MANULE DATA PROTECTION

CODICE DI COMPORTAMENTO

PLURIMA S.P.A.

REV.	DATA	DESCRIZIONE E RIFERIMENTI	APPROVATO DA (FIRMA)
0	18.04.2018	Revisione Iniziale	

Sommario

1. SCOPO E CAMPO DI APPLICAZIONE

Il presente Sistema di Gestione della Protezione dei Dati di Plurima S.p.a. (da adesso in poi Plurima) è un modello organizzativo che interpreta la corretta applicazione del REGOLAMENTO UE 2016/679 in considerazione del contesto specifico della realtà organizzativa, delle sue dimensioni e dei settori di trattamento, delle esigenze specifiche dell'impresa e fornendo indicazioni chiare a tutti gli attori del trattamento. Il documento tiene in considerazione la quantità di dati personali trattati in relazione al contesto e ambito aziendale, ciò permette di governare ogni aspetto dei processi legati al trattamento dei dati introducendo il miglioramento continuo aiutando le imprese ad applicare correttamente le norme e ad agire virtuosamente.

Il Sistema di Gestione della Protezione dei Dati ha lo scopo di precisare l'applicazione del Regolamento UE 2016/679 ai Titolari del trattamento e ai Responsabili del trattamento al fine di adottare ed efficacemente attuare i requisiti cogenti in modo adeguato.

Il Sistema di Gestione della Protezione dei Dati di Plurima è utilizzabile a fini interni, per il miglioramento continuo della gestione della protezione dei dati, a fini esterni per scopi di dimostrazione di allineamento normativo, comunicazione e per la certificazione dello stesso modello organizzativo per la protezione dei dati.

Il Sistema di Gestione della Protezione dei Dati conferma l'impegno di Plurima al raggiungimento della conformità con il Regolamento UE 2016/679, dimostrando di essere in grado di garantire un elevato livello di tutela delle informazioni personali e di aver rafforzato la propria posizione quale organizzazione affidabile.

2. RIFERIMENTI NORMATIVI

I documenti di carattere normativo riportati di seguito compongono i requisiti cogenti e volontari per il corretto utilizzo ed applicazione del Sistema di Gestione della Protezione dei Dati Personali:

I. REGOLAMENTO UE 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 abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati);

II. Direttiva 95/46/CE del Parlamento Europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (abrogata dal successivo REGOLAMENTO UE 2016/679);
III. Regolamento (CE) N. 765/2008 del Parlamento Europeo e del Consiglio del 9 luglio 2008 che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il Regolamento (CEE) n. 339/93;
IV. Legge n. 675/1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali del 31 dicembre 1996;
V. D.lgs 196/2003 – Codice in materia di protezione dei dati personali che abroga la precedente legge n. 675/1996 (sopra);
VI. Trattato sul funzionamento dell'Unione europea (TFUE) introdotto dal trattato di Lisbona;
VII. Decisione quadro 2008/977/GAI;
VIII. Carta dei diritti fondamentali dell'Unione europea;
IX. Direttiva UE 2015/1535 del Parlamento Europeo e del Consiglio del 9 settembre 2015 che prevede una procedura d'informazione nel settore delle regolamentazioni tecniche e delle regole relative ai servizi della società dell'informazione (codificazione);
X. ISO/IEC 17065:2012 – Conformity assessment – Requirements for bodies certifying, processes and services;
XI. ISO 19011:2011 – Guidelines for auditing management Systems;
XII. ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements;
XIII. UNI EN ISO/IEC 9001:2015 – Quality management system – Requirements;
XIV. UNI ISO 31000:2010 – Risk Management – Principles and guidelines.

3. TERMINI E DEFINIZIONI

Nel Sistema di Gestione della Protezione dei Dati si applicano i termini e le definizioni di seguito specificati.

Accountability: l'assegnazione della responsabilità di un'attività o processi aziendale, con il conseguente compito di rispondere delle operazioni svolte e dei risultati conseguiti, a una determinata figura aziendale; in ambito tecnico, si intende la garanzia di poter attribuire ciascuna operazione a soggetti (utenti o applicazioni) univocamente identificabili. *(Banca d'Italia, Circolare 285)*

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.

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.

Autorità di Controllo: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; 4.5.2016 L 119/34 Gazzetta ufficiale dell'Unione europea IT.

Comunicazione: il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione. *(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.

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.

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.

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.

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.

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 4.5.2016 L 119/33 Gazzetta ufficiale dell'Unione europea IT 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.

Evidenza: 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.

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.

Interessato: la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali. *(D. Lgs 196/03)*

Limitazione di Trattamento: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

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.

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.

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.

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.

Pseudonimizzazione: il trattamento dei dati personali 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 intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

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.

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.

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.

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; 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.

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.

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.

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.

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.

Utente: qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata. *(D. Lgs 196/03)*

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.

4. CONTESTO E AMBIENTE IN CUI OPERA L'ORGANIZZAZIONE

4.1 CONTESTO E AMBIENTE IN CUI SI SVOLGE L'ATTIVITA' PER LA PROTEZIONE DEI DATI

Plurima è un'azienda che nasce negli anni '90 nella medesima località dov'è sita attualmente la sede principale. Inizia il proprio percorso specializzandosi nei servizi in outsourcing per la gestione di dati Sanitari fino a ricoprire il servizio di gestione documentale completa di ogni tipologia di dato. Nel tempo l'azienda si è specializzata in servizi di logistica integrata, gestione magazzini economali e farmaceutici e all'organizzazione e fornitura di trasporti sanitari vari.

L'ambito di applicazione del presente documento riguarda il trattamento dei dati personali, il trattamento delle categorie particolari di dati, i dati relativi a condanne penali e a reati trattati in azienda.

La determinazione delle realtà interne ed esterne in grado di influenzare la protezione dei dati è basata sul concetto di risk-based-thinking, su questa base si creano le strutture e le politiche interne promosse alla sicurezza, alla liceità e al monitoraggio dei dati trattati, si

assicura un trattamento adeguato dei dati in possesso e la loro gestione mediante modalità informatiche e cartacee, al fine di rivolgere particolare attenzione alla clientela, ai fornitori e al personale interno.

4.2 STAKEHOLDERS: INDIVIDUAZIONE INTERESSI, NECESSITA' E ASPETTATIVE

L'azienda, operando nel settore di outsourcing e servizi sopracitati, ha raccolto una vasta clientela, dalle pubbliche amministrazioni fino alle aziende private. In ogni caso Plurima gestisce una vasta quantità di dati, alcuni dei quali fondamentali per la protezione dei diritti e delle libertà dell'interessato (es. ambito sanitario), l'azienda ha piena coscienza dell'importanza dei trattamenti sviluppati quotidianamente e si è sempre impegnata a trasmetterla ai propri dipendenti e collaboratori.

Gli stakeholders individuati sono il Responsabile del Trattamento dei Dati Personali, il Data Protection Officer (DPO) come figure rilevanti in azienda, all'esterno invece si individuano associazioni ed organizzazioni per la gestione di dati fiscali/retributivi dei dipendenti, professionisti per le attività consulenziali e per la raccolta dei dati sanitari, ed infine di aziende specializzate per sviluppo e la manutenzione della struttura IT.

Plurima ha sviluppato l'analisi nel documento **MDP. 8-A.12 "Ambito e Perimetro di Applicazione"**.

4.3 IL PERIMETRO DEL SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI

Plurima ha esternalizzato pochissimi servizi privilegiando, così, l'internalizzazione delle lavorazioni. La gestione del dato personale è comunque organizzata in buona parte del territorio italiano ed anche la clientela, nella stragrande maggioranza, risiede in gran parte all'interno del medesimo perimetro.

Per comprendere meglio il perimetro di azione dell'azienda è necessario determinare, oltre all'ambiente, agli interessi e alle attività, anche le interfacce tra le attività svolte ed alle entità esterne che hanno rapporti con questa (si rimanda a **MPD. 8-A.11 "Elenco dei Responsabili Esterni del Trattamento"**).

La precisa determinazione del perimetro del Sistema di Gestione della Protezione dei Dati è sviluppata, mantenuta e disponibile come informazione documentata in **MDP. 8-A.12 "Ambito e Perimetro di Applicazione"**.

4.4 IL SISTEMA DI GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI: I REQUISITI E I PROCESSI NECESSARI AL DPMS E ALLA LORO APPLICAZIONE NELL'AMBITO DELL'ORGANIZZAZIONE

Il presente paragrafo ha lo scopo di descrivere il modello in grado di supportare e gestire le entità, i titolari del trattamento o i responsabili del trattamento ad applicare i requisiti cogenti in modo adeguato. Il modello DPMS di Plurima è concepito come uno strumento agile e flessibile, per facilitare al massimo il lavoro del titolare o del responsabile del trattamento dei dati personali.

L'azienda Plurima predispone le proprie risorse per:

- Mantenere informazioni documentate per supportare il funzionamento dei propri processi sui dati personali;
- Conservare le informazioni documentate affinché si possa avere fiducia nel fatto che i processi siano condotti come pianificato;
- Aggiornare il suo profilo di rischio rispetto ai dati personali trattati.

Il Manuale DMPS chiarisce la Politica Direzionale in materia di Protezione dei Dati Personali; definisce l'approccio e le disposizioni generali relative ai processi aziendali aventi influenza sulla Protezione dei Dati Personali e descrive il campo di applicazione del Sistema di Gestione della Protezione dei Dati Personali.

In un apposito capitolo del presente Manuale di Gestione della Protezione dei Dati Personali è dato l'elenco delle procedure.

Nel Manuale DPMS sono descritti:

- i processi necessari del Sistema di Gestione della Protezione dei Dati Personali e la loro interazione;
- i riferimenti normativi dove il Manuale rimanda direttamente agli articoli del Reg. UE 2016/679;

- i riferimenti alle PDP (Procedure Data Protection);
- i riferimenti alle MDP (Modelli Data Protection);
- la politica direzionale in materia di Protezione dei Dati Personali che definisce l'approccio generale agli aspetti trattati;
- regole relative alla Gestione della Protezione dei Dati Personali;
- regole per la conduzione delle valutazioni operate da terzi.

Il Manuale è costituito da:

- 1 pagina identificativa di copia,
- 2 pagine di indice dei capitoli
- capitoli da 1 a 10.

Il Titolare del Trattamento dei Dati trattiene una copia del Manuale di Gestione della Protezione dei Dati presso la sede di Corciano (Perugia), l'altra copia è destinata alla consultazione sempre all'interno della sede di Plurima.

Al momento della distribuzione il Titolare del Trattamento identifica ogni copia distribuita, ne verifica la completezza e lo stato di aggiornamento, compila la pagina identificativa di copia e vi appone la propria sigla.

Copie del Manuale sono diffuse internamente a:

n°1 Direzione Plurima

n°1 Amministrazione

La copia è disponibile per la consultazione da parte di tutto il personale impegnato nel trattamento dei dati. Tutte le copie sono gestite dal Titolare del Trattamento che provvede ad aggiornarle contemporaneamente in caso di modifica. La distribuzione a soggetti esterni è autorizzata dal Titolare del Trattamento.

Le copie non siglate sono da intendersi inutilizzabili.

4.4.1 METODOLOGI A PDCA

Il Data Protection Management System è basato sul ciclo PDCA o *Plan-Do-Check-Act,* ovvero lo strumento utilizzato per conseguire il miglioramento dell'Organizzazione, dei processi e delle attività, viene riassunto nelle 4 aree di cui è composto:

1. Plan (Pianificare): stabilire target e sequenze di attività per fornire risultati conformi alle politiche per la protezione dei dati dell'entità;
2. Do (Fare): attuare le attività per la protezione dei dati;
3. Check (Verificare): controllare le attività per la protezione dei dati rispetto alle politiche della protezione dei dati, ai target, ai requisiti cogenti, riportando opportune informazioni documentate su quanto ottenuto;
4. Act (Intervenire): attività e azioni a seguire il progresso continuo del modello "DPMS".

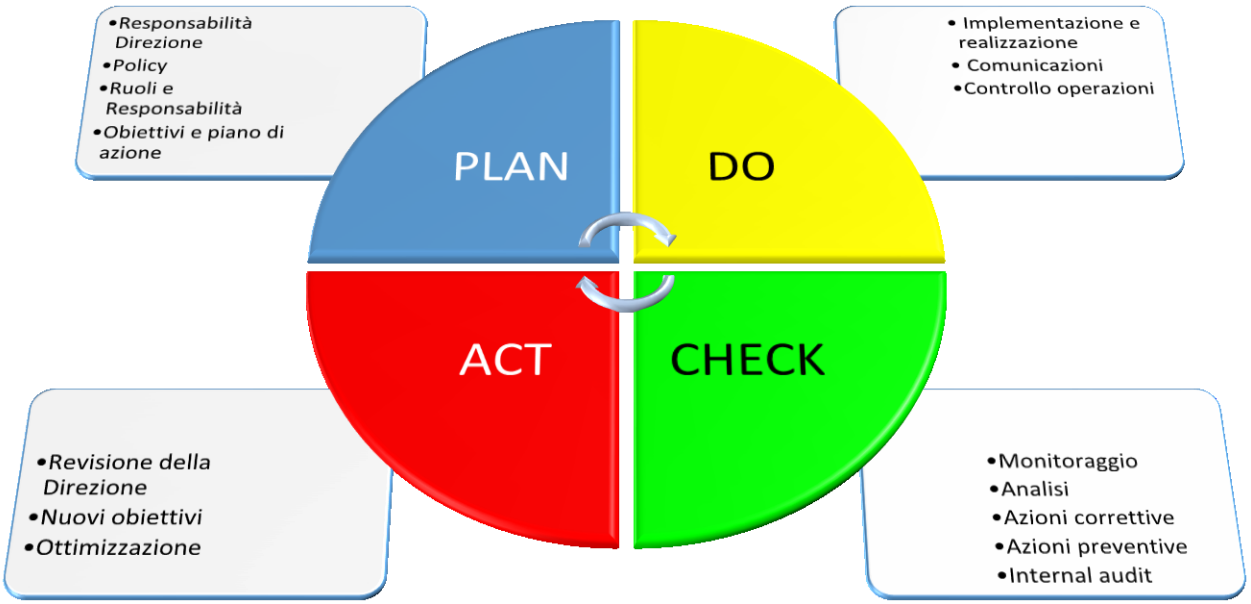

Figura 1. Ciclo PDCA

4.4.2 METODOLOGIA RISK-BASED-THINKING

Il modello DPMS di Plurima sviluppa e mantiene operativa la gestione della protezione del dato personale tramite i principi della gestione del rischio, ovvero strutturare e pianificare il

trattamento dei dati il riferimento al livello di rischio evidenziato per ogni tipologia di trattamento. La gestione operativa ed i riferimenti normativi vengono descritti nel paragrafo 6.1 "Risk Management".

Di seguito è rappresentato il processo di gestione del rischio come tratto dalla norma UNI ISO 31000 "Risk management – Principles and guidelines".

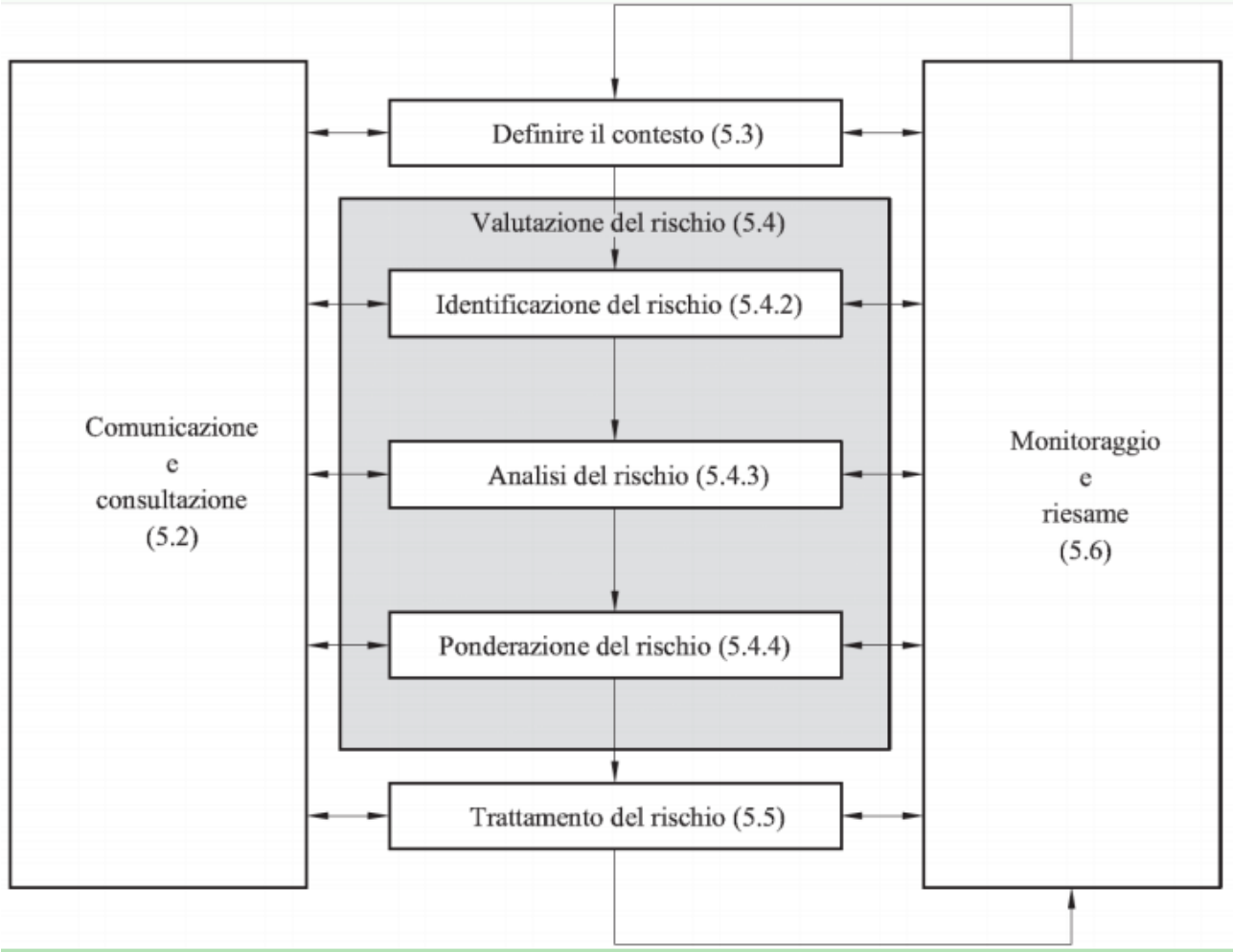

Figura 2. Processo di gestione del rischio, UNI ISO 31000:2010

4.5 DPMS: PROCESSI E PROCEDURE

4.5.1 LE PROCEDURE PER LA GESTIONE DELLA PROTEZIONE DEI DATI PERSONALI

Le Procedure per la protezione dei dati personali descrivono i processi richiesti per attuare il Sistema di Gestione della Protezione dei Dati Personali e comprendono:

- le Procedura Protezione dei Dati Personali che descrivono i processi e le attività necessarie per mettere in atto il sistema
- le Procedura Protezione dei Dati Personali che descrivono le sequenze e la natura interattiva dei processi rilevanti per garantire la sicurezza e la protezione dei dati personali in possesso dell'organizzazione.

Le Procedure Protezione dei Dati personali sono diffuse a tutte le persone che prendono parte alle attività indicate.

Ogni Procedura Protezione dei Dati Personali contiene, come parte integrante, i moduli necessari a produrre i documenti utilizzati.

4.5.2 PROCEDURE DEL SISTEMA DI GESTIONE PER LA PROTEZIONE DEI DATI PERSONALI

La seguente tabella riporta lo schema dei processi e la loro interazione

Procedure	ID procedure
Analisi dei Rischi	**PDP.5-A**
Data Breach e Notifiche	**PDP.7-A**
Diritti dell'Interessato	**PDP.7-B**
Misure di Sicurezza	**PDP.7-C**
Riesame della Direzione	**PDP.7-D**

I processi sono descritti nelle Procedure Protezione dei Dati Personali e per ognuno sono definiti:

- la sequenza e le interazioni dei processi
- i criteri, i metodi (incluse misurazioni e indicatori di prestazioni) e modalità di controllo dei processi
- le risorse necessarie e le modalità per garantire la loro disponibilità
- compiti e responsabilità assegnate
- rischi ed opportunità e piano di implementazione delle azioni per affrontarli
- metodi per monitorare, misurare e valutare i processi e, se necessario, le modifiche da adottare per raggiungere i risultati attesi
- opportunità per il miglioramento del processo e del sistema di gestione per la protezione dei dati personali.

Tutte le informazioni relative al funzionamento dei processi sono documentate e conservate come previsto nelle apposite procedure.

5. IL TITOLARE DEL TRATTAMENTO

Il titolare del trattamento ed il responsabile del trattamento cooperano, su richiesta, con l'autorità di controllo nell'esecuzione dei suoi compiti.

5.1 I DOVERI DEL TITOLARE DEL TRATTAMENTO DELLA PROTEZIONE DEI DATI

Tenuto conto della natura, del perimetro (paragrafo 4.3), dell'ambiente (paragrafo 4.1) e delle finalità del trattamento, nonché dei rischi (accennato nel paragrafo 4.4.2 e descritto nel paragrafo 6.1) aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche ed organizzative adeguate (paragrafo 6.1.3) per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al documento cogente di riferimento. Dette misure sono riesaminate ed aggiornate qualora necessario (6.1.2 e 9.1).

Il titolare del trattamento deve essere informato, competente e dimostrare l'onere che si è assunto in merito al rispetto dei principi applicabili al trattamento dei dati personali e deve essere in grado di comprovarlo fornendo evidenza di adeguata responsabilizzazione in merito.

Il titolare del trattamento deve dimostrare un'oggettiva responsabilità in merito al sistema di gestione della protezione dei dati:

a. POLITICHE: assicurando che le politiche dell'organizzazione verso la protezione dati (descritte al paragrafo 5.2) siano definite e congruenti con la linea strategica dell'organizzazione, con l'ambiente in cui opera l'organizzazione e con il profilo di rischio dell'organizzazione stessa;
b. RISORSE: mettendo a disposizione risorse umane, tecniche e finanziarie (paragrafo 6.1.3) necessarie al sistema di gestione della protezione dei dati personali per operare in modo efficace;
c. MISURE: adottando misure appropriate per fornite all'interessato tutte le informazioni qualora i dati personali siano raccolti presso l'interessato e qualora i dati personali non siano stati ottenuti presso l'interessato;

d. COMUNICAZIONI: effettuando le comunicazioni (paragrafo 7.4) relative al diritto di accesso dell'interessato, alla rettifica e cancellazione, al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche, comprese le informazioni relative alle attività di profilazione e la comunicazione di una violazione dei dati personali all'interessato. Dette comunicazione sono informazioni documentate (vedi paragrafo 7.5);
e. DIRITTI DELL'INTERESSATO: agevolando l'esercizio dei diritti dell'interessato ovvero: diritto di accesso dell'interessato, diritto alla rettifica e alla cancellazione ("oblio"), al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche;
f. INFORMAZIONI: fornendo all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta riferita al diritto di accesso dell'interessato, alla rettifica e cancellazione, al diritto di opposizione ed al processo decisionale automatizzato relativo alle persone fisiche, senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.

5.1.1 I Principi Applicabili Al Trattamento Dei Dati Personali

I principi applicabili al trattamento dei dati personali sono individuati ed organizzati dall'art. 5 del Regolamento UE 2016/679:

a) "Liceità, correttezza e trasparenza": i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato;
b) "Limitazione della finalità": i dati personali devono essere raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è considerato incompatibile con le finalità iniziali;
c) "Minimizzazione dei dati": i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

d) "Esattezza": i dati personali devono essere esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
e) "Limitazione della conservazione": i dati personali devono essere conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal documento cogente di riferimento a tutela dei diritti e delle libertà dell'interessato;
f) "Integrità e riservatezza": i dati personali devono essere trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

5.2 POLITICHE PER LA PROTEZIONE DEI DATI

Plurima ha proporzionato rispetto alle attività di trattamento effettuate, le misure tecniche e organizzative adeguate, le quali, includono la predisposizione e l'attuazione di specifiche politiche in materia di protezione dei dati da parte del titolare del trattamento. Dette politiche sono

- Definite in una o più politiche per la protezione dei dati e sono appropriate alle finalità del trattamento ed all'ambiente (4.1) dell'organizzazione, supportando la linea strategica del titolare del trattamento;
- Costituiscono un riferimento per gli obiettivi posti per la protezione dei dati;
- Includono l'impegno alla soddisfazione dei requisiti cogenti e volontari applicabili ed esplicitamente l'impegno formale a soddisfare i requisiti del Documento cogente di rifermento;
- Comprendono la volontà espressa del titolare del trattamento per il miglioramento continuo del sistema di gestione per la protezione dei dati messo in atto.

Queste politiche sono stabilite e fatte proprie dal titolare del trattamento e conosciute dai responsabili del trattamento e dai lavoratori. L'evidenza della comunicazione delle

politiche è data nella forma decisa dal titolare e risulta allineata con il principio di dimostrabilità risultando disponibile come informazione documentata.
La politica per la Protezione dei Dati Personali è disponibile all'interno dell'organizzazione ed è allegata al presente documento come "**Politica Generale per la Protezione dei Dati Personali**" **(ALL. I)**.

5.3 ORGANIZZAZIONE DELL'ENTITA': RUOLI, RESPONSABILITA' E AUTORITA' NELL'ORGANIZZAZIONE

Il titolare del trattamento determina e mette a disposizione risorse umane, economiche, patrimoniali, finanziarie necessarie per il corretto funzionamento del sistema di gestione della protezione dei dati, si assicura che siano definite adeguate deleghe formalizzate in responsabilità ed autorità. Viene predisposta un'informazione documentata per descrivere la struttura organizzativa (Figura 3. Matrice nominativa identificativa e Figura 4. Organigramma nominativo) con ruoli dell'entità, ne è data comunicazione all'interno dell'organizzazione e viene diffusa la consapevolezza delle interdipendenze organizzative stabilite dal titolare del trattamento.

Il titolare del trattamento ha definito, assegnato e comunicato ai pertinenti ruoli dell'organizzazione le relative responsabilità ed autorità, comprese quelle per:

- Assicurare che il DPMS sia allineato al Regolamento UE 2016/679;
- Assicurarsi che le modalità di gestione producano l'adeguata protezione dei dati personali;

Responsabilità, autorità, incarichi e mansioni delle varie posizioni organizzative di Plurima sono dettagliate nel modello del Sistema di Gestione Integrato **SGI – M. 4A-1 "Job Analysis" ,** invece le figure chiave relative al Sistema Data Protection sono descritte in ogni lettera di responsabilità/incarico.

I collegamenti funzionali Data Protection sono riportati nell'**Organigramma Aziendale (ALL. II)**, al paragrafo successivo o allegato al Manuale di Gestione per la Protezione dei Dati Personali, mentre l'elenco degli incaricati al trattamento è stato implementato nel documento **Registro Elenco Incaricati al Trattamento (ALL III)**. Quest'ultimo viene compilato dagli incaricati dell'ufficio IT, in accordo con gli incaricati dell'ufficio Risorse Umane, gestito e aggiornato sotto la responsabilità del Responsabile dei Sistemi Informativi.

5.3.1 Matrice Ed Organigramma

Si riporta di seguito, in ordine, la matrice nominativa identificativa e l'organigramma aziendale con le figure coinvolte nel Sistema di Protezione dei Dati Personali.

NOME E COGNOME	FUNZIONE	DATA NOMINA	REVOCA NOMINA

Matrice nominativa identificativa

Organigramma nominativo

5.3.2 Contitolari Del Trattamento

Plurima non si avvale di contitolari del trattamento come eventualmente previsto dall'art.26 del Reg. UE 2016/679.

5.3.3 Responsabili Del Trattamento

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del qui presente Manuale per il Sistema di gestione dei Dati Personali, nel rispetto dei requisiti cogenti e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di

autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento, la natura e la finalità del trattamento, il tipo di dati personali trattati e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.

Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;
b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;
c) adotti tutte le misure richieste sulla sicurezza del trattamento;
d) rispetti le condizioni (contrattuali o da altro atto giuridico) per ricorrere a un altro responsabile del trattamento;
e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato;
f) assista il titolare del trattamento nel garantire il rispetto degli obblighi sulla sicurezza del trattamento, sulla notifica di una violazione dei dati personali all'autorità di controllo, sulla comunicazione di una violazione dei dati personali all'interessato, sulla valutazione d'impatto sulla protezione dei dati, sulla consultazione preventiva; tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli (rendendoli inutilizzabili) o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli (rendendoli inutilizzabili) le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

5.3.4 Data Protection Officer (DPO)

Il titolare del trattamento e il responsabile del trattamento designano sistemicamente un responsabile della protezione dei dati (Data Protection Officer, in sigla DPO), ogniqualvolta che:

- le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
- le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali sensibili e cioè che rivelino l'origine razziale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona, o di dati relativi a condanne penali e a reati.

Plurima ha rilevato la necessità di un DPO e ne ha predisposto adeguata designazione mediante il modello **MDP.8-A.5a "Nomina Data Protection Officer".**

Il titolare del trattamento e il responsabile del trattamento si assicurano che il DPO non riceva alcuna istruzione per quanto riguarda l'esecuzione dei suoi compiti. Il DPO non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il DPO riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento. Il DPO può svolgere altri compiti e funzioni che non diano adito ad un conflitto di interessi.

Gli interessati possono contattare il DPO per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal documento cogente di riferimento.

5.3.4.1 I Compiti Minimi Del DPO

Di seguito sono individuati i compiti minimi del DPO:

1. informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
2. sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche (5.2) del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
3. fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati (6.1.4) e sorvegliarne lo svolgimento;
4. cooperare con l'autorità di controllo;
5. fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

6. PIANIFICAZIONE

6.1 RISK MANAGEMENT

Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al documento cogente di riferimento, tenuto conto della natura, del perimetro (4.3), dell'ambiente (4.1) e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, fornendo assicurazione che il Sistema di Gestione per la Protezione dei Dati sia efficace nel conseguire i risultati attesi, prevedendo o riducendo gli effetti indesiderati. Plurima pianifica azioni adeguate per affrontare i rischi, per definire i criteri di accettazione e le modalità di trattamento e per valutarne l'efficacia.

6.1.1 Analisi E Valutazione Dei Rischi

Plurima mantiene informazioni documentate sull'analisi dei rischi effettuata. Detta analisi dei rischi viene revisionata periodicamente (vedi procedura **PDP.7-D "Riesame della Direzione"** paragrafo 7.1 "Riesame del Sistema") e mantenuta aggiornata a seguito modifiche del trattamento.

Tutti i dettagli, sulla procedura di analisi dei rischi, sui contenuti e le risultanze sono riportate nei documenti nella tabella sottostante:

ANALISI DEI RISCHI

DESCRIZIONE	*DOCUMENTO/PROCEDURA*
Analisi dei rischi	PDP. 5-A
Risk Assessment	MDP. 5
Asset Inventory	MDP. 5
Data Mapping	MDP. 4.1-A
Registro di Data Mapping	MDP. 8.9
Penetration Test	-
DPIA	MDP. 6

Tabella documenti/procedure analisi dei rischi

6.1.2 Misure Tecniche E Organizzative

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, dell'ambiente e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

a) la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura (7.5) per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si deve tenere 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.

Le misure di sicurezza adottate da Plurima, sono gestite attraverso le seguenti procedure ed i moduli del Sistema di Gestione della Protezione dei Dati Personali; in corrispondenza di ognuno dei punti esposti è stato redatto un apposito documento che descrive le procedure di sicurezza fisiche, logiche e comportamentali adottate all'interno dell'organizzazione.

TIPOLOGIA	DESCRIZIONE	PROCEDURA	MODULO
Allegato I al Manuale Data Protection	Politica Generale per la Protezione dei Dati		
	Misure di Sicurezza	PDP. 7-C	
	Report di Penetration Test		
	Risk Assessment		MDP. 5
	Asset Inventory		MDP. 5
	Manuale delle Regole di Base		MDP. 7-C.1

Tabella Documenti di Sicurezza

6.1.3 DPIA: Data Protection Impact Assessment

Quando un tipo di trattamenti prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

Plurima deve mantenere informazioni documentate sulla valutazione dei rischi effettuata, la documentazione dedicata è la DPIA (Data Protection Impact Analisys) identificata da **MDP. 6 "DPIA: Data Protection Impact Analisys".**

La valutazione d'impatto sulla protezione dei dati (all'interno dall'analisi dei rischi) è predisposta, mantenuta aggiornata ed effettuata in modo approfondito ogni qual volta l'organizzazione effettua:

1. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
2. il trattamento, su larga scala, di categorie particolari di dati personali (dati sensibili) che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona; o di dati relativi a condanne penali e a reati;
3. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico;

La valutazione d'impatto, contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati; e
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al documento cogente di riferimento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
e) L'identificazione del responsabile del trattamento se esplicitamente delegato dal titolare del trattamento.

6.1.4 Consultazione Preventiva E Trattamento Del Rischio

Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati, indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. Plurima predispone la documentazione necessaria alla consultazione preventiva.

6.2 OBIETTIVI PER LA PROTEZIONE DEI DATI

Plurima ha stabilito obiettivi (targets) per la protezione dei dati, congruenti con le politiche in materia di protezione dei dati (5.2), quantificabili, pertinenti ai trattamenti relativi alle attività ed ai trattamenti dell'organizzazione. Detti obiettivi vengono comunicati e compresi nella procedura "**PDP. 7-D Riesame della Direzione"** e periodicamente rivisti una volta all'anno (vedi 9.3).

Plurima pianifica annualmente gli obiettivi per la protezione dei dati personali in sede di riesame della direzione, definendo:

- Le azioni e le risorse necessarie;
- Le figure responsabili e le eventuali scadenze;
- Criteri di monitoraggio e di verifica delle misure di sicurezza messe in atto per la protezione dei dati personali;

In funzione dei risultati rilevati in sede di monitoraggio, la direzione valuta la necessità di eventuali aggiornamenti degli obiettivi del Sistema di Gestione per la Protezione dei Dati Personali definiti ad inizio periodo in sede di riesame della direzione (vedi paragrafo 9.3).

6.3 CAMBIAMENTI: ATTIVITA' E TRATTAMENTO

Quando Plurima determina la necessità di cambiamento delle attività e/o dei trattamenti e le conseguenti variazioni al Sistema di Gestione della Protezione dei Dati Personali adottato, riesamina l'analisi dei rischi (6.1), valuta l'integrità del Sistema di Gestione della Protezione dei Dati Personali, la disponibilità di risorse (economiche, finanziarie, personale), e valuta l'eventuale nuova distribuzione delle responsabilità (5.3).

Plurima, almeno, considera:

- Lo scopo delle modifiche e tutti i relativi effetti potenziali
- La necessità di conservare l'integrità del Sistema di Gestione per la Protezione dei Dati Personali
- La disponibilità di risorse
- La revisione delle responsabilità e delle figure incaricate.

Dette eventuali modifiche sono input del riesame della direzione (vedi paragrafo 9.3).

7. SOSTEGNO ALL'OPERATIVITA'

7.1 RISORSE E MEZZI PER LA PROTEZIONE DEI DATI

Il titolare del trattamento stabilisce e fornisce risorse (umane, tecniche e finanziarie) ed i mezzi (ambiente di lavoro/infrastrutture) necessari per l'effettivo adempimento dei suoi compiti e per l'esercizio dei propri poteri.

7.1.1 Responsabile Del Trattamento Competente

Per garantire che siano rispettate le prescrizioni del documento di riferimento riguardo al trattamento che il responsabile del trattamento deve eseguire per conto del titolare del trattamento, quando affida delle attività di trattamento a un responsabile del trattamento, il titolare del trattamento deve ricorrere unicamente a responsabili del trattamento che presentino garanzie sufficienti, in particolare in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto misure tecniche e organizzative che soddisfino i requisiti del documento cogente di riferimento, anche per la sicurezza del trattamento.

Il titolare del trattamento mette a disposizione e mantiene l'infrastruttura necessaria a garantire la conformità ai requisiti del documento cogente di riferimento; considerando che come infrastruttura si intende: edifici e impianti, hardware e software, tecnologie dell'informazione e sistemi di comunicazione, dispositivi portatili e sistemi di telelavoro, supporti rimovibili, sistemi di controllo accessi, reti e servizi di rete, infrastrutture di supporto, sistemi di backup, sistemi di messaggistica elettronica, ambienti di sviluppo, filiera di fornitura ICT (Information and Comunication Technology).

7.2 COMPETENZA NELLA MANSIONE PER IL TRATTAMENTO DEI DATI

Il titolare del trattamento determina le competenze nella mansione necessarie all'efficace gestione del Sistema di Protezione dei Dati, e si assicura che le risorse umane coinvolte nella gestione dei dati, siano competenti nella mansione. La competenza nella mansione è resa disponibile come informazione documentata (7.5) sulla base di un apprendimento formale (titolo di studio), apprendimento non formale (corsi di formazione), apprendimento informale (esperienza lavorativa).

Plurima predispone annualmente un **"Piano di Formazione" (MDP. 8-A.13)**, ne monitora l'andamento e ne tiene evidenza tramite il **MDP. 8-A.14 "Registro della Formazione".**

7.2.1 DPO Con Conoscenza Specialistica

Il DPO è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti (5.3.4.1).

Il titolare del trattamento e il responsabile del trattamento sostengono il DPO nell'esecuzione dei compiti, fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria competenza e conoscenza specialistica.

Il DPO può essere un dipendente del titolare del trattamento o del responsabile del trattamento, oppure assolvere i suoi compiti in base a un contratto di servizi (7.5).

Il DPO, quando presente, è incaricato di diffondere la cultura sulla protezione dei dati personali in azienda e la sua competenza deve essere comprovata e mantenuta da opportuni titoli. Il Data Protection Officer, certifica le proprie competenze specialistiche suddette, tramite la Certificazione delle Competenze rilasciata da Organismi di Certificazione del personale in conformità alla norma ISO/IEC 17024, così fornisce evidenza oggettiva di competenza nella mansione per lo svolgimento dei compiti relativi alla protezione dei dati.

La figura del DPO viene descritta nel modello **SGI – M.4A-1 "Job Analisys"**, vengono riportati i requisiti e le conoscenze necessarie per ricoprire tale ruolo, tenendo sempre in considerazione la conoscenza specifica di tale figura all'interno dell'ambito e del contesto dell'Organizzazione.

7.3 COGNIZIONE E CONSAPEVOLEZZA SUL TRATTAMENTO DEI DATI

Il titolare del trattamento, anche attraverso le attività del DPO, quando presente, promuove la cognizione sul corretto trattamento dei dati ai responsabili del trattamento ed a tutto il personale dell'entità, riguardo agli obblighi imposti loro dal documento cogente di riferimento. In particolare, le persone dell'organizzazione devono aver cognizione delle politiche per la protezione dei dati (5.2), di come la loro attività

contribuiscono al corretto trattamento dei dati, e di cosa accadrebbe nel caso di violazione dei requisiti indicati dal Regolamento UE 2016/679.

7.4 COMUNICAZIONI ESTERNE O INTERNE PER LA PROTEZIONE DEI DATI

Il titolare del trattamento deve determinare quali comunicazioni siano pertinenti per il corretto funzionamento del Sistema di Gestione della Protezione dei Dati,

a. Esterne:
    - Comunicazioni all'interessato (7.4.1)
    - Comunicazioni all'autorità di controllo (7.4.2)

7.4.1 Comunicazioni All'Interessato

Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le comunicazioni per il diritto di accesso dell'interessato, per la rettifica e la cancellazione, per il diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche e per la comunicazione di una violazione dei dati personali all'interessato, relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificatamente ai minori.

Le eventuali comunicazioni e le azioni intraprese in riferimento a quanto indicato al punto 7.4, sono gratuite. Se le richieste dell'interessato sono manifestatamente infondate o eccessive, in particolare per il loro carattere ripetitivo, il titolare del trattamento piò addebitare un contributo spese ragionevole tenendo conto dei costi amministrativi sostenuti per la comunicazione previa adeguata informazione preliminare.

Particolare tipo di comunicazione è quella relativa ad una violazione dei dati personali all'interessato, suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. In questo caso il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione descrive con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le misure seguenti:

- il nome e i dati di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;

- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Non è richiesta e, quindi, non si procede alla comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

I. il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
II. il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
III. detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Le comunicazioni all'interessato sono disponibili tramite le apposite informative **MDP. 8-A.1 "Informative".**

7.4.2 Comunicazioni All'Autorità Di Controllo

In caso di comunicazione all'Autorità di Controllo il titolare del trattamento o il responsabile del trattamento comunica all'autorità di controllo i dati di contatto del DPO, mantenendo la comunicazione come informazione documentata (7.5).

All'interno della procedura **PDP. 7-A "Data Breach e Notifiche"** sono descritte le modalità di comunicazione all'autorità di controllo, il modello che sarà utilizzato è **"Notifica al Garante",** attualmente non presente ed in attesa di pubblicazione da parte del Garante Privacy**.**

7.5 INFORMAZIONI DOCUMENTATE PER LA PROTEZIONE DEI DATI

Il titolare del trattamento adotta misure appropriate per fornire tutte le informazioni documentate richieste dal documento cogente di riferimento e dal presente Sistema di Gestione per la Protezione dei Dati Personali. Le informazioni documentate sono fornite

per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni di suo interesse possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. Le informazioni documentate sono tenute sotto controllo in termini di distribuzione, accesso, facile reperimento, utilizzo, archiviazione e corretta conservazione (per il mantenimento della leggibilità nel tempo), controllo delle modifiche, conservazione ed eliminazione.

Le informazioni documentate relative ai requisiti cogenti (normativi, legislativi, regolamentari, volontari) sono tenute sotto controllo, ed è predisposto, dal titolare del trattamento, un adeguato sistema di identificazione ed accesso ai requisiti cogenti applicabili.

Le informazioni documentate relative al Sistema di Gestione della Protezione dei Dati Personali si riassume nell'elenco aggiornato **MDP. 8-A.15 "Elenco Documentazione"**.

8. ESECUZIONE DEI CONTROLLI PER LA PROTEZIONE DEI DATI

8.1 PIANI, CONTROLLI E CAMBIAMENTI SUI PROCESSI

Il titolare del trattamento identifica fin dall'analisi dei rischi (6.1), in riferimento al perimetro (4.3), i processi (anche quelli affidati all'esterno), che deve controllare per la protezione dei dati. Adeguate informazioni documentate (7.5) sui controlli sono presenti e conservate per verificare che i processi individuati siano svolti come predisposto. Il titolare del trattamento rivolge la propria attenzione ai cambiamenti (sui processi, sull'organizzazione, sulle tecnologie, sull'ambiente di lavoro, sulle attrezzature, sulle competenze, sulle persone, sulle funzioni, sui subappaltatori, sui fornitori, sui clienti) e valuta le relative conseguenze sulla protezione dei dati personali, avviando attività per ridurre ogni conseguenza dannosa sulla protezione dei dati.

8.2 MINIMIZZAZIONE DEL DATO PERSONALE

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del perimetro (4.3), dell'ambiente (4.1) e delle finalità del trattamento, come anche dei rischi (6.1) aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, il titolare del trattamento mette in atto misure tecniche e

organizzative adeguate, quali la minimizzazione, ed a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del documento cogente di riferimento e tutelare i diritti degli interessati. Plurima adempie alla minimizzazione del dato personale trattando solamente dati personali strettamente necessari.

8.3 REGISTRI DEL TRATTAMENTO

Ogni titolare del trattamento [e, ove applicabile, il suo rappresentate] tiene un registro delle attività del trattamento (7.5) svolte sotto la propria responsabilità, registrando la quantità di dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. Tale registro contiene tutte le seguenti informazioni:

a) Il nome e i dati di contatto del titolare del trattamento;
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 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.

Plurima ha predisposto il documento **MDP.8-A.9 "Registro del Titolare del Trattamento".**

Ogni responsabile del trattamento tiene un registro di tutte le categorie attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

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 la documentazione delle garanzie adeguate;
d) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Plurima ha predisposto il documento **MDP.8-A.10 "Registro del Responsabile del Trattamento".**

Il titolare del trattamento e il responsabile del trattamento garantiscono un livello di sicurezza adeguato al rischio, che comprende, tra le altre, se del caso:

a) La cifratura dei dati personali;
b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

9. ANALISI E CONTROLLO PER LA PROTEZIONE DEI DATI: VALUTAZIONE DELLE PRESTAZIONI

9.1 METODI E STRUMENTI DI CONTROLLO: MONITORAGGIO, TEST, ANALISI E VALUTAZIONE

A seguito delle analisi e dei processi identificati, il titolare del trattamento identifica le persone o le funzioni interne che hanno il compito di effettuare i controlli, i monitoraggi, le misure e i test, le tempistiche della loro effettuazione e le modalità di analisi dei risultati.

Le metodologie scelte da Plurima sono in linea strategica alle politiche adottate e proporzionali al rischio sulla protezione dei dati e coerenti con il rischio d'impresa. Di seguito si individuano le modalità di analisi e monitoraggio implementate per la corretta gestione del Sistema in questione.

9.2 SELF AUDIT

L'organizzazione conduce cicli continui con cadenza almeno semestrale di self audit (audit interni), per verificare che il Sistema di gestione della Protezione dei Dati sia adeguato, costantemente implementato ed efficacemente attuato. L'utilizzo del sistema di self audit fornisce evidenza che il Sistema di Gestione della Protezione dei Dati sia conforme alle politiche definite. I programmi di audit (con responsabilità, piani, report, metodi, frequenze, criteri, campi di applicazione), sono predisposti ed attuati tenendo conto dell'importanza dei processi relativi alla protezione dei dati e dagli eventuali risultati dei self audit precedenti o di audit eventualmente condotti da terzi.

La gestione dei self audit viene gestita e monitorata tramite **MDP. 8-A.2 "Audit Interno".**

9.3 ANALISI DEL TITOLARE DEL TRATTAMENTO: RIESAME DELLA DIREZIONE

Il titolare del trattamento, periodicamente, sottopone ad analisi l'intero Sistema di gestione per la Protezione dei Dati, per acquisire contezza della sua continua adeguatezza, implementazione, idoneità ed efficacia. Il riesame della direzione è gestito tramite la procedura **PDP. 7-D "Riesame della Direzione"** ed i risultati delle analisi sono conservati come informazioni documentate.

10. AZIONI E PROGRESSI SUL SISTEMA PER LA PROTEZIONE DEI DATI: MIGLIORAMENTO

10.1 REAZIONI E AZIONI CORRETTIVE AL DATA BREACH

Al verificarsi di un Data Breach, il titolare del trattamento, e/o il personale individuato, reagisce con immediatezza attraverso la procedura **PDP. 7-A "Data Breach e Notifiche"**, allo scopo di affrontare e valutare la minaccia accaduta.

I Data Breach vengono affrontati tramite il modello **MDP. 7-A.1 "Data Breach",** questi sono conservati come informazioni documentate (7.5) per il tempo necessario al valore storico.

10.2 DATA BREACH E COMUNICAZIONE ALL'INTERESSATO E ALL'AUTORITA' GARANTE

Nel caso in cui violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento emette una non conformità e comunica la violazione dell'interessato senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, essa dev'essere corredata dei motivi del ritardo.

Il responsabile del trattamento deve informare il titolare del trattamento, senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.

Le comunicazioni all'interessato e all'autorità garante vengono gestite tramite la procedura **PDP. 7-A "Data Breach e Notifiche"** ed i modelli **MDP. 7-A.1 "Data Breach"** e **MDP. 7-A.2 "Notifica al Garante".**

10.3 PROGRESSO E MIGLIORAMENTO CONTINUO DEL DPMS

Tramite le analisi descritte nel presente documento, l'organizzazione adempie e fornisce evidenza del progresso continuo del Sistema di Gestione per la Protezione dei Dati Personali messo in atto.
Plurima ha predisposto un Piano di Miglioramento per l'anno corrente consultabile all'interno della procedura **PDP. 7-D "Riesame della Direzione"** al paragrafo 7.2 "Piano di Miglioramento (anno corrente)". Durante il periodo descritto Plurima mette a disposizione energie e risorse necessarie a raggiungere gli obiettivi prefissati.
Al termine di ogni anno il Piano di Miglioramento viene confrontato con gli avanzamenti sviluppati durante l'anno ed infine valutato mediante il modello **MDP. 7-D.1 "Verbale del Riesame della Direzione",** si procede alla strutturazione di un nuovo Piano di Miglioramento.
Il Sistema di Gestione per la Protezione del Dato Personale viene anch'esso valutato mediante alcuni punti strutturati nella procedura **PDP. 7-D "Riesame della Direzione"** al paragrafo 7.1 "Riesame del Sistema" per verificarne l'efficacia ed una possibile implementazione.