica o altro ente locale, proprietario dei dati, che singolarmente o insieme ad altri determina finalità e i mezzi del trattamento di dati personali.

- **Designato del trattamento:** ai sensi dell'Art. 2-quaterdecies del D.lgs. 101 del 10.08.2018, Il titolare può prevedere, sotto la propria responsabilità e nell'ambito del proprio assetto organizzativo, che specifici compiti e funzioni connessi al trattamento di dati personali siano attribuiti a persone fisiche, espressamente designate, che operano sotto la loro autorità.

- **Persona Autorizzata al trattamento:** il dipendente della struttura organizzativa dell'AMET, nominato dal Designato nell'articolazione organizzativa di rispettiva competenza, per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento (elabora o utilizza materialmente i dati personali).

- **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"

- **Responsabile per la protezione dati – RPD:** il dipendente della struttura organizzativa dell'AMET, il professionista privato o impresa esterna, incaricato dal Titolare del trattamento.

- **Registri delle attività di trattamento:** elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento secondo le rispettive competenze.

- **DPIA - Data Protection Impact Assessment - Valutazione d'impatto sulla protezione dei dati:** è una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali.

- **Garante Privacy**: il Garante per la protezione dei dati personali istituito dalla Legge 31 dicembre 1996 n. 765, quale autorità amministrativa pubblica di controllo indipendente.

Ai fini del Registro Unico delle attività di trattamento, si intende per:

- **Categorie di trattamento:** Raccolta; registrazione; organizzazione; strutturazione;

conservazione; adattamento o modifica; estrazione; consultazione; uso; comunicazione mediante trasmissione; diffusione o qualsiasi altra forma di messa a disposizione; raffronto od interconnessione; limitazione; cancellazione o distruzione; profilazione; pseudonimizzazione; ogni altra operazione applicata a dati personali.

- **Categorie di dati personali:** Dati identificativi: cognome e nome, residenza, domicilio, nascita, identificativo online (username, password, customer ID, altro), situazione familiare, immagini, elementi caratteristici della identità fisica, fisiologica, genetica, psichica, economica, culturale, sociale. Dati inerenti allo stile di vita Situazione economica, finanziaria, patrimoniale, fiscale. Dati di connessione: indirizzo IP, login, altro. Dati di localizzazione: ubicazione, GPS, GSM, altro.

- **Finalità del trattamento:** Esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: funzioni amministrative inerenti la popolazione ed il territorio, nei settori organici dei servizi alla persona, alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico; la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica; l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all'AMET. Adempimento di un obbligo legale al quale è soggetto l'AMET. Esecuzione di un contratto con i soggetti interessati. Altre specifiche e diverse finalità.

- **Misure tecniche ed organizzative:** Pseudonimizzazione; minimizzazione; cifratura; misure specifiche per assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; procedure specifiche per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento; altre misure specifiche adottate per il trattamento di cui trattasi. Sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro) adottati per il trattamento di cui trattasi ovvero dal Servizio/Ente nel suo complesso. Misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature; sistemi di copiatura e conservazione archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico - adottati per il trattamento di cui trattasi ovvero dal Servizio/Società nel suo complesso. Procedure per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

- **Dati sensibili:** Dati inerenti all'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, la salute, la vita o l'orientamento sessuale, dati genetici e biometrici, dati relativi a condanne penali.

- **Categorie interessati:** Viaggiatori; utenti; minori di anni 16; dipendenti; amministratori; fornitori; altro.

- **Categorie destinatari:** Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.

16. Allegati

Del presente Regolamento fanno parte integrante i seguenti allegati:

- Nomina Responsabile della protezione dei dati
- Nomina Designato al Trattamento dei dati - sotto diretta autorità - DIPENDENTI
- Nomina Designato al Trattamento dei dati - sotto propria autorità – ESTERNI
- Nomina Autorizzato al Trattamento dei dati
- Nomina Amministratore di Sistema
- Nomina Responsabile del trattamento dei dati