



REGOLAMENTO sul Modello Organizzativo in materia di Protezione dati personali (MOP) dell'ATS di Pavia

REG MOP 01

(Approvato con Decreto n. 21/DGi del 16/01/2025)

Preparato	Gruppo Coordinamento Privacy ATS di Pavia
Verificato	Direttore Amministrativo
Approvato	Direttore Generale
Identificato ed editato	Responsabile Qualità Aziendale

1	Modifica artt. n.3, n. 6, n.9, n.10	Data di adozione del Decreto
0	Prima emissione	Decreto 252/DGi del 04/04/2023
Rev.	Descrizione modifica	Data di applicazione



SOMMARIO

CAPO I – DISPOSIZIONI GENERALI	2
Art. 1 Oggetto	2
Art. 2 Definizioni	2
Art. 3 Finalità e basi giuridiche del trattamento	3
CAPO II – MODELLO ORGANIZZATIVO	3
Art. 4 Titolare del trattamento	3
Art. 5 Data Protection Officer (DPO)	4
Art. 6 Responsabile interno del trattamento dei dati	6
Art. 7 Responsabile esterno del trattamento	6
Art. 8 Autorizzati al trattamento	7
Art. 9 Gruppo Coordinamento Privacy	7
Art. 10 Struttura competente in materia di ICT	7
CAPO III – SICUREZZA E PROTEZIONE DATI	8
Art. 11 Sicurezza del trattamento	8
Art. 12 Registro del Titolare del trattamento	8
Art. 13 Registro del Responsabile interno del trattamento	9
Art. 14 Registro del Responsabile esterno del trattamento	9
Art. 15 Valutazione d’impatto sulla protezione dei dati (DPIA)	9
Art. 16 Violazione dei dati personali (Data Breach)	10
CAPO IV – DISPOSIZIONI FINALI	10
Art. 17 Abrogazioni e rinvii	10



CAPO I – DISPOSIZIONI GENERALI

Art. 1 Oggetto

Il presente Regolamento sul Modello Organizzativo in materia di protezione dati personali (MOP) disciplina l'assetto di *governance* e le disposizioni procedurali per l'adeguamento dell'ATS di Pavia al Regolamento Generale Protezione Dati UE del 27 aprile 2016 n. 679 (GDPR¹) ed al “Codice in materia di protezione dei dati personali”, D.Lgs. n. 196 del 30 giugno 2003 e ss.mm. e ii..

Art. 2 Definizioni

Ai fini del presente Regolamento si intende per:

GDPR: Regolamento Generale Protezione Dati Personali - Regolamento (UE) n. 2016/679, è un regolamento dell'Unione europea in materia di trattamento dei dati personali e di privacy, adottato il 27 aprile 2016, pubblicato sulla Gazzetta ufficiale dell'Unione europea il 4 maggio 2016 ed entrato in vigore il 24 maggio dello stesso anno ed operativo a partire dal 25 maggio 2018.

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.

DPO: Data Protection Officer.

Responsabile interno del trattamento: la persona fisica espressamente nominata che tratta dati personali per conto dell'ATS di Pavia nell'ambito dell'assetto organizzativo interno all'Ente a cui sono attribuiti specifici compiti e funzioni.

Responsabile esterno del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo esterno che tratta dati personali per conto del Titolare del trattamento.

Interessato: la persona fisica a cui si riferiscono i dati personali.

Autorizzato: il soggetto (persona fisica) autorizzato ad effettuare materialmente le operazioni di trattamento sui dati personali.

Data Breach (Violazione dei dati personali): la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

¹ Come presente sul sito del Garante.



Art. 3 Finalità e basi giuridiche del trattamento

1. L'ATS di Pavia tratta i dati personali nel perseguimento delle proprie finalità istituzionali.

2. Ai sensi degli artt. 6, 9 e 10 del Regolamento Ue 2016/679 (GDPR), l'ATS tratta i dati personali cd. comuni (identificativi e di contatto), le categorie particolari di dati personali e i dati giudiziari per legislazione di diritto europeo, per legge e/o regolamento, nel rispetto dei principi di finalità, proporzionalità e necessità, per:

- adempiere ad obblighi legali (art. 6, par. 1, lett. c) del GDPR);
- salvaguardare gli interessi vitali dell'interessato o di altra persona fisica (art. 6, par. 1, lett. d) e art. 9, par. 2, lett. c) del GDPR);
- eseguire compiti di rilevante interesse pubblico relativi alla tutela della salute (art. 6, par. 1, lett. e) e art. 9, par. 2, lett. g) del GDPR);
- esercizio di pubblici poteri di cui l'ATS è investita (art. 6, par. 1, lett. e) del GDPR);
- esecuzione di un contratto con soggetti interessati (art. 6, par. 1, lett. b) del GDPR);
- finalità di assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (art. 9, par. 2, lett. h) del GDPR);
- finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica o per finalità statistiche (art. 9, par. 2, lett. j) del GDPR);
- specifiche finalità, diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento (art. 6, par. 1, lett. a) e art. 9, par. 2, lett. a) del GDPR).

3. In particolare, il trattamento dei dati relativi alla salute, genetici e biometrici è altresì effettuato in conformità alle misure di garanzia disposte dal Garante della Protezione dei dati personali, mentre il trattamento dei dati giudiziari è effettuato in conformità alle misure di garanzia disposte con Decreto del Ministero di Giustizia.

CAPO II – MODELLO ORGANIZZATIVO

Art. 4 Titolare del trattamento

1. L'ATS di Pavia, rappresentata, ai fini previsti dal GDPR, dal Direttore Generale, è il Titolare del trattamento dei dati personali (di seguito, il "Titolare") raccolti anche in banche dati, digitali o cartacee.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 del GDPR:

- a) liceità, correttezza e trasparenza;
- b) limitazione della finalità e minimizzazione dei dati;
- c) esattezza;
- d) limitazione della conservazione;
- e) integrità e riservatezza.

3. Il Titolare mette in atto le 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 GDPR. Le



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

4. Il Titolare provvede a:

- a) nominare il Data Protection Officer (DPO);
- b) nominare i Responsabili interni del trattamento dei dati nelle persone dei direttori amministrativo, sanitario e sociosanitario, direttori/responsabili di SC, SSD e SS in cui si articola l'organizzazione dell'ATS di Pavia, quali soggetti responsabili degli adempimenti necessari per la conformità dei trattamenti dei dati personali effettuati dall'Ente e preposti al trattamento dei dati contenuti nelle banche dati di competenza delle articolazioni organizzative cui sono preposti (art. 6.1 del presente Regolamento);
- c) assegnare distinti compiti a specifiche Strutture, in ragione delle peculiari competenze alle medesime attribuite dal POAS, al fine di avvalersi di particolari contributi ed apporti funzionali per il concreto e fattivo adeguamento dell'Ente al GDPR.
- d) nominare con apposito atto i Responsabili esterni ex art. 28 GDPR individuati dai Responsabili interni nell'ambito delle proprie competenze (art. 6.3.i e art. 7 del presente Regolamento).

5. Il Titolare, per il tramite della segreteria di direzione, garantisce la corretta gestione e conservazione di tutta la documentazione attestante l'attuazione del modello organizzativo privacy adottato.

6. Il Titolare è Contitolare del trattamento, ai sensi dell'art. 26 del GDPR, nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'ATS di Pavia da enti ed organismi statali o regionali, allorché due o più Titolari determinino congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento.

Art. 5 Data Protection Officer (DPO)

1. Il DPO, nominato dal Titolare del trattamento, è scelto tra il personale dipendente dell'ATS di Pavia (DPO interno) da nominarsi mediante specifico atto di designazione, ovvero nella figura unica di un professionista o di una società (DPO esterno) che possiede le medesime prerogative e tutele di quello interno e che dovrà operare in base a un contratto di servizi o in forza di una convenzione stipulata dall'ATS con altri enti pubblici.

In entrambi i casi il soggetto deve possedere i requisiti specificati dagli artt. 37 e 38 del GDPR.

2. Il DPO è incaricato dei seguenti compiti (art. 39 del GDPR):

- a) informare e fornire consulenza all'ATS di Pavia in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati personali;
- b) fungere da supporto alle Strutture competenti sulle richieste di accesso per tutti gli aspetti relativi alla protezione dei dati personali, ai sensi del GDPR;
- c) fornire, se richiesto, un parere in merito alla Valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento (art. 15 del presente Regolamento);
- d) rendere una consulenza idonea, scritta od orale, anche nell'individuazione dei rapporti intercorrenti con soggetti terzi in materia di protezione dei dati;
- 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 GDPR, ed effettuare, se del caso, consultazioni relativamente ad ogni altra questione inerente al trattamento di dati personali;



- f) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, ferme restando le responsabilità dell'ATS di Pavia. 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 e l'attività di informazione, consulenza e indirizzo nei confronti dell'ATS di Pavia;
- g) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dall'ATS di Pavia;
- h) altri compiti e funzioni a condizione che l'ATS di Pavia si assicuri che non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del DPO.

3. Il DPO deve disporre di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente. L'ATS di Pavia mette a disposizione del DPO le risorse necessarie per assolvere ai compiti attribuiti e per accedere ai dati personali ed ai trattamenti.

In particolare, al DPO sono assicurati:

- a) il supporto attivo da parte dei Responsabili interni (art. 6.3.d del presente Regolamento) e dal Gruppo Coordinamento Privacy (art. 9.2.c del presente Regolamento) per lo svolgimento dei compiti di cui al paragrafo precedente;
- b) l'accesso alle articolazioni funzionali dell'Ente per fornire il supporto, le informazioni e gli *input* essenziali.

4. Il DPO opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti e non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione riguardante la normativa sulla protezione dei dati personali. Ferma restando l'indipendenza nello svolgimento di detti compiti, il DPO riferisce direttamente all'ATS di Pavia. Nel caso in cui siano rilevate dal DPO o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso DPO, quest'ultimo è tenuto a manifestare il proprio dissenso comunicandolo all'ATS di Pavia.

Art. 6 Responsabile interno del trattamento dei dati

1. Il Titolare nomina, quali Responsabili interni al trattamento dei dati personali relativamente ai trattamenti effettuati dall'articolazione organizzativa di competenza (art. 4.4.b del presente Regolamento), i direttori amministrativo, sanitario e sociosanitario, e i direttori/responsabili di SC, SSD e SS in cui si articola l'organizzazione dell'Ente. Ciascun Responsabile interno deve essere in grado di offrire garanzie sufficienti in termini di conoscenza, esperienza, capacità ed affidabilità per mettere in atto le misure tecniche e organizzative rivolte a garantire che i trattamenti siano effettuati in conformità al GDPR.

La nomina avviene contestualmente alla sottoscrizione dell'incarico conferito, con istruttoria a carico della SC Gestione e sviluppo delle risorse umane.

2. Il Titolare, nell'atto di nomina, indica gli specifici ambiti di attività, o l'elenco dei trattamenti di dati personali, di cui i singoli Responsabili interni sono responsabili.

3. Al Responsabile interno sono attribuiti i seguenti compiti:

- a) tenuta del Registro delle categorie di dati da lui trattati per conto del Titolare. Tale Registro ha lo stesso contenuto informativo del Registro del Titolare (cfr. art. 12 del presente



- Regolamento) e del Registro del Responsabile esterno del trattamento (cfr. art. 14 del presente Regolamento) di cui ne costituisce parte integrante e sostanziale e viene dal Responsabile alimentato ed aggiornato;
- b) verifica della legittimità dei trattamenti di dati personali effettuati dalla Struttura di riferimento;
 - c) garantire il rispetto dei provvedimenti emessi dal Garante e disporre l'attuazione;
 - d) collaborare con il DPO al fine di consentire allo stesso l'esecuzione dei compiti e delle funzioni assegnate (art. 5.3.b del presente Regolamento);
 - e) individuare i soggetti Autorizzati al trattamento per la Struttura organizzativa di competenza e attribuire loro specifici compiti e attività di protezione dei dati (art. 8.1 del presente Regolamento);
 - f) individuare il personale della propria articolazione organizzativa da sottoporre alle attività formative in materia di protezione dei dati;
 - g) adottare soluzioni di privacy "by design e by default", ovvero di protezione dei dati fin dalla progettazione e per impostazione predefinita, prevedendo, già dall'origine, in considerazione del contesto complessivo ove il trattamento si colloca e dei rischi stimati, un paradigma di trattamento e misure di protezione prefissate;
 - h) procedere alla comunicazione delle modifiche intervenute ai trattamenti di competenza e aggiornare i contenuti in materia di protezione dati presenti nella modulistica relativa alla propria Struttura organizzativa;
 - i) individuare e proporre al Titolare la nomina dei Responsabili esterni del trattamento (art. 4.4.d del presente Regolamento);
 - j) adottare, se necessario, specifici disciplinari tecnici di settore, anche congiuntamente con altri Responsabili interni e/o Responsabili esterni del trattamento, per stabilire e dettagliare le modalità di effettuazione di particolari trattamenti di dati personali relativi alla specifica area di competenza;
 - k) fornire riscontro alle richieste dell'Interessato per i trattamenti di dati di competenza della propria Struttura organizzativa avvalendosi, se necessario, del supporto del Gruppo Coordinamento Privacy (art. 9.2.a del presente Regolamento);
 - l) rilevare e comunicare al Titolare i casi di violazione dei dati personali (*Data Breach*) nell'ambito organizzativo di riferimento (art. 16.3 del presente Regolamento);
 - m) gestire l'analisi del rischio e la Valutazione di impatto (DPIA) (art. 15.2 del presente Regolamento).

4. Per i trattamenti dei dati personali che coinvolgono più Strutture in modo trasversale, laddove applicabile, vige il criterio della prevalenza, secondo il quale la Struttura che ha competenza principale nel trattamento dei dati personali coordina le attività delle altre Strutture coinvolte.

Art. 7 Responsabile esterno del trattamento

1. Il Responsabile esterno del trattamento è il soggetto, pubblico o privato, che tratta dati personali, anche particolari, per conto del Titolare, e che presenta garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti previsti dal GDPR e garantisca la tutela dei dati dell'Interessato. Tale soggetto assume il ruolo di Responsabile esterno del trattamento ai sensi dell'art. 28 del GDPR mediante un atto giuridico in forma scritta.



L'atto di nomina viene predisposto dal Responsabile interno del trattamento dei dati e sottoposto alla firma del Titolare.

2. I rapporti tra il Titolare ed i Responsabili esterni sono disciplinati dagli atti di cui al comma 1 del presente articolo, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del Responsabile esterno del trattamento e le modalità di trattamento. Tali atti possono anche basarsi su "clausole contrattuali tipo" adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.

3. Il Responsabile esterno del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla normativa e ai compiti affidatigli dal Titolare.

4. Qualora l'Ente proceda alla nomina di Responsabili esterni dovrà prevedere, in sede di stipula di contratto e/o convenzione, che questi sviluppino il Registro dei trattamenti coordinandosi con l'ATS di Pavia.

Art. 8 Autorizzati al trattamento

1. Il Titolare, o i Responsabili interni (art. 6.3.e del presente Regolamento), individuano, nell'ambito della propria responsabilità, gli Autorizzati al trattamento quali persone ammesse a compiere operazioni sui dati personali.

2. Nell'atto di individuazione, il Titolare o i Responsabili interni indicano, per ciascun Autorizzato, gli ambiti di attività e/o l'elenco dei trattamenti di dati personali di competenza.

Art. 9 Gruppo Coordinamento Privacy

1. Il Gruppo Coordinamento Privacy, costituito da personale dell'ATS di Pavia in possesso di competenze diversificate ed individuato dal Titolare del trattamento, ha il compito di supportare il Titolare stesso nell'applicazione del Modello Organizzativo Privacy dell'Agenzia, confrontandosi, se necessario, con il Data Protection Officer (DPO).

2. Il Gruppo Coordinamento Privacy si riunisce, di norma, con cadenza bimestrale o più frequentemente, se necessario.

3. Al Gruppo Coordinamento Privacy compete inoltre:

- a) il supporto ai Responsabili interni nell'attività di riscontro alle richieste degli interessati (art. 6.3.k del presente Regolamento);
- b) la definizione e la proposta di attività formativa in materia di privacy.

Art. 10 Struttura competente in materia di ICT

1. La Struttura competente in materia di ICT è la struttura che in ambito di protezione dati fornisce il contributo nella valutazione degli aspetti tecnologici relativamente all'impatto di questi sulle attività di trattamento.

2. La Struttura, in particolare, svolge i seguenti compiti:

- a) gestisce l'infrastruttura tecnologica hardware e software utilizzata dall'Ente per le attività di trattamento di dati;
- b) sviluppa gli aspetti tecnologici inerenti l'analisi del rischio (ai sensi dell'art. 32 GDPR) e la Valutazione di impatto (ai sensi dell'art. 35 GDPR);
- c) gestisce i Registri dei trattamenti dell'ATS (Registro del Titolare del trattamento - art. 12 del presente Regolamento, Registro del Responsabile esterno - art. 14 del presente



Regolamento) che vengono alimentati ed aggiornati con i singoli Registri dei trattamenti di ciascun Responsabile interno (art. 13 del presente Regolamento) per quanto di propria competenza.

CAPO III – SICUREZZA E PROTEZIONE DATI

Art. 11 Sicurezza del trattamento

1. Il Titolare del trattamento e tutti i soggetti/ruoli descritti al Capo II del presente Regolamento mettono in atto, per i distinti profili di responsabilità e di azione, misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio. Costituiscono misure tecniche ed organizzative che possono essere adottate, tra le altre, i sistemi di autenticazione, autorizzazione, rilevazione di intrusione, sorveglianza, di protezione (antivirus, firewall), sistemi di copiatura e conservazione di archivi elettronici.
2. L'ATS di Pavia, attraverso i ruoli individuati nel presente Regolamento, impartisce adeguate istruzioni sul rispetto delle predette misure anche a coloro che agiscono per suo conto ed abbiano accesso a dati personali.
3. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati particolari (ex sensibili) per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi adottati ai sensi del D. Lgs. 196/2003 nella versione antecedente alle modifiche apportate dal D. Lgs. 101/2018.

Art. 12 Registro del Titolare del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente reca per ciascun trattamento almeno le seguenti informazioni, come previste dall'art. 30, par. 1, del GDPR:
 - a) il nome ed i dati di contatto del Titolare del trattamento, del Data Protection Officer (DPO), del Responsabile interno, del Responsabile esterno ex art. 28 GDPR e, ove applicabile, del Contitolare del trattamento;
 - 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.
2. La gestione del Registro dei trattamenti dell'ATS è affidata alla Struttura competente in materia di ICT dell'ATS (art. 10.2.c del presente Regolamento) ed è alimentato ed aggiornato con i singoli Registri dei trattamenti di ciascun Responsabile interno (art. 6.3.a del presente Regolamento) per quanto di propria competenza.
3. Il Registro è conservato dalla Segreteria di Direzione in apposito fascicolo digitale nel sistema di gestione documentale aziendale.



Art. 13 Registro del Responsabile interno del trattamento

1. Il Responsabile interno del trattamento tiene il Registro delle categorie di attività da lui trattate per conto del Titolare. Tale registro ha lo stesso contenuto informativo del Registro del Titolare di cui all'art. 12 e del Registro del Responsabile esterno di cui all'art. 14 del presente Regolamento. Il Registro del Responsabile interno del trattamento, alimentato ed aggiornato dallo stesso Responsabile interno, costituisce parte integrante e sostanziale dei predetti Registri.
2. Il Registro è conservato in apposito fascicolo digitale della struttura diretta dal Responsabile interno nel sistema gestione documentale aziendale.
3. Il Registro è periodicamente aggiornato dal Responsabile interno al trattamento e trasmesso in occasione di ogni modifica alla Struttura competente in materia di ICT dell'ATS.

Art. 14 Registro del Responsabile esterno del trattamento

1. Il Registro delle attività di trattamento svolte dall'Ente in qualità di Responsabile esterno del trattamento contiene almeno le seguenti informazioni, come previsto dall'art. 30, par. 2, del GDPR:
 - a) il nome e i dati di contatto del Responsabile esterno o dei Responsabili esterni del trattamento, di ogni Titolare del trattamento per conto del quale agisce il Responsabile esterno del trattamento, del Rappresentante del Titolare del trattamento o del Responsabile esterno del trattamento e del DPO;
 - b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
 - c) l'eventuale trasferimento di dati personali verso un Paese terzo od un'organizzazione internazionale;
 - d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. La gestione del Registro dei trattamenti dell'ATS è affidata alla Struttura competente in materia di ICT dell'ATS (art. 10.2.c del presente Regolamento) ed è alimentato ed aggiornato con i singoli Registri dei trattamenti di ciascun Responsabile interno (art. 6.3.a del presente Regolamento) per quanto di propria competenza.
3. Il Registro è conservato dalla Segreteria di Direzione in apposito fascicolo digitale nel sistema di gestione documentale aziendale.

Art. 15 Valutazione d'impatto sulla protezione dei dati (DPIA)

1. Il Titolare, prima di effettuare un nuovo trattamento o qualora vengano apportate modifiche rilevanti ad un trattamento già esistente, deve attuare una Valutazione d'impatto (DPIA) ai sensi dell'art. 35 GDPR quando il trattamento medesimo, considerati la natura, l'oggetto, il contesto e le finalità dello stesso, nonché l'eventuale utilizzo di nuove tecnologie, presenti un rischio elevato per i diritti e le libertà delle persone fisiche.
2. L'attività di gestione dell'analisi del rischio e della Valutazione di impatto (DPIA) rispetto al nuovo trattamento di dati, o qualora vengano apportate modifiche significative all'attività dell'ATS di Pavia che impattano su trattamenti già esistenti, viene effettuata dal Responsabile interno competente (art. 6.3.m del presente Regolamento).
3. 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 per la protezione dei dati personali ai sensi dell'art. 35 del GDPR.
4. La DPIA non è necessaria nei casi seguenti:
 - a) se il trattamento non presenta un rischio elevato per i diritti e le libertà di persone fisiche;



- b) 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;
- c) 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;
- d) 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;
- e) se i trattamenti sono già stati oggetto di verifica preliminare da parte del Garante Privacy o del DPO e che proseguono con le stesse modalità oggetto di tale verifica.

Art. 16 Violazione dei dati personali (Data Breach)

1. La violazione dei dati personali (Data Breach) è una 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'Ente.
2. L'ATS di Pavia 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 a cura della Segreteria di Direzione.
3. Gli episodi di violazione dei dati personali, rilevati dal Responsabile interno, devono essere comunicati da tale soggetto al Titolare del trattamento (art. 6.3.1 del presente Regolamento).
4. L'ATS di Pavia, per il tramite del rappresentante legale dell'Ente o di un suo delegato, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui l'ATS ne è venuta a conoscenza, deve notificare la violazione al Garante Privacy a meno che sia improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la violazione comporta un rischio elevato per i diritti delle persone, l'ATS di Pavia, per il tramite del rappresentante legale dell'Ente o di un suo delegato, deve comunicarla a tutti gli interessati utilizzando i canali più idonei, a meno che abbia già preso misure tali da ridurre l'impatto. Il Titolare del trattamento, a prescindere dalla notifica al Garante, deve documentare tutte le violazioni dei dati personali in un apposito registro la cui tenuta è in carico alla segreteria di direzione. Tale documentazione consente all'Autorità di effettuare eventuali verifiche sul rispetto della normativa.
5. Chiunque venga a conoscenza di una eventuale violazione è tenuto a informare tempestivamente il Titolare nel rispetto della procedura aziendale vigente.
6. Le notifiche al Garante effettuate oltre il termine delle 72 ore devono essere accompagnate dai motivi del ritardo.

CAPO IV – DISPOSIZIONI FINALI

Art. 17 Abrogazioni e rinvii

Il presente Regolamento abroga ogni precedente disposizione aziendale regolamentante il trattamento dei dati personali ai sensi del D.lgs. 196/2003 e ss.mm. e ii..



Per tutto quanto non espressamente disciplinato, si rinvia alle disposizioni del GDPR ed a tutte le norme vigenti in materia.