Regolamento per l'attuazione del

Regolamento UE 2016/679 relativo alla protezione ed il trattamento dei dati personali

Art. 1 - Oggetto

Art. 2 - Titolare del trattamento

Art. 3 - Finalità del trattamento

Art. 4 - Responsabile del trattamento

Art. 5 - Responsabile della protezione dati

Art. 6 – Incaricato trattamento dati

Art. 7 - Sicurezza del trattamento

Art. 8 - Registro delle attività di trattamento e Procedure

Art. 9 - Valutazione d'impatto sulla protezione dei dati

Art. 10 - Violazione dei dati personali

Art. 11 - Rinvio

Art. 1

Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati.

Art.2

Titolare del trattamento

1. L'azienda ASP è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"), nella persona del suo Direttore generale. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 6 RGDP: liceità, correttezza e trasparenza.
2. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.
3. Le misure sono definite fin dalla fase di progettazione e 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 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.
4. Il Titolare adotta misure appropriate per fornire all'interessato:

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

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

5. 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") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.
6. Il Titolare, inoltre, provvede a:

   a) designare gli incaricati del trattamento tra le persone dell'organizzazione aziendale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza;

   b) nominare il Responsabile della protezione dei dati, che può essere una figura esterna, a condizione che garantisca l'effettivo assolvimento dei compiti che il Regolamento UE 2016/679 assegna a tale figura;

   c) tenuta dei registri richiesti (trattamento e procedure).

Art.3

Finalità del trattamento

1. I trattamenti sono compiuti dal ASP per le seguenti finalità:

   a) l'esercizio delle funzioni amministrative e fiscali che riguardano gli utenti dei servizi,

   b) la gestione dei dati socio-sanitari contenti nelle cartelle individuali degli ospiti delle strutture residenziali e semi-residenziali,

   c) la gestione dei dati anagrafici dei famigliari degli utenti ai fini delle attività amministrative

   d) la gestione rilevazioni e statistiche al fine di ottimizzare l'efficienza organizzativa.

   e) La programmazione e pianificazione/esecuzione delle attività di animazione e socializzazione;

   f) l'erogazione di prestazioni e interventi, socio-assistenziali e socio-sanitari ed attività amministrative connesse

Art.4

Responsabile del trattamento

1. Il Responsabile del trattamento (nel nuovo regolamento europeo *data processor*) è la persona fisica, giuridica, pubblica amministrazione o ente che elabora i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 GDPR).
2. Si tratta di un soggetto, distinto dal titolare, che deve essere in grado di fornire garanzie al fine di assicurare il pieno rispetto delle disposizioni in materia di trattamento dei dati personali, nonché di garantire la tutela dei diritti dell'interessato.
3. Il titolare del trattamento risponde della gestione effettuata dal responsabile, dovendo ricorrere ad aziende che presentino garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che soddisfino i requisiti del Regolamento (Considerando 81 GDPR), e che le sue decisioni siano conformi alle leggi. Compito specifico del titolare è, infatti, quello di valutare il rischio del trattamento che pone in essere tramite i responsabili. Il titolare deve sempre poter sindacare le decisioni dei responsabili.
4. Il responsabile del trattamento dovrà avere innanzitutto una competenza qualificata e garantire una particolare affidabilità, un requisito fondato su aspetti etici e deontologici (ad esempio, l'assenza di condanne penali). Ovviamente dovrà disporre delle risorse tecniche adeguate per l'attuazione degli obblighi derivanti dal contratto di designazione e dalle norme in materia. Se è soggetto interno all'azienda le risorse saranno a carico del titolare.
5. Il ruolo del responsabile del trattamento di cui al regolamento europeo è riservato ad un soggetto esterno all'azienda, con riferimento ai fornitori di servizi. Infatti, vi è uno specifico obbligo di predisporre un contratto per la designazione delle responsabilità a carico del responsabile. A livello europeo, inoltre, si è da sempre affermata l'idea che il responsabile del trattamento non possa essere un soggetto alle dipendenze del titolare.

Art.5

Responsabile della protezione dati o DPO (Data Protection Officer)

1. L'ASP "Magiera Ansaloni" prevede di affidare esternamente, tramite **Lepida Spa/Regione Emilia Romagna**, le funzioni di Responsabile del trattamento e protezione dati.
2. Il Responsabile della protezione dei dati all'interno del Regolamento Europeo viene indicato come (DPO). E' una figura autonoma, che esegue le proprie funzioni in completa indipendenza (senza ricevere alcuna istruzione o impostazione gerarchica), e riferisce sul suo operato direttamente ai vertici aziendali, i quali, per la piena esecuzione dei suoi compiti si occupano di fornire le risorse necessarie.
3. Il DPO è incaricato dei seguenti compiti:
   a) informare e fornire consulenza al Titolare, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il DPO può indicare al Titolare i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

   b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare. 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;

   c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare;

   d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il DPO in merito a se condurre o meno una DPIA (Data Protection Impact Assessment – valutazione d'impatto sulla protezione dei dati) e quale metodologia adottare nel condurre una DPIA;

   e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del DPO è comunicato dal Titolare al Garante;

   f) altri compiti e funzioni a condizione che il Titolare si assicuri che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

1. Il DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali.

2. Nello svolgimento dei compiti affidatigli il DPO deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il DPO:

   a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere, incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare.

3. Il Titolare fornisce al DPO le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

4. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Art. 6

Incaricato trattamento dati

L'ASP "Magiera Ansaloni" prevede di affidare ad ogni dipendente che opera in azienda nei vari Servizi, l'incarico di addetto al trattamento dei dati.

Pur non essendo l'incaricato una figura giuridica autonoma del GDPR, il termine Incaricato è utilizzato nella informativa fornita agli interessati, tramite un atto formale di nomina.

Tale nomina non esclude l'obbligo di formazione e di fornire istruzioni come previsto dal Regolamento UE, secondo il quale la regola generale prevede che chiunque agisca sotto l'autorità del responsabile del trattamento o sotto quella del titolare del trattamento che abbia accesso a dati personali, non può trattare tali dati se non è istruito in tal senso.

Art.7

Sicurezza del trattamento

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

2. Le misure tecniche ed organizzative di sicurezza messe in atto per ridurre i rischi del trattamento comprendono:

- la pseudonimizzazione (utilizzo di sigle per identificare l'utente);
- la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità 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.

Costituiscono misure tecniche ed organizzative che possono essere adottate:

- sistemi di autenticazione alle postazioni di lavoro (password personali e riservate per ogni incaricato trattamento dati rinnovate ogni 3 mesi);
- sistemi di autorizzazione all'accesso degli applicativi;
- sistemi di protezione (antivirus; firewall; antintrusione; altro);

- sistemi di rilevazione di intrusione (allarme attivato in ogni struttura ed in sede);

- registrazione accessi (tramite apposito software che rileva ogni accesso agli archivi dati;

- sistemi di archiviazione e conservazione di archivi elettronici con accesso univoco e solo previa autorizzazione, effettuato esclusivamente da personale addetto;

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

3. Il Titolare ed il DPO si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

4. I nominativi ed i dati del DPO sono pubblicati sul sito istituzionale del ASP, sezione Amministrazione trasparente, oltre che nella sezione "privacy".

5. 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 (D.Lgs. n. 193/2006 così come modificato ed integrato dal successivo D.lgs. 101/2018).

Art.8

Registro delle attività di trattamento

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

a) il nome ed i dati di contatto dell' ASP, ai sensi del precedente art.2;

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 ente terzo;

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.

Il Registro è tenuto dal Titolare, tramite personale all'iopo incaricato, a disposizione del soggetto dallo stesso delegato ai sensi del precedente art. 5 (DPO), tenuto presso gli uffici della struttura organizzativa dell' ASP in forma telematica e cartacea.

Art. 9

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 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

2. 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'at. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche.

4. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, 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, RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di 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 dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche/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.

5. 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 ad ASP.

6. Il DPO 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.

7. 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, RGDP;

- ✓ 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 RDP 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.

8. 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;
- □ 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 RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

9. 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.

10. 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.

11. 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.

12. E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art. 10

Violazione dei dati personali

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

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 Responsabile del trattamento/DPO è obbligato ad informare 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 RGPD, sono i seguenti:

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

4. Se il 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;
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

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

Art.11

Rinvio

1. Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD (Regolamento Generale Protezione Dati ossia il Regolamento Europeo 679/2016) e tutte le sue norme attuative vigenti.

GLOSSARIO REGOLAMENTO

- **Titolare del trattamento**

  l'autorità pubblica (ASP) che determina finalità e mezzi del trattamento di dati personali.

- **Responsabile del trattamento**

  il Responsabile esterno che tratta dati personali per conto del Titolare del trattamento.

- **Responsabile per la protezione dati – DPO o DPO (Data Protection Officer)**

  il dipendente della struttura organizzativa dell'ASP, il professionista privato o impresa esterna, incaricati dal Titolare o dal Responsabile del trattamento/DPO.

- **Registri delle attività di trattamento**

  elenchi dei trattamenti in forma cartacea o telematica tenuti dal Titolare e dal Responsabile del trattamento/DPO 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.

GLOSSARIO REGISTRI

Ai fini delle proposte dei registri, 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 lo 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, l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate all' ASP.
Adempimento di un obbligo legale al quale è soggetto il ASP.
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/Ente 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 l'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

Cittadini residenti; utenti; partecipanti al procedimento; dipendenti; amministratori; fornitori; altro.

❖ Categorie destinatari

Persone fisiche; autorità pubbliche ed altre PA; persone giuridiche private; altri soggetti.