Comune
di Trepuzzi
Provincia di Lecce

MODELLO ORGANIZZATIVO per la PROTEZIONI dei DATI

MOPD

MANUALE DI GESTIONE DEL MODELLO ORGANIZZATIVO PER LA PROTEZIONE DATI

Organizzazione, Gestione e Controllo
sulla protezione dei dati personali

in attuazione del Regolamento UE 2016/679

General Data Protection Regulation

Release 4.0 del 13/02/2021

Comune di Trepuzzi
Corso Garibaldi, 10 - 73019 Trepuzzi (LE)
Codice fiscale: 00463680751
PEC: protocollo.comune.trepuzzi@pec.rupar.puglia.it
Email: protocollo@comune.trepuzzi.le.it

[Pagina intenzionalmente lasciata in bianco]

Indice

Revisioni e modifiche al documento

Revisione	Data	Descrizione della revisione
1.0	23/05/2018	Emissione
2.0	21/09/2018	Adeguamento al Dlgs 101/2018 di modifica del D.lgs. 196/2003
3.0	21/06/2019	Aggiornamento tecnico
4.0	13/02/2021	Aggiornamento tecnico

1. Premessa

1.1 Scopo del documento

Il **Modello Organizzativo per la Protezione dei Dati** (d'ora in poi anche solo "**MOPD**") è uno strumento dinamico che si pone l'obiettvo di ***dimostrare,*** rappresentare e rendere comprensibili le misure tecniche e organizzative implementate, il livello di conformità del titolare del trattamento e/o del responsabile del trattamento, nonché delle responsabilità che ognuno di tali soggetti si è assunto nel garantire la sicurezza e la protezione dei dati trattati per conto degli interessati.

Il Modello Organizzativo per la Protezione dei Dati (MOPD) è quell'**insieme di principi, obiettivi, prescrizioni, procedure operative, documenti e politiche finalizzate a garantire la sicurezza dei dati e dei relativi trattamenti**.

Il MOPD è lo strumento che fornisce ad ogni Organizzazione le indicazioni necessarie per la gestione dei trattamenti in sicurezza, come parte integrante dei processi e della struttura gestionale.

Il Modello Organizzativo serve:

- ad avere il pieno controllo, da parte dell'Organizzazione, delle attività di trattamento dei dati personali e delle procedure di protezione attuate;
- a orientare l'Organizzazione verso il miglioramento continuo della protezione dei dati e dei trattamenti.

1.2 Struttura del Modello Organizzativo per la Protezione dei Dati

Il MOPD è così strutturato:

a) **Procedure operative**
b) **Modulistica**
c) **Politiche**

Le procedure operative sono le seguenti:

MOPD PR03	Tenuta del registro attività di trattamento
MOPD PR04	Gestione ed evasione richieste (istanze) degli interessati
MOPD PR05	Gestione dei responsabili esterni
MOPD PR06	Gestione analisi dei rischi e valutazione di impatto sulla protezione dei dati
MOPD PR07	Gestione della violazione dei dati (Data breach)
MOPD PR09	Verifiche periodiche (Audit Interni)

Le **procedure** definiscono le modalità operative attraverso le quali Titolare, Responsabile, Soggetti autorizzati e designati di specifici compiti e funzioni (c.d. "delegati"), devono operare per garantire l'applicazione delle misure tecniche ed organizzative necessarie per raggiungere la piena conformità normativa nonché la continuità operativa (business continuity).

La **modulistica**, invece, è rappresentata da quell'insieme di documenti da redigere per designare, elencare, verbalizzare e, più in generale, mettere in grado il Titolare di dimostrare di aver applicato le misure di protezione corrette.

Con le **politiche** il titolare del trattamento dimostra una oggettiva responsabilità in merito al sistema di gestione della protezione dei dati, e assicura che i principi applicati dall'Organizzazione verso la protezione siano definiti e congruenti con la linea strategica, con l'ambiente in cui opera e con il profilo di rischio che caratterizza l'attività dell'Organizzazione stessa.

1.3 Diritto alla protezione dei dati personali

Il trattamento dei dati personali da parte dell'Organizzazione si svolge nel rispetto dei diritti e delle libertà fondamentali della Persona, con l'intento di tutelarne la dignità, il diritto alla riservatezza, all'identità personale nonchè alla protezione dei dati personali.

1.4 Trattamento dei dati

Ai sensi dell'art. 4 del Regolamento UE 679/2016, per "trattamento" si intende qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

1.5 Principio di responsabilizzazione (Accountability)

Il regolamento prevede il principio di accountability che promuove una maggiore responsabilizzazione dei titolari e responsabili del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per essere in grado di dimostrare che il trattamento dei dati è conforme al Regolamento.

A tal proposito il Regolamento prevede il principio di "privacy by design", ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.

In sostanza il principio di responsabilizzazione aiuta a dimostrare la conformità al regolamento anche attraverso l'adesione a linee guida, ai codici di condotta o a un meccanismo di certificazione.

2. Riferimenti normativi e documentali

Vengono gestiti dall'Organizzazione:

a) legislazione, giurisprudenza e regolamentazione di carattere generale o di settore, incluse leggi e disposizioni specifiche relative ai documenti, agli archivi, all'accesso, alla tutela della riservatezza, alla capacità probatoria, al commercio elettronico, alla protezione dei dati e all'informazione,

b) provvedimenti a carattere generale dell'Autorità Garante per la protezione dei dati personali; direttive operative obbligatorie,

c) codici di autoregolamentazione,

d) codici deontologici.

Tutti i riferimenti normativi del presente manuale e del Modello Organizzativo sono elencati nel documento "**MOPD 10-002 Elenco leggi e norme applicabili**", nel quale sono specificate anche le modalità di accesso ai documenti stessi.

L'aggiornamento dei riferimenti normativi e documentali della Organizzazione viene garantito dall'invio da parte degli enti di normazione e/o di certificazione dei bollettini di aggiornamento. L'Organizzazione è infatti iscritta a più newsletter che consentono un rapido e costante aggiornamento.

Il Referente Organizzativo Privacy interno, o il Responsabile Protezione dei Dati, o il Titolare del trattamento, ricevuto il bollettino, e consultati i vari responsabili di funzione nonché la direzione aziendale, stabilisce quali aggiornamenti acquisire.

Normativa

Regolamento (UE) 2016/679	**GDPR** (General Data Protection Regulation) **–** relativo alla protezione delle persone fisiche con riguardo al **trattamento e alla libera circolazione dei dati personali**
Codice privacy	**D.Lgs. 196/2003 e s.m.i.** Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abrogala direttiva 95/46/CE
Decreto legislativo 10 agosto 2018, n. 101	Relativo all'adeguamento del Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679
Direttiva (UE) 2016/680	Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio
Decreto legislativo 18 maggio 2018, n. 51	Attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

3. Ambito di applicazione e definizioni

3.1 Introduzione

Il presente documento descrive il **Modello Organizzativo per la Protezione dei Dati** (in seguito denominato **MOPD**) adottato dal **COMUNE DI TREPUZZI** (di seguito **"Titolare", "Ente" o "Organizzazione"**) per garantire l'attuazione e il mantenimento della protezione dei dati personali, il corretto trattamento dei dati personali, relativamente alle attività e processi interni, nonché il miglioramento continuo delle procedure attuate per garantire protezione e riservatezza dei dati, il tutto nel pieno rispetto della normativa vigente in materia (Regolamento UE 2016/679 e D.Lgs 196/2003 e s.m.i.).

Esso costituisce il riferimento per il corretto funzionamento del Sistema di Gestione e l'espressione delle Politiche per la Protezione dei dati personali (Policy) così come definite dalla Direzione, oltre che svolgere funzioni di guida vincolante per tutto il personale interno.

Inoltre in questo documento sono delineate le misure di sicurezza, tecniche, organizzative, fisiche e logiche, adottate per il trattamento dei dati personali.

Dati del Titolare del trattamento

Denominazione	**COMUNE DI TREPUZZI**
Codice fiscale/p.iva	00463680751
Indirizzo	**Corso Garibaldi, 10** **73019 Trepuzzi (LE)**
E-mail	**protocollo@comune.trepuzzi.le.it**
PEC	**protocollo.comune.trepuzzi@pec.rupar.puglia.it**
Legale rappresentante	**Avv. Giuseppe Maria Taurino**
	Sindaco

Dati del Responsabile della Protezione dei dati (Data Protection Officer – DPO)

Tipo di designazione	**Persona giuridica esterna**
Denominazione	**231 PROFESSIONISTI IN NETWORK S.R.L.**
Codice fiscale/Partita IVA	**04461880751**
Indirizzo	**Piazzale Sondrio, 10** **73100 Lecce**
E-mail	**serviziorpd@231pin.it**

Soggetto individuato quale referente per il Titolare

Cognome e nome	**Carrisi Rosario**
Mobile	**3485121997**
E-mail	**serviziorpd@231pin.it**
PEC	**rosario.carrisi@pec.it**

Incarico e designazione

Estremi incarico	**Unione dei Comuni del Nord Salento** **Determinazione Dirigenziale nr. 32 del 24/05/2018**
Estremi della designazione	**Ordinanza sindacale N. 20 DEL 24/05/2018 PROT. 8296**
Comunicazione dei dati di contatto all'Autorità Garante	**GPDP.Ufficio registro RPD Prot. 0024076.25/05/2018**

3.2 Definizioni

Termine	Definizione	Rif. norma
Archivio	qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;	GDPR
Autorità di controllo	l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;	GDPR
Autorità di controllo interessata	un'autorità di controllo interessata dal trattamento di dati personali in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo;	GDPR
Comunicazione	Il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-quaterdecies, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;	D.Lgs. 196/03
Comunicazione elettronica	Ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile	D.Lgs. 196/03
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;	GDPR
Dati biometrici	I dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;	GDPR
Dati genetici	I dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;	GDPR
Dati giudiziari (ovvero relativi a condanne penali o reati)	I dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;	GDPR
Dati identificativi	I dati personali che permettono l'identificazione diretta dell'interessato;	D.Lgs. 196/03
Dati relativi all'ubicazione	Ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;	D.Lgs. 196/03
Dati relativi alla salute	I dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;	GDPR
Categorie particolari di dati (ex Dati sensibili)	I dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso,	GDPR

	filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; ripresi dall'art. 9 del GDPR	
Dato anonimo	Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile	-
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale	GDPR
Destinatario	La persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;	GDPR
Diffusione	l dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;	D.Lgs. 196/03
Evidenza	Nell'ambito della ISO 19011 sono definite evidenze dell'audit le registrazioni, dichiarazioni di fatti o altre informazioni, che sono pertinenti ai criteri dell'audit e verificabili. Possono essere qualitative o quantitative	ISO 19011
Gruppo imprenditoriale	Un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;	GDPR
Impresa	La persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica	GDPR
Autorizzati	Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;	-
Interessato	La persona fisica cui si riferiscono i dati personali	GDPR
Limitazione di trattamento	Il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;	GDPR
Norme vincolanti d'impresa	Le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;	GDPR
Obiezione pertinente e motivata	Un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione	GDPR
Organizzazione internazionale	Un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati	GDPR
Politica (Policy)	Descrive, ad alto livello, la posizione di una organizzazione rispetto ad un determinato argomento. La policy, comportando un'assunzione di rischio, deve essere approvata dal top management	
Procedura	Una procedura descrive, con il livello di dettaglio adeguato, come un'organizzazione realizza uno specifico obiettivo. È possibile che	

	un'organizzazione si doti di un impianto documentale con procedure a diverso livello di dettaglio, dalle più generiche alle istruzioni operative. La modalità, il formato, la responsabilità di creazione e gestione, le modalità di revisione devono essere formalmente definite.	
Profilazione	Qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;	GDPR
Profilo di autorizzazione	L'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti	-
Pseudonimizzazione	Il trattamento dei dati personali eseguito in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative tese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;	GDPR
Rappresentante	La persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;	GDPR
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;	GDPR
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;	GDPR
Trattamento	Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;	GDPR
Terzo	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;	GDPR
Trattamento transfrontaliero	a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro	GDPR
Stabilimento principale	a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;	GDPR

	b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;	
Servizio della società dell'informazione	Il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio	GDPR
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;	GDPR
Audit interno	Esame sistematico ed indipendente per determinare se le attività svolte per la qualità ed i risultati ottenuti sono in accordo con quanto pianificato, e se quanto predisposto viene attuato efficacemente e risulta idoneo al conseguimento degli obiettivi.	-
Sistema informatizzato	Si definisce "sistema informatizzato" l'insieme delle risorse hardware, delle procedure software -di base ed applicative- e dei dispositivi medici, connessi o separati dal resto del sistema informatico, utilizzati per il supporto ad una specifica attività, in collegamento o separatamente rispetto ad altri sistemi. In relazione alle modalità di uso e di gestione all'interno dell'organizzazione, i sistemi informatizzati sono classificabili in tre categorie: a) "**centralizzato**", si intendono quei sistemi, usualmente articolati e complessi, di uso diffuso all'interno dell'Organizzazione, installati per i componenti centrali (server, basi dati, procedure applicative, etc.) in ambienti centralizzati e dedicati e gestiti centralmente da personale dedicato. b) "**condiviso**", si intendono quei sistemi installati anche nelle componenti centrali all'interno di diversi settori dell'Organizzazione e utilizzati a supporto specifiche attività e/o organizzative di interesse locale per il settore. Operano autonomamente (collegati o meno con il sistema centrale dell'organizzazione) e sono gestiti su chiamata dalla struttura centrale dell'organizzazione e/o da personale dello specifico settore di afferenza. c) c. "**individuale**", si intendono quei sistemi utilizzabili individualmente da parte del personale (all'esterno e/o all'interno della sede dell'organizzazione)	-

3.3 Sigle ed Abbreviazioni

MOPD	Modello Organizzativo per la Protezione dei Dati personali
PROC / PRO	Procedure gestionali
MOD	Moduli
TIT	Titolare del trattamento
NC	Non Conformità
RPA	Referente Privacy Aziendale
RPD/DPO	Responsabile Protezione Dati / Data Protection Officer
AMSYS	Amministratore di Sistema

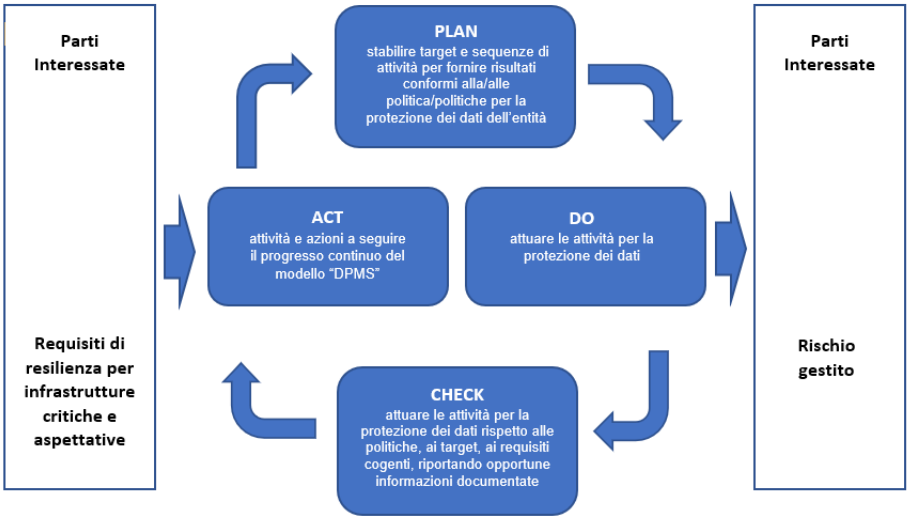
3.4 Approccio metodologico

Il Modello Organizzativo per la Protezione dei Dati (MOPD) si basa sulla metodologia nota come PDCA -Plan-Do-Check-Act (Pianificare-Attuare-Verificare-Agire).

La metodologia PDCA può essere brevemente descritta nel modo seguente:

(P) PLAN	Nella **fase di pianificazione** si fissano gli obiettivi, si individuano le risorse e si definiscono gli strumenti e i processi indispensabili per garantire il raggiungimento del risultato atteso. • Analisi del contesto • Leadership e impegno • Policy e campo di applicazione del MOPD • Risk management
(D) DO	Nella **fase di attuazione** si implementano le specifiche del sistema secondo quanto definito e pianificato nella fase precedente. • Organigramma e documentazione • Comunicazione e formazione • Controlli • Gestione degli incidenti • Attivazione del MOPD
(C) CHECK	Nella **fase di controllo** del MOPD si misura lo "stato di salute" del sistema per mezzo di appositi indicatori progettati nella fase di PLAN • Monitoraggio e Audit interno • Riesame di Direzione
(A) ACT	Nella **fase di manutenzione** e miglioramento, si perfeziona il MOPD, apportando i miglioramenti necessari per ottenere risultati di misurazione più soddisfacenti. • Non conformità e miglioramento continuo

Il metodo è quindi quello di riorganizzare il Regolamento nella visione sistemica delle norme.



L'analisi degli articoli del Regolamento sono riepilogati nella tabella allegata.

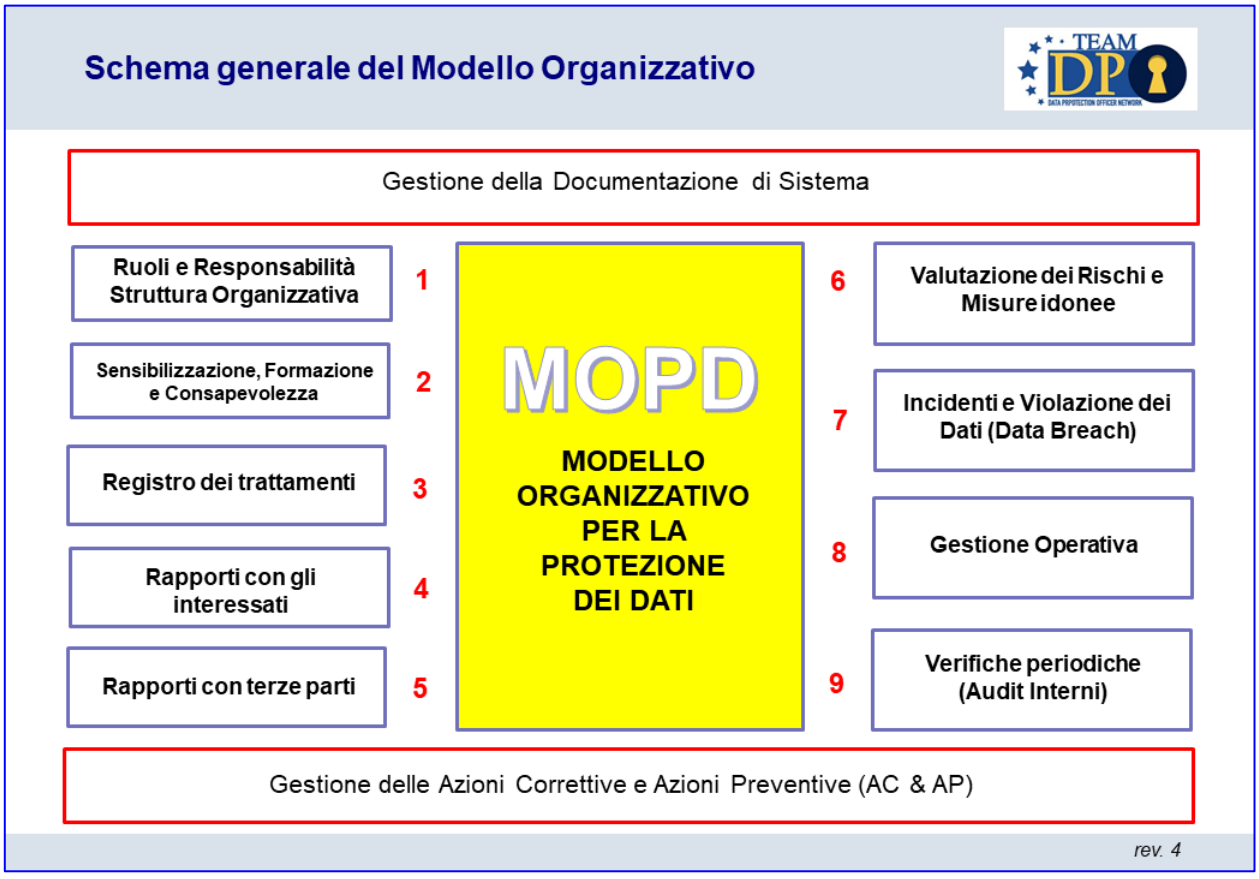
Tabella di correlazione PDCA/Regolamento		
Plan	Articoli che definiscono gli ambiti e le risorse necessarie per rispettare i principi di liceità e gli altri diritti dell'interessato:	
	Artt. 4,5 e 6	principi, liceità e consenso
	Art. 24	responsabilità del Titolare e delle politiche di protezione
	Art. 28	Responsabile
	Artt. 15, 16, 17, 18, 19, 20 e 21	Diritti dell'interessato
	Artt. 37, 38 e 39	Responsabile della protezione dati personali
	Pianificazione iniziale (PLAN) per individuare le analisi di rischio del trattamento e gli obiettivi che il Titolare si prefigge per il miglioramento del rapporto con le parti interessate.	
	Art. 35	Privacy Impact Analisys (DPIA)
	Art. 25	Privacy by default, privacy by design
	Art. 32	Sicurezza del trattamento
	Artt. 44, 45,46,47,48,49	Trasferimenti dei dati personali
Do	Azioni (DO) che dovranno essere eseguite dal Titolare per rispettare i diritti degli interessati	
	Art. 7	Consenso
	Artt. 12,13 e 14	Evidenze da dare agli interessati (Informative)
	Art. 30	Registro dei trattamenti
	Art. 34	Comunicazioni in caso di violazioni
	Art. 36	Consultazioni preventive verso l'Autorità
Check	Il rispetto va opportunamente documentato per dimostrare costantemente (CHECK) il percorso virtuoso del Titolare	
	Art. 7,12, 13, 14, 25, 30, 33, 34, 35 e 36	Attività per le quali è necessario prevedere documentazione comprovante la corretta applicazione di quanto effettuato ne punti precedenti
Act	Dimostrare che il Titolare vuole perseguire un miglioramento continuo attraverso un costante monitoraggio sia delle tecnologie sia delle metodologie (ACT)	
	Art. 32	Adeguatezza della sicurezza del trattamento alle tecnologie
	Art. 30	Registro del trattamento
	Art. 39	Sorveglianza per l'osservanza del Regolamento

3.5 Struttura generale del Modello Organizzativo

Il Modello Organizzativo per la Protezione dei Dati (MOPD) si compone dei seguenti "domini applicativi":

Dominio	Descrizione del dominio
01	**Struttura organizzativa: Ruoli e responsabilità**
02	**Sensibilizzazione, Formazione e Consapevolezza**
03	**Registri attività di trattamento**
04	**Rapporti con gli interessati: informative, consenso e diritti degli interessati**
05	**Rapporti con terze parti**
06	**Valutazione dei rischi e misure di sicurezza**
07	**Gestione violazione dei dati (data breach)**
08	**Gestione operativa**
09	**Verifiche periodiche (Audit Interni)**
10	**Gestione della documentazione di sistema**

Riepilogati nello schema seguente:



4. Politica aziendale per la protezione dei dati personali

In coerenza con la Missione e i Valori aziendali, l'Organizzazione, in materia di protezione dei dati personali, fa propri nella sua attività alcuni principi ai quali devono fare riferimento strategie ed obiettivi:

- Impegno a proteggere i dati personali di ogni individuo (*Protezione*);
- Garanzia dell'intimità della sfera personale e della vita privata di ognuno (*Riservatezza*);
- Rispetto dell'identità e della personalità, della dignità di ogni essere umano (*Individualità e Dignità*);
- Rispetto delle libertà fondamentali costituzionalmente garantite (*Tutela*).

Detti principi sono tradotti, in conformità alla normativa vigente, come segue:

- i dati personali sono raccolti e trattati solo per finalità predeterminate, esplicite e legittime (*Finalità della raccolta*);
- l'utilizzo di dati personali è sempre ridotto al minimo necessario essenziale per il raggiungimento delle finalità dichiarate (*Necessità, Non eccedenza e Essenzialità*);
- i dati personali sono raccolti e trattati solo se funzionali al raggiungimento delle finalità dichiarate (*Pertinenza*);
- i dati personali sono trattati con modalità e strumenti proporzionali alle finalità da raggiungere (*Proporzionalità*);
- i dati personali raccolti e trattati sono sempre puntualmente verificati in modo che sia garantita la loro correttezza e attendibilità (*Esattezza e Completezza*);
- i dati personali raccolti e trattati sono sempre aggiornati con cadenza periodica (*Aggiornamento*);
- i dati personali raccolti sono sempre conservati per un periodo di tempo limitato al raggiungimento delle finalità dichiarate (*Conservazione*);
- i dati personali sono sempre raccolti e trattati previa adozione di idonee misure di sicurezza (*Sicurezza*);
- i dati personali non possono essere trattati per finalità diverse da quelle dichiarate in fase di raccolta o in violazione della disciplina in materia di protezione dei dati personali (*Divieto di Trattamenti Illeciti*).

OBIETTIVI PERSEGUITI

Miglioramento continuo della Tutela dei dati personali mediante:

- l'adozione di un adeguato sistema documentale (procedure, istruzioni operative, modelli documentali standard);
- l'identificazione di delegati dotati di adeguati requisiti e poteri per garantire il corretto funzionamento del sistema di gestione privacy;
- la definizione di un modello organizzativo adeguato al presidio del trattamento dei dati personali inerenti ad ogni processo aziendale;
- l'adozione di misure di sicurezza idonee a prevenire e ridurre al minimo i rischi inerenti il trattamento di dati personali;
- l'adozione delle migliori tecniche disponibili ed economicamente sostenibili per limitare i danni in caso di incidenti o eventi negativi in materia di trattamento di dati personali;
- l'adozione di opportuni criteri e modalità di ripristino dei dati in caso di danneggiamento e perdita accidentale.

Coinvolgimento degli stakeholder e protezione dei dati personali con azioni mirate a:

- sensibilizzare dipendenti, collaboratori, fornitori e clienti su obiettivi e impegni assunti in materia di protezione dei dati personali;
- motivare e coinvolgere il personale dipendente affinché vengano raggiunti gli obiettivi prefissati e sviluppato, ad ogni livello, il senso di responsabilità verso la tutela dei dati personali e la sicurezza delle informazioni;
- formare informare ad un lecito e corretto trattamento dei dati personali e sicurezza delle informazioni;
- promuovere il dialogo e il confronto con tutti i portatori d'interesse tenendo conto delle loro istanze, in materia di trattamento di dati personali.

I principi sopra esposti trovano riscontro nel ***MOPD – Modello Organizzativo per la Protezione dei Dati*** adottato dall'Ente.

4.1 Politiche per la protezione dei Dati Personali

Il titolare del trattamento dimostra una oggettiva responsabilità in merito al sistema di gestione della protezione dei dati, assicurando che le politiche dell'Organizzazione verso la protezione siano definite e congruenti con la linea strategica dell'Organizzazione, con l'ambiente in cui opera e con il profilo di rischio che caratterizza l'attività dell'Organizzazione stessa.

Detti principi sono definiti in più politiche per la protezione dei dati personali, che:

- siano appropriate alla finalità di trattamento ed all'ambiente in cui opera l'Organizzazione, supportando la linea strategica del titolare del trattamento;
- costituiscano un riferimento per i targets posti per la protezione dei dati,
- includano l'impegno alla soddisfazione dei requisiti cogenti e volontari applicabili ed, in particolare, l'impegno formale a soddisfare i requisiti del Regolamento UE 679/2016;
- comprendano la volontà espressa dal titolare del trattamento per il miglioramento continuo del modello organizzativo per la protezione dei dati messo in atto (Plan – Do – Check – Act).

Le politiche per la protezione dei dati devono essere disponibili come informazioni documentate, oltre ad essere costantemente aggiornate in relazione ai mutamenti dell'ambiente, comunicate, recapitate ed attuate all'interno dell'Organizzazione e comunicate agli stakeholders ritenuti importanti per il trattamento dei dati.

Documenti di riferimento:

IOPD 02-002	**Politica generale per il trattamento dei dati personali**
IOPD 02-003	**Politica per la sicurezza, utilizzo degli strumenti informatici, posta elettronica ed Internet**

5. Struttura organizzativa per la protezione dei dati

La normativa sulla protezione dei dati personali individua una serie di figure organizzative.

5.1 Titolare del trattamento

L'Organizzazione**,** rappresentata ai fini previsti dal GDPR dal suo rappresentante legale, è il Titolare del trattamento dei dati personali raccolti in banche dati, automatizzate o cartacee (di seguito indicato con "**Titolare**").

Il Titolare garantisce il 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.

Al **Titolare** di cui all'art. 4 par. 1 punto 7) del Regolamento (UE) 2016/679 sono riconducibili le seguenti principali competenze:

a) determina le finalità e i mezzi del trattamento dei dati personali (art. 4);
b) in caso di minori, verifica che il consenso sia prestato o autorizzato dal titolare della responsabilità genitoriale (art. 9);
c) agevola l'esercizio dei diritti dell'interessato (art. 12) e fornisce agli interessati le informazioni indicate dal GDPR (art. 13);
d) mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento: è il principio di responsabilizzazione (accountability), perno di tutto il GDPR (art. 24);
e) individua i responsabili del trattamento e ne controlla e garantisce l'operato (art. 28);
f) tiene un registro delle attività di trattamento svolte sotto la propria responsabilità (art. 30);
g) garantisce l'idonea formazione del personale autotizzato al trattamento (art. 32 paragrafo 4);
h) comunica all'autorità di controllo (art. 33) e all'interessato (art. 34) eventuali violazioni dei dati;
i) effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali (art. 35);
j) designa il responsabile della protezione dei dati (art. 37) mettendolo in grado di svolgere adeguatamente l'attività (art. 38);
k) è destinatario di provvedimenti, notifiche e ingiunzioni dell'autorità di controllo (art. 58);
l) risponde per il danno cagionato dal suo trattamento che violi il Regolamento (art. 82);
m) è destinatario delle sanzioni amministrative pecuniarie inflitte ai sensi del GDPR (art. 83).

L'Organizzazione 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.

5.2 Contitolari del trattamento

Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Ente da parte di altri enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente e in modo trasparente, anche a mezzo di corrispondenza, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 RGPD.

L'intercorsa corrispondenza definisce le responsabilità di ciascun titolare in merito all'osservanza degli obblighi derivanti dal RGPD, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa europea, statale specificatamente applicabile. L'intesa di contitolarità può individuare un punto di contatto comune per gli interessati.

5.3 Designati al trattamento (delegati)

L'art. 2-quaterdecies (Attribuzione di funzioni e compiti a soggetti designati) del D.Lgs. 196/2003 dispone che "1) Il titolare o il responsabile del trattamento possono 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. 2)

Il titolare o il responsabile del trattamento individuano le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la propria autorità diretta."

Pertanto, ogni responsabile di settore o P.O. può essere individuato quale "**delegato al trattamento dei dati**" relativamente ai servizi e uffici di competenza.

Il Delegato è designato dal Titolare con apposito atto formale, accompagnato da puntuali indicazioni operative per il corretto assolvimento dei compiti in materia di protezione dei dati, da notificarsi per iscritto al Delegato.

Il Delegato al trattamento dei dati personali, relativamente al proprio settore di competenza, risponde al Titolare di ogni violazione o mancata attivazione di quanto previsto dalla normativa in materia di riservatezza, sicurezza, protezione dei dati e amministrazione digitale; riferisce periodicamente al Titolare in ordine alle modalità di svolgimento dei compiti assegnati; verifica che la documentazione cartacea e digitale e le relative procedure informatizzate che supportano l'attività di trattamento dei dati di propria competenza, rispondano ai principi di necessità, pertinenza e non eccedenza, segnalando al Titolare eventuali situazioni di potenziale rischio.

Il Delegato al trattamento dei dati è dotato di autonomia gestionale ed organizzativa per il trattamento dei dati di propria competenza ed è tenuto ad adottare ogni misura necessaria per il rispetto della riservatezza nell'erogazione delle prestazioni e dei servizi in favore del titolare del dato.

5.4 Soggetti autorizzati al trattamento

I dipendenti dell'Organizzazione a tempo determinato o indeterminato ed i collaboratori a qualsiasi titolo, anche tirocinanti, che operano sotto la diretta autorità del Titolare e dei Delegati, sono **soggetti autorizzati** al compimento delle operazioni di trattamento dei dati in forza del contratto di lavoro, o altra tipologia di contratto, e dell'inserimento nella struttura organizzativa dell'organizzazione.

Pertanto è necessario predisporre specifici atti di autorizzazione, limitatamente ai trattamenti di competenza del servizio/ufficio di appartenenza.

I responsabili di area eventualmente designati "**Delegati al trattamento dei dati**" nel cui ufficio/servizio tale personale è inserito o, in mancanza, il Titolare del trattamento, ne curano la formazione in materia di trattamento dei dati e forniscono le necessarie istruzioni, verificandone l'applicazione.

I collaboratori a qualsiasi titolo, anche tirocinanti, e che operano sotto la diretta autorità del Titolare e dei Delegati sono autorizzati al trattamento dati mediante espressa attribuzione nell'atto di incarico. La designazione scritta deve inoltre contenere, quando necessarie, le istruzioni specifiche non già contenute nelle istruzioni generali impartite al personale dipendente o inserito ad altro titolo.

5.5 Responsabile del trattamento dei dati

Nei casi in cui un soggetto terzo effettua trattamenti di dati personali per conto dell'Organizzazione e non può essere considerato come autonomo Titolare, questi è nominato come **Responsabile del trattamento dei dati** ai sensi dell'art. 28 del Regolamento UE 2016/679.

Sono designati responsabili esterni del trattamento di dati personali i soggetti estranei all'Organizzazione che siano tenuti, a seguito di convenzione, contratto, verbale di aggiudicazione o provvedimento di nomina, ad effettuare trattamenti di dati personali per conto del titolare. Pertanto, qualora occorra affidare un incarico comportante anche trattamenti di dati personali, la scelta del soggetto deve essere effettuata valutando anche l'esperienza, la capacità e l'affidabilità in materia di protezione dei dati personali del soggetto cui affidare l'incarico, affinché lo stesso soggetto sia in grado di fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza.

Relativamente alla formalizzazione della nomina conseguente a tutte le tipologie di accordi/contratti, ogni responsabile di settore, designato "delegato al trattamento dei dati" o, in mancaza, il Titolare del trattamento, hanno la responsabilità di garantire che tutti i contratti aventi per oggetto in via diretta o indiretta un trattamento dei dati in nome e per conto dell'Organizzazione contemplino delle specifiche clausole,

definite in accordo con il Responsabile Protezione Dati, ove nominato, relative alla designazione della controparte a Responsabile esterno del trattamento.

In alternativa il contratto dovrà essere integrato con la lettera di designazione a Responsabile Trattamento esterno del trattamento.

Gli atti di incarico riportano, sinteticamente gli elementi di cui all'art. 28 del Regolamento.

A tal proposito l'Organizzazione ha predisposto un'apposita **procedura** operativa così individuata: **MOPD PR05 (Procedura di gestione dei responsabili esterni).**

5.6 Amministratori di sistema (AmmSys)

L'Organizzazione adotta le misure di sicurezza necessarie ad adempiere alle prescrizioni definite dal Garante nel Provvedimento[1] dedicato alla figura dell'Amministratore di Sistema.

L'Organizzazione ha definito specifiche procedure operative per disciplinare i seguenti aspetti:

- selezione e nomina degli Amministratori di Sistema (sia per il personale interno che per i consulenti), attribuzione privilegi, aggiornamento dell'elenco degli amministratori di sistema e relativa formazione obbligatoria
- modifica e revoca delle nomine degli Amministratori di Sistema e dei relativi privilegi prevedendo il successivo aggiornamento del suddetto elenco
- verifica dell'attività degli Amministratori di Sistema
- gestione dei contratti di outsourcing e introduzione in questi ultimi delle opportune clausole per gli adempimenti Privacy in materia di Amministratori di Sistema
- gestione delle richieste da parte degli interessati di consultazione dell'elenco degli Amministratori di Sistema.

Nell'ambito dell'Organizzazione, Il Responsabile Protezione Dati o un soggetto dallo stesso delegato provvede alla verifica almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

L'Organizzazione non ha nominato l'Amministratore di Sistema avendo affidato a Responsabili esterni le relative attività.

5.7 Responsabile della protezione dati (Data Protection Officer)

Il Titolare del trattamento può designare come **Responsabile della protezione dei dati** / **Data Protection Officer** (in seguito indicato con "RPD" o "DPO") un soggetto giuridico esterno qualificato.

Il Responsabile Protezione Dati - RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento, nonché ai dipendenti e collaboratori che eseguono il trattamento, in merito agli obblighi derivanti dal GDPR e dalle altre normative 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 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 GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.
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;

[1] Provvedimento Garante del 27 novembre 2008 - Gazzetta Ufficiale n. 300 del 24 dicembre 2008 (modificato in base al provvedimento del 25 giugno 2009), "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema".

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. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno 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 e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;
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 RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;
f) altri compiti e funzioni a condizione che il Titolare o il Delegato/Referente di settore si assicurino 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 RPD.

Il Titolare del trattamento assicura 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 dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle 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 determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente (Data Breach).

5.8 Referente Organizzativo Privacy

Nell'Organizzazione è prevista la figura del **Referente Organizzativo Privacy dell'Ente.** Esso cura la corretta attuazione delle norme inerenti il trattamento dei dati personali e svolge attività operative che si rendono progressivamente necessarie durante il ciclo di vita di un trattamento dei dati personali collaborando con il Titolare, con i Responsabili dei trattamenti e con eventuali consulenti esterni.

5.9 Coordinamento (Privacy Team)

In assistenza al Titolare può essere costituito un **gruppo di gestione delle attività di trattamento** (**Privacy Team**) costituito dal segretario generale dell'Organizzazione e dai responsabili di settore (responsabile competente per i sistemi informatici (o consulente/tecnico esterno), responsabile dell'ufficio economico-finanziario, ecc.).

Al gruppo compete il coordinamento generale delle funzioni e attività in materia di trattamento dati con particolare riferimento alla gestione delle relazioni con il RPD-Responsabile Protezione dei Dati (o DPO-Data Protection Officer), all'organizzazione della formazione rivolta al personale, alla proposta di aggiornamento della modulistica, alla formulazione di istruzioni in materia di trattamento e verifica della loro applicazione e alla gestione delle violazioni dei dati.

6. Sensibilizzazione, Formazione e Consapevolezza

Le persone che svolgono attività di trattamento sotto il controllo dell'Organizzazione, attraverso nomine e incarichi ad personam ed interventi di informazione e formazione continui e mirati, vengono rese consapevoli:

- della politica per la protezione dei dati personali;
- del proprio contributo all'efficacia del sistema di gestione per la protezione dei dati personali, inclusi i benefici derivanti dal miglioramento delle prestazioni relative alla sicurezza;
- delle implicazioni del non essere conformi ai requisiti del sistema di gestione per la protezione dei dati personali.

6.1 Istruzioni specifiche fornite ai soggetti autorizzati

Ai soggetti autorizzati vengono consegnate formalmente, in allegato alla lettera di autorizzazione alcune istruzioni operative:

- **IOPD 02-001 Politica aziendale per la protezione dei dati personali**
- **IOPD 02-002 Politica generale per il trattamento dei dati personali**
- **IOPD 02-003 Politica per la sicurezza, utilizzo degli strumenti informatici, posta elettronica ed Internet**

Periodicamente, con cadenza almeno annuale, si procederà ad aggiornare la definizione dei dati cui gli autorizzati possono accedere e dei trattamenti che sono autorizzati a porre in essere, al fine di verificare la sussistenza delle condizioni che giustificano tali autorizzazioni.

Il titolare provvederà ad aggiornare periodicamente, almeno annualmente, l'individuazione dell'ambito di trattamento consentito ai singoli autorizzati, ove variato, anche parzialmente (verifica e definizione della struttura organizzativa: aggiornamento delle nomine di responsabilità ed autorizzazione agli autorizzati al trattamento dei dati) revisionando le lettere di nomina.

6.2 Formazione del personale che partecipa ai trattamenti

L'art 32 paragrafo 4 del GDPR stabilisce che: ***"il Titolare del trattamento e il Responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso ai dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"***.

Pertanto, sono previsti **interventi formativi e di sensibilizzazione ai soggetti autorizzati al trattamento**, finalizzati a renderli edotti sui seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli autorizzati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati;
- misure disponibili per prevenire eventi dannosi;
- modalità di aggiornamento sulle misure di sicurezza, adottate dal titolare.

Tali interventi formativi sono programmati in modo tale, da avere luogo al verificarsi di una delle seguenti circostanze:

- già al momento dell'ingresso in servizio;
- durante lo svolgimento delle attività di trattamento, in base ad una specifica pianificazione degli eventi formativi;
- in occasione di cambiamenti di mansioni, che implichino modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti, che implichino modifiche rilevanti nel trattamento di dati personali.

Gli interventi formativi possono avvenire sia all'interno, a cura del Responsabile per il trattamento dei dati o di altri soggetti esperti nella materia, che all'esterno, presso soggetti specializzati.

In ogni caso, sono previste riunioni periodiche per fare il punto sull'evoluzione degli aspetti legati alla sicurezza nel trattamento dei dati personali.

7. Registro delle attività di trattamento

Il principio di responsabilizzazione prevede che ogni titolare "tenga un registro delle attività di trattamento svolte sotto la propria responsabilità (art.30 del GDPR)".

Tale registro deve contenere le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Se l'Organizzazione ha designato uno o più "Responsabili del Trattamento dei Dati" ai sensi dell'art. 28 GDPR, questi ultimi provvederanno a tenere ed aggiornare un registro di tutte le categorie di attività relative al trattamento svolte per conto del titolare del trattamento committente; tale registro deve contenere:

a) il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;
b) le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;
c) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1 del GDPR.

I registri delle attività di trattamento saranno tenuti in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Maggiori dettagli operativi sono riportati nella procedura operativa "**MOPD PR03 – Tenuta del registro attività di trattamento"**.

Documenti di riferimento:

MOPD 03-002	**Registro delle attività di trattamento del Titolare**

8. Rapporti con gli interessati

8.1 Informazione agli interessati (Informativa)

L'informativa contiene le informazioni di cui agli articoli 13 e 14 del Regolamento UE 2016/679 e viene redatta secondo le infìdicazioni delle Linee Guida elaborate dal Gruppo Art. 29 in materia di trasparenza (documento WP 260), definite in base alle previsioni del Regolamento.
In base a quanto stabilito dall'articolo 12 del Regolamento UE 2016/679*, "il Titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma* ***concisa****,* ***trasparente****,* ***intellegibile*** *e* ***facilmente accessibile****,* ***con linguaggio semplice e chiaro****, in particolare nel caso di informazioni destinate specificatamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purchè sia comprovata con altri mezzi l'identità dell'interessato."*

Pertanto l'informativa all'interessato è resa nota nelle seguenti forme:

- è affissa in modo evidente, ed è fornita su supporto cartaceo a fronte di richesta dell'interessato, negli uffici dell'Organizzazione dedicati alle relazioni amministrative con gli interessati (clienti, persone fisiche cui i dati si riferiscono, dipendenti, ecc);
- è pubblicata, in posizione evidente e facilmente raggiungibile sul sito web dell'Organizzazione;
- è comunicata verbalmente e/o per iscritto, dal personale che "accoglie" il potenziale cliente;
- è allegata ai contratti che l'Organizzazione stipula con i propri interessati.

In caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato le seguenti informazioni:

- L'dentità e i dati di contatto del Titolare;
- I dati di contatto del Responsabile della protezione dei dati, ove nominato;
- Le finalità del trattamento nonché la base guridica del trattamento;
- Gli eventuali leggettimi interessi perseguiti dal Titolare del trattamento;
- Gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- Ove applivabile, l'intenzione del Titolare del trattamento di trasferire i dati personali a un paese terzo.

8.2 Acquisizione del consenso degli interessati

Il consenso dell'interessato rappresenta una delle basi giuridiche che rendono ***"Lecito"*** il trattamento; ciò significa che il consenso non sempre è necessario (articolo 6 del Regolamento UE 2016/679).

Quindi, il consenso dell'interessato acquisito, relativamente ai trattamenti per i quali è necessario, si intende a tempo indeterminato, fino ad esplicita revoca da parte dell'interessato.

Il consenso al trattamento è manifestato al personale che ha erogato l'informativa mediante dichiarazione scritta dell'Interessato. La volontà dello stesso è documentata dal personale sull'apposito modulo adottato dall'Organizzazione.

Il consenso dell'interessato deve essere una manifestazione di volontà consapevole, specifica, informata ed esplicita con la quale l'interessato accetta, mediante dichiarazione, che i dati personali che lo riguardano siano oggetto di trattamento.

Il consenso al trattamento dei dati, alla loro raccolta totale o parziale, è revocabile in qualsiasi momento, durante uno specifico episodio o in seguito.

In caso di minori, il consenso deve essere acquisito da chi esercita la potestà genitoriale/legale sull'interessato. In caso di minori, una volta raggiunta la maggiore età, il consenso dell'interessato deve essere acquisito nuovamente.

Il titolare tiene registrazione dell'avvenuta acquisizione del consenso in un archivio centralizzato, preferibilmente in forma informatizzata.

8.3 Modulistica

L'Organizzazione ha adottato modelli uniformi di informativa e attestazioni del consenso, disponibili presso gli Uffici Amministrativi.

Nel caso in cui la specificità di un processo o un trattamento renda necessario adottare moduli ulteriori o difformi, il "Delegato al trattamento", prima di adottare un nuovo modello di informativa/consenso, deve informare il "Titolare del trattamento"; ottenuta l'autorizzazione all'adozione formale del nuovo modello, potrà procedere con la sua elaborazione.

Se l'Organizzazione ha designato il **Responsabile per la Protezione dei Dati** (RPD/DPO), deve essere consultato prima dell'effettivo utilizzo della nuova modulistica.

8.4 Esercizio dei diritti degli interessati

Gli interessati hanno il diritto di ottenere dal Titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento) senza pregiudizio per la liceità del trattamento basata sul consenso acquisto prima della revoca (art. 7, par. 3 Regolamento UE 679/2016).

Inoltre l'interessato potrà proporre reclamo all'Autorità Garante per la Protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

L'esercizio dei premessi diritti può essere esercitato mediante comunicazione scritta da inviare a mezzo PEC, email, fax o lettera raccomandata agli indirizzi di contatto del Titolare o del Responsabile della protezione dei dati (informazioni riportate nella sezione "Identità e dati di contatto del titolare").

Il titolare ha definito una procedura gestionale (**MOPD PR04 – Gestione ed evasione istanze degli interessati**) che descrive i principi generali che disciplinano l'esercizio dei nuovi diritti dell'interessato (accesso, cancellazione, limitazione e portabilità) previsti dal Regolamento UE 2016/679.

Documenti di riferimento:

MOPD 04-001	**Informativa trattamento dati generale**
MOPD 04-010	**Modello esercizio diritti dati personali**
MOPD 04-011	**Registro esercizi diritti interessati**
MOPD 04-022	**Informativa videosorveglianza (estesa)**
MOPD 04-056	**Informativa ai dipendenti**
MOPD 04-101	**Informativa per il sito web**
MOPD 04-102	**Informativa cookie**

9. Affidamento di dati personali all'esterno

L'Organizzazione, in qualità di Titolare del trattamento, deve provvedere alla nomina del Responsabile del trattamento (ai sensi dell'art. 28 del Regolamento) in tutti i casi in cui una terza parte - in qualità di fornitore, partner, appaltatore, subfornitore, subappaltatore, etc. - *esegue per conto dell'Organizzazione, attività, servizi o forniture che comportino un trattamento di dati personali, e tale soggetto non può essere considerato come autonomo titolare o un contitolare del relativo trattamento*.

La nomina a Responsabile deve essere *formalizzata dall'Organizzazione Titolare con apposita lettera o atto scritto* a firma del Titolare o dei soggetti autorizzati ad agire in nome e per conto del Titolare (es "delegati" di specifici compiti e/o funzioni).

Il Responsabile del trattamento designato formalmente dall'Organizzazione si obbliga a rispettare la normativa in materia di Protezione dei Dati Personali e a trattare tali dati secondo le istruzioni impartite dal Titolare. È facoltà del Titolare concedere al Responsabile un margine di discrezionalità in merito alla scelta dei mezzi tecnici ed organizzativi più adatti per l'esecuzione delle attività affidate. Tale margine non può riguardare comunque aspetti essenziali relativi al trattamento previsti dal Regolamento UE 2016/679 (attinenti ad esempio alle modalità e alle finalità con cui sono trattati i dati, alla durata della conservazione, all'accesso ai dati e ad altre misure di sicurezza implementate).

Il Responsabile del trattamento si impegna inoltre a cooperare con il Titolare in qualsiasi momento al fine di assicurare il corretto trattamento dei dati personali e si impegna a fornire al Titolare tutte le informazioni o i documenti che potranno essere richiesti da quest'ultima per l'adempimento degli obblighi di legge e per comprovare l'adozione delle misure tecniche e organizzative definite in qualità di Titolare.

Il titolare ha definito una procedura gestionale (**MOPD PR05 – Gestione dei responsabili esterni**) che descrive i principi generali che disciplinano la nomina dei Responsabili del trattamento nei rapporti contrattuali con i soggetti terzi ai quali sono affidate attività che comportino un trattamento di dati personali.

Documenti di riferimento:

MOPD 05-001	**Elenco dei responsabili del trattamento designati**
MOPD 05-010	**DPA Responsabile esterno del trattamento_ template standard**
MOPD 05-011	**DPA Responsabile esterno del trattamento_ template servizi informatici**

10. Valutazione dei rischi ed adozione delle misure

10.1 Valutazione del rischio

L'Organizzazione ha pianificato e definito un processo di valutazione dei rischi relativi alla protezione dei dati personali che:

- stabilisce i criteri di rischio compresi quelli per la loro valutazione e l'accettazione;
- attua una metodologia di analisi univoca che garantisce nel caso di ripetute valutazioni vengano prodotti risultati coerenti, validi e confrontabili tra loro;
- identifica i rischi relativi alla sicurezza delle informazioni associati alla perdita della riservatezza, integrità e disponibilità delle informazioni incluse nel campo di applicazione del sistema di gestione per la sicurezza delle informazioni ed identifica il responsabile dei rischi;
- analizza i rischi relativi alla sicurezza delle informazioni valutando le possibili conseguenze, la verosimiglianza ed il livello che risulterebbe dal concretizzarsi dei rischi identificati;
- pondera i rischi identificati comparando i risultati dell'analisi con i criteri definiti per la valutazione e l'accettazione e stabilisce le priorità per il trattamento dei rischi per la sicurezza delle informazioni.

La procedura **MOPD PR06 "Gestione analisi dei rischi e valutazione di impatto sulla protezione dei dati (DPIA)"** descrive il dettaglio del processo nonché le modalità di rivalutazione nel tempo.

10.2 Valutazioni d'impatto sulla protezione dei dati (DPIA)

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 del 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 del trattamento alle norme in vigore.

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.

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 individuati i trattamenti determinanti un rischio intrinsecamente elevato, sono determinati in base a quanto precisato dal provvedimento del Garante per la protezione dei dati personali n. 467 del 11/10/2018, e cioè:

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 categorie 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 relative a condanne penali e a reati di cui all'art. 10, GDPR;
f) trattamenti effettuati nell'ambito del raporto di lavoro mediante sistemi tecnologici (anche a riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derive la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;

g) 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;

h) trattamenti su larga scala di dati aventi carattere estremamente personale; dati connessi alla vita familiare o private;

i) trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche;

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

k) 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;

l) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

m) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto;

n) trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza dell'attività di trattamento;

o) trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza dell'attività di trattamento

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.

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'Organizzazione.

Il Titolare deve consultarsi con il RPD, se nominato, 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.

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, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

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.

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 GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

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.

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 l'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.

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.

La procedura **MOPD PR06 "Gestione analisi dei rischi e valutazione di impatto sulla protezione dei dati (DPIA)"** descrive il dettaglio del processo nonché le modalità di rivalutazione nel tempo.

10.3 Sicurezza del trattamento

Il Titolare del trattamento mette in atto misure tecniche ed organizzative 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.

Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: 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.

Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Delegato/Referente di settore del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro), back up e procedure di disaster recovery (business continuity);
- 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.

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.

Il Titolare e ciascun Delegato/Refente di settore 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.

L'adozione di adeguate misure di sicurezza è lo strumento fondamentale per garantire la tutela dei diritti e delle libertà delle persone fisiche. Il livello di sicurezza è valutato tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. L'efficace protezione dei dati personali è perseguita sia al momento di determinare i mezzi del trattamento (fase progettuale) sia all'atto del trattamento.

Nel documento ***IOPD 02-003*** "**Politica per la sicurezza, utilizzo degli strumenti informatici, posta elettronica ed Internet"** vengono riepilogati i criteri e le caratteristiche delle password, e le regole da rispettare per l'utilizzo degli strumenti informatici.

11. Violazione dei dati personali (Data Breach)

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'Organizzazione.

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 all'Autorità di controllo (Garante Privacy). La notifica dovrà avvenire **entro 72 ore** e comunque senza ingiustificato ritardo.

Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del 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, ecc.).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare anche questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali e le modalità con cui si è verificata. 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).

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

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.

Il Titolare ha definito una procedura operativa (**MOPD PR07 – Gestione della violazione dei dati – Data breach**) con l'obiettivo di fornire istruzioni precise e dettagliate nel caso succeda un incidente di sicurezza, e nello specifico una violazione dei dati personali. Assicurare il sistematico trattamento di qualunque violazione dei dati personali, ai sensi degli artt. 33 e 34 del Regolamento europeo UE 2016/679.

Documenti di riferimento:

MOPD 07-001	**Scheda segnalazione incidente**
MOPD 07-002	**Rilevazione e valutazione violazione dati**
MOPD 07-003	**Registro violazioni dati personali**

12. Gestione Operativa

12.1 Sistemi informatizzati centralizzati, condivisi ed individuali

La classificazione dei sistemi informatizzati (inclusi i dispositivi medici) in termini di “centralizzato”, “condiviso” ed “individuale, secondo i criteri espressi nelle definizioni, viene esplicitata nel “Registro dei sistemi informatici (Hw-Sw)”.

Considerata la maggiore criticità, per loro stessa natura anche dal punto di vista della dislocazione, protezione ed accessibilità, dei sistemi classificati come “condivisi” ed “individuali”, il Titolare definisce procedure specifiche per la gestione ed il monitoraggio degli stessi, con particolare riguardo a:

a) le modalità di registrazione e di accessibilità locale ai dati, che devono essere preferibilmente crittografati e non devono essere accessibili al di fuori delle procedure applicative se non a profili di utenza specifici, assegnati individualmente;
b) le modalità di backup;
c) il non utilizzo di dispositivi di registrazione dati removibili;
d) le modalità per un eventuale accesso remoto e comunicazione autonoma con l’esterno.

12.2 Identificazione

L’identificazione dell’utente e l’accesso alle procedure informatizzate è consentito a fronte di credenziali individuali, il più possibile gestite centralmente ed uniche per ogni utente per tutte le procedure dell’organizzazione.

Il titolare definisce una procedura per l’assegnazione delle credenziali che preveda l’identificazione ed il riconoscimento documentato della persona prima dell’assegnazione delle credenziali stesse.

L’anagrafica di tutti gli utenti abilitati ai sistemi informatici è gestita centralmente, e contiene, oltre ai dati identificativi dell’utente stesso, informazioni relative all’affiliazione dell’utente (dipendente o collaboratore dell’organizzazione del titolare, singolo professionista esterno, dipendente o collaboratore di altra struttura sanitaria cooperante nella cura ed assistenza del paziente, dipendente o collaboratore di un fornitore, etc.), e il periodo di abilitazione. La disattivazione di un utente non comporta la cancellazione fisica dello stesso dall’archivio. L’accesso all’archivio degli utenti è riservato a personale autorizzato, mediante un apposito profilo di abilitazione.

Le credenziali hanno il solo scopo di identificare l’utente e non comportano automaticamente alcun profilo di abilitazione, che deve essere esplicitamente associato ad ogni utenza, fra quelli previsti nel sistema acceduto.

12.3 Registrazione degli accessi e delle attività

È obiettivo del titolare che:

a) tutti gli accessi ai sistemi informatici siano registrati in un log, il più possibile centralizzato, all’inizio ed alla fine di ogni sessione;
b) le sessioni operative non possano rimanere attive a tempo indeterminato, al fine di limitare il rischio di accesso non autorizzato a stazioni di lavoro temporaneamente non presidiate.
c) i sistemi informatizzati siano in grado di tenere traccia della data e dell’autore dell’ultima variazione di ogni record contenente dati personali e di mantenere in un log il dettaglio delle attività effettuate da ogni utente nel corso della sessione, con i dati acceduti e/o modificati.

Almeno per i sistemi informatizzati a supporto delle aree di maggior criticità e per i sistemi informatizzati accessibili dall’esterno dell’organizzazione da parte di utenti di altre organizzazioni e/o dal cliente/utente stesso in un contesto di collaborazione territoriale, è impegno del titolare implementare queste funzionalità nelle nuove realizzazioni e di evolvere -ove non comporti uno sforzo sproporzionato- in questo senso i sistemi già esistenti.

13. Verifiche periodiche (Audit Interni)

13.1 Audit interni (Self Audit)

L'Organizzazione deve condurre, ad intervalli pianificati, self audit (audit interni) per verificare che il sistema di gestione (modello organizzativo) per la protezione dei dati sia adeguato, constantemente implementato ed efficamentente attuato.

L'Organizzazione ha predisposto la procedura **MOPD PR09 – Audit interni** al fine di:

- pianificare, stabilire, attuare e mantenere programmi di audit, comprensivi di frequenze, metodi, responsabilità, requisiti di pianificazione e reporting. I programmi di audit devono prendere in considerazione l'importanza dei processi coinvolti e i risultati di audit precedenti;
- definire i criteri di audit e il campo di applicazione per ciascun audit;
- selezionare gli auditor e condurre gli audit in modo da assicurare l'obiettività e l'imparzialità del processo di audit;
- assicurare che i risultati degli audit siano riportati ai pertinenti responsabili;
- conservare le informazioni documentate quale evidenza dell'attuazione del programma di audit e dei risultati di audit.

L'Organizzazione potrà incaricare, in alternativa, un soggetto esterno quaificato per effetture le attività di audit interno.

Se l'Organizzazione ha designato il Responsabile della Protezione dei Dati personali (RPD/DPO) gli audit saranno effettuati dal RPD nell'ambito delle sue funzioni di sorveglianza.

Documenti di riferimento:

MOPD 09-001	**Piano delle Verifiche Ispettive Interne – PVII**
MOPD 09-002	**Rapporto di verifica ispettiva interna**

14. Gestione della documentazione

Il Modello Organizzativo (Sistema di Gestione) per la Protezione dei Dati personali dell'organizzazione comprende:

- le informazioni documentate richieste dalla normativa vigente;
- le informazioni documentate che l'organizzazione ritiene necessarie per l'efficacia del sistema di gestione e per la sicurezza delle informazioni.

Il Titolare e le parti interessate nella fase di pianificazione e monitoraggio del Modello Organizzativo garantiscono che l'estensione delle informazioni documentate sia adeguato rispetto alla:

- dimensione dell'organizzazione e il suo tipo di attività, processi, prodotti e servizi;
- complessità dei processi e delle loro interazioni;
- competenza delle persone.

14.1 Controllo delle informazioni documentate

Le informazioni documentate richieste dal Modello Organizzativo (Sistema di Gestione) per la Protezione dei Dati personali (MOPD) devono essere tenute sotto controllo per assicurare che:

- siano disponibili e idonee all'uso, dove e quando necessario;
- siano adeguatamente protette (per esempio da perdita di riservatezza, uso improprio o perdita d'integrità).

Il controllo delle informazioni documentate, da parte dell'Organizzazione, riguarda le seguenti attività:

- distribuzione, accesso, reperimento e uso;
- archiviazione e preservazione, compreso il mantenimento della leggibilità;
- tenuta sotto controllo delle modifiche (per esempio delle versioni);
- conservazione e successive disposizioni.

Le informazioni documentate di origine esterna ritenute necessarie dall'Organizzazione per la pianificazione e per il funzionamento del Modello Organizzativo (Sistema di Gestione) per la Protezione dei Dati personali (MOPD), vengono identificate e tenute sotto controllo.

Le nomine e gli incarichi definiti nell'ambito del Modello Organizzativo (Sistema di Gestione) per la Protezione dei Dati personali (MOPD) garantiscono che i livelli di accesso siano differenziati in funzione di:

- permessi per prendere soltanto visione delle informazioni documentate;
- permessi e autorità per visualizzarle e modificarle.

Documenti di riferimento:

MOPD 10-001	**Elenco documenti di sistema in uso**
MOPD 10-002	**Elenco leggi e norme applicabili**

15. Miglioramento e revisione

L'Organizzazione individua e seleziona le opportunità di miglioramento ed attua ogni azione necessaria per garantire un livello adeguato di sicurezza delle informazioni e per accrescerne il livello generale di soddisfazione gestendo tutti i processi con un approccio migliorativo.

Questo include:

- Le opportunità di miglioramento della sicurezza delle informazioni così come per affrontare le esigenze e le aspettative future
- La correzione, la prevenzione e la riduzione degli effetti indesiderati
- Il miglioramento delle prestazioni e dell'efficacia del sistema di gestione per la sicurezza delle Informazioni

Sono elementi di miglioramento dell'Organizzazione:

- Il miglioramento della risposta ai requisiti ed alle esigenze del cliente, mediante una continua evoluzione dei propri prodotti e servizi
- L'abbattimento degli eventi indesiderati (contenimento del rischio) quali, ad esempio, i reclami dei clienti o le NC (non conformità) di prodotto o processo

15.1 Non conformità e azioni correttive

Quando si verifica una non conformità l'organizzazione garantisce che vengano attuate le seguenti azioni:

a) reagire alla non conformità e, per quanto applicabile:
   - intraprendere azioni per tenerla sotto controllo e correggerla;
   - fronteggiarne le conseguenze;

b) valutare la necessità di azioni per eliminare le cause della non conformità, in modo che non si ripeta o non accada altrove:
   - riesaminando la non conformità;
   - determinando le cause della non conformità;
   - determinando se esistono o potrebbero verificarsi non conformità simili;

c) attuare ogni azione necessaria;

d) riesaminare l'efficacia di ogni azione correttiva intrapresa;

e) effettuare, se necessario, modifiche al modello organizzativo (sistema di gestione) per la sicurezza delle informazioni.

Le azioni correttive devono essere adeguate agli effetti delle non conformità riscontrate. L'Organizzazione gestisce in accordo alle procedure del Modello Organizzativo le informazioni documentate quale evidenza:

- della natura delle non conformità e ogni successiva azione intrapresa,
- dei risultati di ogni azione correttiva.

15.2 Miglioramento continuo

L'organizzazione migliora in modo continuo l'idoneità, l'adeguatezza e l'efficacia del proprio Modello Organizzativo (Sistema di gestione) per la Protezione dei Dati personali.

Essa considera i risultati delle analisi, delle valutazioni e degli output del riesame annuale della direzione al fine di determinare se ci sono o meno esigenze di opportunità che devono essere considerate come parte del miglioramento continuo.

Tutti i processi descritti dal Modello Organizzativo vengono gestiti in un'ottica di miglioramento continuo.

15.3 Revisione del Modello Organizzativo

La tabella evidenzia le circostanze/cause che rendono necessarie la revisione e l'aggiornamento, anche parziali, del Modello Organizzativo per la Protezione dei Dati (MOPD) dei Dati Personali:

La revisione del MOPD			
1. Approvazione o revisione di norme	**2. Cambiamenti nell'organizzazione**	**3. Innovazione tecnologica e nuove minacce**	**4. Fatti che costituiscono violazioni**
Disposizioni di legge o aventi forza di legge	Nuova *governance* e/o modifiche nel sistema di responsabilità o dell'organigramma	Adozione di nuovi strumenti di lavoro e/o dispositivi per il controllo a distanza	Violazione della riservatezza dei dati
Provvedimenti del Garante e altri atti aventi natura regolamentare	Progettazione di nuove attività/linee di business	Implementazione di versioni aggiornate di strumenti, dispositivi, software	Furto/sottrazione di dati/banche di dati
Revisione di standard	Creazione, accorpamento o dismissione di funzioni	Definizione o censimento di nuove minacce	Perdita accidentale di dati/banche di dati

Le prime tre cause sono di normale verificazione; non generano allarme, sebbene l'organizzazione debba essere pronta a recepire i cambiamenti (ove non addirittura ad anticiparli) e a trarne le dovute conseguenze sul piano formale e operativo.

Le cause di cui al n. 4 devono essere oggetto di particolare attenzione, nel senso che possono evidenziare falle o difetti anche grossolani nel sistema di gestione. L'organizzazione è chiamata ad intervenire sia nel senso di attuare interventi di rimedio, per contenere quanto possibile le conseguenze dell'evento, sia per prevenire il ripetersi di simili eventi. Dal punto di vista giuridico, inoltre, sono tutt'altro che banali le implicazioni in termini di obblighi di cui agli artt. 33 e 34 del Regolamento.

Tale elenco deve essere considerato come indicativo e, sicuramente, non esaustivo.