Manuale Privacy

Versione	Descrizione	Modifica	Approvazione
01	Prima emissione	RSGTDP (18/04/2020)	TTD (18/04/2020)

SOMMARIO

1 SCOPO E CAMPO DI APPLICAZIONE

DOMUSMEDIA. al fine di essere conforme ai requisiti del 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:

- protegge i diritti e le libertà fondamentali delle persone fisiche, con particolare riferimento ai dati personali;
- controlla e proteggere i dati personali da accessi non autorizzati o involontari;
- preserva i principi fondamentali per la sicurezza dei dati personali: “riservatezza”, “integrità”, “disponibilità”, “resilienza”;
- assicura la continuità del business e dei servizi;
- minimizza i danni derivanti da eventuali “Data Breach” e/o incidenti per la sicurezza dei dati personali;
- disciplina la circolazione dei dati personali;
- incrementa la sicurezza dei dati attraverso l’efficace applicazione del sistema e dei processi di miglioramento continuo in conformità ai requisiti e alle disposizioni del Regolamento UE 2016/679.
- definisce la struttura organizzativa e le responsabilità al suo interno;
- regolamenta tutte le attività che prevedono il trattamento dei dati personali;
- fornisce evidenza oggettiva che tutti i trattamenti sono condotti in conformità ai requisiti normativi e alle prescrizioni di riferimento.

Sono inclusi:

- i requisiti per la valutazione e la gestione dei rischi
- i requisiti per la valutazione e la gestione e degli impatti relativi ai trattamenti dei dati personali
-

in modo che essi siano adattati alle necessità dell’organizzazione.

Nel presente documento ***DOMUSMEDIA.*** individua e definisce in sintesi:

- la politica per la protezione dei dati personali;
- l'organizzazione dell'azienda;
- i processi;
- le responsabilità;
- le modalità di svolgimento e le responsabilità specifiche delle attività e dei processi aziendali fondamentali.

2 RIFERIMENTI NORMATIVI

DOMUSMEDIA. per l'esecuzione delle attività indirizzate nel presente documento si attiene ai seguenti riferimenti normativi generali

Codice	Titolo
Regolamento UE 2016/679	Regolamento Generale sulla Protezione dei Dati
D Lgs 101/2018	Decreto Legislativo sulla Protezione dei Dati
ISO 29100:2011	Security Techniques – Privacy Framework
ISO 29134:2017	Linee Guida Privacy Impact Assessment (PIA)
ISO 29151:2017	Linee Guida per la protezione delle informazioni personali identificative
WP 243	Linea guida sui responsabili della protezione dei dati (RPD)
WP 248	Linea guida in materia di valutazione impatto sulla protezione dati
WP 250	Guidelines on Personal data breach notification under Regulation 2016-679
WP 185	Linee guida sui servizi di geolocalizzazione su dispositivi mobili intelligenti
WP 242	Linee guida sul diritto alla portabilità dei dati
WP 214	schema di clausole contrattuali per trasferimenti transfrontalieri da responsabile stabilito in Unione Europea a sub-responsabile stabilito in un Paese terzo
WP 185	Linee guida sui servizi di geolocalizzazione su dispositivi mobili intelligenti
WP 253	Linee guida sulle sanzioni amministrative pecuniarie Reg UE 2016-679
G.U. n. 300 del 24 dicembre 2008	Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema
G.U. n. 99 del 29 aprile 2010	Provvedimento in materia di videosorveglianza
Sito Garante Privacy	www.garanteprivacy.it

3 TERMINI E ACRONIMI

3.1 TERMINI

Ai fini del presente documento si applica la terminologia riportata nell'art. 4 *"Definizioni"* del Regolamento UE 2016/679 "Regolamento Generale sulla Protezione dei Dati"

Si ritiene inoltre di specificare la seguente terminologia:

Termine	Definizione
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.
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.
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.
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.
Interessato	Persona fisica cui si riferiscono i dati personali.
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.
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.
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 della Protezione dei Dati o DPO (Data Protection Officer)	Il Titolare del trattamento e il Responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico; 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; le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di dati relativi a condanne penali e a reati. Ha una posizione di supervisione potenzialmente necessaria per le aziende, a seconda del modo in cui usano i dati personali. I DPO devono assicurarsi che le loro aziende si conformino ai requisiti di protezione dei dati.
Dati particolari	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona.
Dati giudiziari	Dati personali relativi alle condanne penali e ai reati.
Informativa	Le informazioni che il Titolare del trattamento deve fornire ad ogni interessato, verbalmente o per iscritto, al momento della raccolta dei dati.

Termine	Definizione
Consenso dell'interessato	Qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazioni o azione positiva inequivocabile, che i dati personali che lo riguardano siano effetto di trattamento.
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.
Riservatezza	La capacità del titolare e del responsabile al trattamento di custodire i dati e renderli fruibili solo a coloro provvisti delle dovute autorizzazioni adottando le misure adeguate di accesso a chi non è autorizzato.
Integrità	Si intende la capacità del titolare e del responsabile al trattamento, di garantire che l'informazione, contenuta all'interno di supporti digitali e/o cartacei, non subisca modifiche o cancellazioni a seguito di errori, di azioni volontarie, malfunzionamenti o danni dei sistemi tecnologici.
Disponibilità	Si intende la capacità di rendere disponibile, per ciascun utente abilitato, le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti.
Resilienza	La capacità di affrontare positivamente, adattarsi alle condizioni d'uso e di resistere all'usura in modo da garantire la disponibilità dei servizi erogati.
DPIA (Data Protection Impact Assessment	Valutazione del modo in cui il trattamento dei dati personali in un'azienda potrebbe rappresentare un rischio elevato per i diritti e le libertà della persona fisica e del modo in cui mitigare tali rischi.
Data Breach	Violazione dei dati personali.
Violazione dei dati personali	Violazione di sicurezza che comporta accidentalmente o in modo illegale la distruzione, la perdita, la modifica, la divulgazione o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque elaborati.
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.
Autorità di controllo	L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51; L 119/34 IT Gazzetta ufficiale dell'Unione europea 4.5.2016. In Italia tale autorità è il Garante Privacy.
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.

3.2 ACRONIMI

Acronimo	Descrizione
AC	Azione Correttiva
MP	Manuale Privacy
Mod	Modulo
NC	Non Conformità
TTD	Titolare del trattamento dei dati personali
DPIA	Data Protection Impact Assessment

4 CONTESTO DI RIFERIMENTO

4.1 L'ORGANIZZAZIONE ED IL SUO CONTESTO

Inserire una descrizione che permetta di far comprendere quali sono i clienti, quale è l'attività aziendale/settore di appartenenza e le ambizioni aziendali.

DOMUSMEDIA. ha come obiettivo strategico quello di garantire un elevato livello di tutela delle persone fisiche, con riguardo al trattamento dei dati personali e alla libera circolazione degli stessi nel rispetto dei diritti e delle libertà fondamentali dei soggetti interessati.

DOMUSMEDIA., quindi, oltre a garantire la qualità dei servizi erogati, la soddisfazione delle esigenze, implicite ed esplicite, del Cliente esterno e interno (da attuare attraverso il miglioramento continuo di tutti i processi aziendali), si impegna nell'applicazione delle disposizioni previste dal Regolamento Europeo per la Protezione dei Dati personali, attraverso l'applicazione del presente documento e delle policy che vi sono menzionate.

L'approccio di ***DOMUSMEDIA.*** per la gestione e la sicurezza dei dati personali tiene conto dei seguenti aspetti del contesto di riferimento.

Area	Fattori interni	Fattori esterni
Risorse Umane	▪ Realizzazione professionale e prospettive di crescita ▪ Accesso a percorsi di formazione ▪ Cultura e valori aziendali ▪ Conoscenza processi aziendali ▪ Certificazioni personali ▪ Capacità di attrarre e trattenere talenti ▪ Soddisfazione economica	▪ Disponibilità risorse con competenze adeguate per assunzione ▪ Accesso a finanziamenti per contratti di assunzione e per formazione ▪ Condizioni medie retributive, contrattuali e di crescita dei competitor ▪ Contratti di lavoro
Produzione	▪ Conoscenze, Esperienza e Competenza ▪ Disponibilità risorse interne ▪ Integrazione con forza vendita	▪ Disponibilità di partner a cui accedere per reperire competenze nei tempi richiesti ▪ Normative specifiche
Mercato	▪ Offerta adeguata alle esigenze dei clienti e alle dinamiche del mercato ▪ Capacità di anticipare l'evoluzione del mercato con offerte innovative ▪ Capacità di fidelizzare i clienti ▪ Pluralità di clienti sia per mercato che per dimensione ▪ Certificazioni aziendali	▪ Situazione generale mercato ▪ Presenza di competitor sul mercato ▪ Alte aspettative dei clienti ▪ Pressione alla riduzione delle tariffe e dei prezzi ▪ Normative per partecipazione a gare
Fattori economici	▪ Investimenti interni ▪ Costo risorse ▪ Penali ▪ Necessità di risorse finanziarie per alimentare la crescita	▪ Accesso al credito (reputazione) ▪ Presenza di competitor nell'accesso alle risorse ▪ Tempi di pagamento da parte dei clienti ▪ Finanziamenti esterni
Infrastruttura/Tecnologia	▪ Disponibilità di infrastrutture tecnologiche adeguate (server, pc, software) ▪ Livello di sicurezza informatica infrastruttura interna ▪ Approfondimento e investimento in ambiti innovativi ▪ Partnership con vendor leader	▪ Vincoli cogenti e normativi particolarmente in ambito privacy e sicurezza informatica ▪ Diffusione nuove tecnologie

Area	Fattori interni	Fattori esterni
Contesto	▪ le caratteristiche del modello organizzativo (ruoli e responsabilità); ▪ le politiche di gestione presenti in azienda ed i relativi obiettivi strategici; ▪ le caratteristiche dei processi e delle infrastrutture aziendali (persone, metodologie, sistemi ICT, tempo e risorse finanziarie); ▪ le aspettative delle 3° parti interessate (ad esempio le garanzie di Privacy o le esigenze di formazione richieste dai dipendenti, la riservatezza delle informazioni ritenute critiche dalla Direzione).	▪ le caratteristiche del modello organizzativo (ruoli e responsabilità); ▪ le politiche di gestione presenti in azienda ed i relativi obiettivi strategici; ▪ le caratteristiche dei processi e delle infrastrutture aziendali (persone, metodologie, sistemi ICT, tempo e risorse finanziarie); ▪ le aspettative delle 3° parti interessate (ad esempio le garanzie di Privacy o le esigenze di formazione richieste dai dipendenti, la riservatezza delle informazioni ritenute critiche dalla Direzione).

4.1.1 Flussi e trattamenti dei dati personali

Nell'applicazione delle disposizioni previste dal Regolamento UE 2016/679 e dal presente documento, ***DOMUSMEDIA.*** predispone per gli interessati le informative sul trattamento dei dati personali (vedi **Mod_IDP "Informativa sul trattamento dei dati personali"** e **Mod_IDD "Informativa sul trattamento dei dati personali dei dipendenti"**) specificando le finalità del trattamento di tali dati e, ove previsto, raccoglie in maniera esplicita i consensi degli interessati.

In conformità al Regolamento UE 2016/679, il Titolare del trattamento (TTD), o il suo Rappresentante (se presente) definisce i flussi dei dati personali, identificando tutte le informazioni utili, e tiene un Registro dei Trattamenti svolti sotto la propria responsabilità (cfr. **Mod_RTP "Registro Trattamenti Privacy"**).

NB. Gli obblighi relativi ai Registri delle attività di trattamento non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'art. 9, paragrafo 1 del Regolamento UE 2016/679, o i dati personali relativi a condanne penali e a reati di cui all'art. 10 del Regolamento UE 2016/679.

4.2 NECESSITÀ E ASPETTATIVE DELLE PARTI INTERESSATE

Di seguito le esigenze e le aspettative delle parti interessate

Parte interessata	Esigenza / aspettativa
Clienti	Mantenimento delle informazioni riservate di ogni cliente (segregazione dei dati)
Soggetti coinvolti dai test sui prodotti	Tutela dei dati personali e sensibili (conformità alla legge)
Dipendenti	Tutela dei dati personali e sensibili (conformità alla legge)
	Formazione
	Organizzazione ed accesso ai dati che sia funzionale alla gestione interna
	Tecnologia adeguata
Proprietà	Rispetto della normativa, tutela del know-how (il dato come asset), efficienza dei processi, tutela del marchio

4.3 CAMPO DI APPLICAZIONE E PERIMETRO DEL MANUALE PRIVACY

Il presente documento si applica ai trattamenti interamente o parzialmente automatizzati di dati personali, compresi i dati particolari e giudiziari (qualora applicabile) e a quelli non automatizzati di dati personali contenuti negli archivi di ***DOMUSMEDIA.*** o destinati a figurarvi.

Il presente documento si riferisce al perimetro logico, fisico e tecnologico di ***DOMUSMEDIA.*** definito di seguito.

4.3.1 Perimetro logico, fisico e tecnologico

Descrivere quali sono i processi/servizi e le informazioni da proteggere.

Descrivere, ed eventualmente inserire, mappe/planimetrie/disegni delle sedi, degli uffici, dei CED, ecc.

Descrivere le componenti tecnologiche (server, rete, ecc.), ed eventualmente inserire schemi di rete o dell'infrastruttura, che veicolano le informazioni da proteggere e permettono l'erogazione/esecuzione dei servizi/processi del perimetro logico.

5 LEADERSHIP

5.1 LEADERSHIP E IMPEGNO

In funzione del contesto di riferimento appena descritto e dell'approccio adottato da ***DOMUSMEDIA.***, la Direzione evidenzia il proprio impegno stabilendo che:

- i ruoli e responsabilità per la gestione dei dati personali sono designati e compatibili con gli indirizzi strategici dell'organizzazione;
- sono attuate le misure tecniche ed organizzative per garantire un livello di sicurezza adeguato al rischio;
- sono disciplinati tutti gli aspetti dell'organizzazione dell'azienda, richiesti ai fini privacy ma utili alla normale gestione aziendale;
- i requisiti del presente documento sono integrati nei processi dell'organizzazione;
- sono disponibili le risorse necessarie al controllo e alla gestione della privacy;
- l'importanza di un'efficace gestione dei dati personali è stata comunicata a tutti i livelli aziendali;
- le risorse coinvolte siano guidate e sostenute per garantire l'efficacia del Manuale Privacy;
- il miglioramento viene continuamente promosso.

5.2 POLITICA, PRINCIPI E DIRITTI DELL'INTERESSATO

DOMUSMEDIA. intende essere per i cittadini, i dipendenti, i partner, i fornitori ed i clienti un valore aggiunto in grado di offrire le migliori soluzioni e servizi, nel rispetto della salvaguardia dei diritti e delle libertà fondamentali delle persone fisiche, con particolare riferimento alla tutela e protezione dei dati personali.

A tal fine ha definito ed applica un **Manuale Privacy** in linea con le disposizioni del Regolamento Europeo 2016/679, garantendo la revisione periodica e il miglioramento continuo di tutti i processi aziendali e servizi erogati.

5.2.1 Politica e principi della privacy

DOMUSMEDIA., riconoscendo l'importanza strategica della tutela dei dati personali e della necessità di predisporre opportune risorse, siano esse di natura materiale (risorse umane, dispositivi informatici e infrastrutture) o immateriali (patrimonio delle informazioni), al fine garantire tale aspetto, ha stabilito una politica fondata sui principi di:

- Coerenza; definendo gli obiettivi e i principi fondamentali che sono alla base del sistema di gestione;
- Protezione; Impegnandosi a proteggere i dati personali di ogni individuo;
- Riservatezza; a garanzia dell'intimità della sfera personale e della vita privata di ognuno;
- Individualità e Dignità; nel rispetto dell'identità e della personalità, della dignità di ogni essere umano;
- Tutela; delle libertà fondamentali costituzionalmente garantite

Inoltre ***DOMUSMEDIA.,*** nella definizione del proprio impegno e nell'espletamento della propria attività, rispetta i seguenti principi nel trattamento dei dati personali:

- liceità: l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- correttezza**:** i dati personali verranno trattati unicamente per le finalità e con le modalità comunicate all'interessato;
- trasparenza: le finalità e le modalità del trattamento saranno comunicate in maniera semplice e comprensibile all'interessato;

- limitazione della finalità: i dati personali sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità;
- minimizzazione dei dati: i dati personali trattati sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- esattezza: i dati personali trattati sono 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;
- limitazione della conservazione: i dati personali sono 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;
- integrità e riservatezza: i dati personali sono trattati in maniera da garantirne un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali;
- responsabilizzazione: Il Titolare del trattamento è competente e in grado di comprovarlo.

DOMUSMEDIA. si pone quindi come obiettivo quello di perseguire il miglioramento continuo al fine di garantire nel tempo un livello di tutela dei dati personali adeguato e conforme.

La Direzione di ***DOMUSMEDIA.*** si impegna a rispettare ed attuare tali impegni, assicurando e verificando periodicamente che la politica sia mantenuta attiva, riesaminata, diffusa a tutto il personale e resa disponibile a tutti gli stakeholder.

5.2.2 Diritti dell'interessato

Il Titolare del trattamento fornisce all'interessato tutte le informazioni e le comunicazioni relative ai trattamenti effettuati in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori, ove applicabile (§ 8.1.7).

Le informazioni e le comunicazioni sui diritti dell'interessato sono fornite per iscritto attraverso il documento "Informativa sul trattamento dei dati personali".

5.3 RUOLI E RESPONSABILITÀ

DOMUSMEDIA. assicura che tutte le responsabilità, autorità e autorizzazioni in ambito privacy sono state definite e comunicate nell'ambito dell'organizzazione stessa. A questo proposito si rimanda all'organigramma aziendale.

DOMUSMEDIA. applica il principio di *Accountability* introdotto nel Regolamento UE 2016/679, disponendo che il Titolare del trattamento adotti politiche e attui misure adeguate per garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato sia conforme al regolamento stesso oltre che al presente documento.

6 PIANIFICAZIONE

6.1 GESTIONE DEI RISCHI PRIVACY

6.1.1 Generalità

L'analisi dei rischi e la valutazione degli impatti relativi alla privacy mirano ad avere una stima dei rischi relativi ai trattamenti presi in esame. Vengono considerati gli scenari di rischio (minacce e vulnerabilità) e le conseguenze applicabili e definito (ove necessario) un piano di azioni (Presidi di Sicurezza) per gestire tali rischi.

Tale attività permette anche di definire:

- Cosa deve essere protetto, attraverso un'analisi funzionale e strutturale del contesto di riferimento;
- Quanto deve essere protetto, attraverso la stima dei livelli gravità sull'operatività causata dalla perdita di riservatezza, integrità e disponibilità dei dati personali trattati;
- Contro chi o cosa ci si deve proteggere, attraverso la valutazione delle minacce che possono sfruttare le vulnerabilità e quindi causare danni;
- Come proteggersi in maniera appropriata, attraverso la definizione di specifici presidi di sicurezza e contromisure, sulla base delle esigenze reali e dell'esperienza pregressa sempre in ambito di gestione del rischio.

6.1.2 Valutazione dei rischi

I trattamenti di dati personali, identificati e controllati utilizzando il **Mod_RTP "Registro Trattamenti Privacy"**, vengono riportati nel **Mod_GRP "Gestione dei Rischi Privacy"**.

6.1.2.1 Valutazione di gravità

La valutazione di gravità è un processo qualitativo, la cui determinazione considera una serie di fattori quali la tipologia di dati personali, la criticità dell'operazione di trattamento, il volume dei dati personali.

In tale fase l'organizzazione deve considerare la possibile gravità sull'operatività causata dalla perdita di:

- Riservatezza, cioè la proprietà di un'informazione volta a garantire che la stessa sia accessibile esclusivamente ai soggetti e/o ai processi legittimamente autorizzati;
- Integrità, cioè la proprietà di un'informazione volta a garantire l'inalterabilità e/o la non modificabilità della stessa da parte di soggetti non legittimamente autorizzati;
- Disponibilità, cioè la proprietà che un'informazione sia accessibile ed utilizzabile a fronte di una richiesta autorizzata.

Tale valutazione avviene assegnando, per ciascun trattamento, i valori delle proprietà sopra citate, adottando una scala compresa tra 1 e 5 (vedi tabella seguente).

Valore	Gravità
5	Molto Alta
4	Alta
3	Media
2	Bassa
1	Molto Bassa

6.1.2.2 Probabilità di accadimento

In questa fase, l'organizzazione determina quali sono i rischi pertinenti al trattamento assegnandogli un valore relativo alla probabilità di accadimento dell'evento, adottando una scala compresa tra 1 e 5 (vedi tabella seguente):

Valore	Probabilità
5	Molto alta
4	Alta
3	Media
2	Bassa
1	Molto bassa

La stima, per ciascun evento (scenario di rischio), è un valore che indica la sua probabilità di accadimento, tenendo conto delle vulnerabilità intrinseche e di possibili eventi passati e studi/statistiche di settore.

Spostandosi col mouse nell'elenco dei Rischi il sistema visualizza le Minacce e le Vulnerabilità associate ad ogni classe di rischio.

6.1.2.3 Valutazione del Rischio

Dopo aver eseguito la valutazione della gravità e la stima della probabilità di ciascun trattamento dei dati personali, il sistema provvederà, in automatico, a calcolare il Livello di Rischio relativo alla Privacy attraverso la formula:

LR = G x P

dove:

- LR è il Livello di Rischio di ciascun trattamento dei dati personali;
- G indica la stima di gravità;
- P è la probabilità di accadimento dei possibili scenari.

La seguente tabella riporta i possibili valori di criticità di ciascun trattamento e le soglie per tale classificazione, stabilite dalla Direzione di ***DOMUSMEDIA.***:

- Rischio Molto Basso (LR ≤ 5)
- Rischio Basso (6 ≥ LR ≤ 10)
- Rischio Medio (11 ≥ LR ≤ 15)
- Rischio Alto (16 ≥ LR ≤ 20)
- Rischio Molto Alto (LR ≥ 21)

Probabilità	***Molto Alta***	***Basso***	***Medio***	***Alto***	***Molto Alto***	***Molto Alto***
	Alta	***Molto Basso***	***Basso***	***Medio***	***Alto***	***Molto Alto***
	Media	***Molto Basso***	***Basso***	***Basso***	***Medio***	***Alto***
	Bassa	***Molto Basso***	***Molto Basso***	***Basso***	***Basso***	***Medio***
	Molto Bassa	***Molto Basso***	***Molto Basso***	***Molto Basso***	***Molto Basso***	***Molto Basso***
		Molto Bassa	***Bassa***	***Media***	***Alta***	***Molto Alta***
		Gravità				

6.1.2.4 Presidi di Sicurezza

La metodologia del trattamento dei rischi privacy prevede che l'organizzazione, per ciascun rischio, identifichi l'azione idonea tra le seguenti opzioni disponibili:

- Accettare, qualora i costi per l'implementazione/modifica/eliminazione dei presidi di sicurezza, siano rilevanti o eccessivi rispetto alle possibili conseguenze. Si può, quindi, decidere di non implementare ulteriori contromisure;
- Mitigare, stabilendo l'implementazione di nuovi presidi di sicurezza o modificando o eliminando quelli già in essere;
- Trasferire a terze parti l'onere delle possibili conseguenze (tale opzione può generare nuovi rischi o modificarne altri già esistenti);
- Evitare, adottando delle misure volte a minimizzare le condizioni che hanno portato quel dato livello di rischio;
- DPIA, qualora si ritenesse necessario approfondire l'analisi dei possibili impatti sulla privacy (tale opzione è definita automaticamente dal sistema per i trattamenti che risultano avere un livello di rischio "Alto" o "Molto Alto").

L'organizzazione, per ogni trattamento cui si è scelta l'opzione "mitigare" o "evitare", deve definire i Presidi di Sicurezza che ritiene idonei a diminuire il valore del Livello di Rischio. Tali Presidi devono essere selezionati dalla maschera che comparirà, facendo doppio click, nella cella corrispondente alla colonna "Presidi di Sicurezza (ISO 27001 – ISO 29151)".

I Presidi di Sicurezza sono estrapolati dalla norma ISO 27001:2013 "Sistemi di gestione per la sicurezza delle informazioni." e dalla norma ISO 29151:2011 "Security Techniques – Linee Guida per la protezione delle informazioni personali identificative".

6.1.3 Valutazione degli impatti privacy (DPIA)

Qualora i livelli di rischio dei trattamenti dei dati personali assumano un valore "Alto" e "Molto Alto" in relazione a limitazioni o violazioni dei diritti e delle libertà delle persone fisiche, o nel caso si ritenga opportuno, si procede ad un'analisi più dettagliata degli impatti relativi alla privacy (DPIA).

La DPIA prevede che vengano analizzati 8 tipi di impatto. Per quelli applicabili, si valutano la "magnitudo" (cioè la gravità relativa a ciascun impatto, al verificarsi degli scenari di rischio valutati) e la "probabilità" (cioè il grado di esposizione a quello specifico impatto) utilizzando la scala valori riportata di seguito.

Valore	Livello
5	Molto Alto
4	Alto
3	Medio
2	Basso
1	Molto Basso

Il sistema provvederà, in automatico, a calcolare il Livello di Impatto, come il valore massimo dei risultati della formula:

LI = M x P

di ciascun impatto applicabile, dove:

- LI è il Livello di Impatto di ciascun trattamento dei dati personali per cui è richiesta la DPIA;
- M indica il valore della magnitudo;
- P è la probabilità che si verifichi ciascun specifico impatto.

La seguente tabella riporta i possibili valori di impatto di ciascun trattamento e le soglie per tale classificazione, stabilite dalla Direzione di ***DOMUSMEDIA.***:

- Impatto Molto Basso (LR ≤ 5)
- Impatto Basso (6 ≥ LR ≤ 10)
- Impatto Medio (11 ≥ LR ≤ 15)
- Impatto Alto (16 ≥ LR ≤ 20)
- Impatto Molto Alto (LR ≥ 21)

Probabilità	***Molto Alta***	***Basso***	***Medio***	***Alto***	***Molto Alto***	***Molto Alto***
	Alta	***Molto Basso***	***Basso***	***Medio***	***Alto***	***Molto Alto***
	Media	***Molto Basso***	***Basso***	***Basso***	***Medio***	***Alto***
	Bassa	***Molto Basso***	***Molto Basso***	***Basso***	***Basso***	***Medio***
	Molto Bassa	***Molto Basso***	***Molto Basso***	***Molto Basso***	***Molto Basso***	***Molto Basso***
		Molto Basso	***Basso***	***Medio***	***Alto***	***Molto Alto***
		Impatti				

L'organizzazione, per ogni trattamento cui è richiesta la DPIA, deve definire i Presidi di Sicurezza che ritiene idonei a diminuire il valore del Livello di Impatto. Tali Presidi devono essere selezionati dalla maschera che comparirà, facendo doppio click, nella cella corrispondente alla colonna "Presidi di Sicurezza (ISO 27001 – ISO 29151)".

La Valutazione d'Impatto (DPIA) è effettuata attraverso l'apposito sheet del modello **Mod_GRP "Gestione dei Rischi Privacy"**.

6.1.4 Piano delle Misure di Controllo

Il Piano delle Misure di Controllo viene compilato al fin di definire, per ciascun processo di trattamento dei dati personali per cui è stata effettuata l'analisi dei rischi e, laddove richiesto, la DPIA, la pianificazione delle attività da implementare per attuare i presidi di sicurezza identificati.

Tale piano deve riportare le informazioni relative a:

- misure di controllo;
- responsabile del rischio;
- data di implementazione.

Il Piano delle Misure di Controllo è dettagliato attraverso l'apposito sheet del modello **Mod_GRP "Gestione dei Rischi Privacy"**.

6.2 REGISTRO DEI TRATTAMENTI

Ogni Titolare del trattamento, e il suo Rappresentante (ove presente), tiene un registro delle attività di trattamento svolte sotto la propria responsabilità.

La tenuta del registro del trattamento, che costituisce un adempimento formale previsto dall'Art. 30 del Regolamento UE 2016/679, è funzionale alla definizione delle misure di sicurezza dei trattamenti.

Il **Mod_RTP "Registro dei Trattamenti Privacy"** predisposto da ***DOMUSMEDIA.*** contiene le seguenti informazioni:

- i dati di contatto del Titolare del trattamento, del Contitolare del trattamento (se presente), del Rappresentante del titolare del trattamento (se presente) e del Responsabile della protezione dei dati (se presente);

- nel caso in cui l'azienda svolga attività in qualità di Responsabile del trattamento, i dati di contatto di ogni Titolare per conto del quale agisce, del Rappresentante del Titolare del trattamento (se presente) e del Responsabile della protezione dei dati del titolare (se presente);
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi eventuali Responsabili esterni;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa la loro identificazione, e la documentazione delle garanzie adeguate;
- luoghi e misure di sicurezza tecniche e organizzative di conservazione dei dati personali;
- i tempi di conservazione e i termini ultimi previsti per la cancellazione delle diverse categorie di dati.

Il **Mod_RTP "Registro dei Trattamenti Privacy"** viene aggiornato ad ogni cambiamento importante (ad esempio all'introduzione di un nuovo trattamento), in caso di estensione delle finalità di trattamento, quando ci sono cambiamenti organizzativi, o all'ingresso di un nuovo fornitore; le informazioni contenute nel registro vengono revisionate annualmente ad intervalli pianificati.

Su richiesta, il Titolare o il Responsabile del trattamento (o loro Rappresentanti) mettono il registro a disposizione dell'Autorità di Controllo cooperando con essa nell'esecuzione dei suoi compiti.

6.3 CONSULTAZIONE PREVENTIVA

Il Titolare, prima di procedere al trattamento, consulta l'Autorità di Controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenti un rischio elevato in assenza di misure adottate per attenuare il rischio.

Al momento di consultare l'Autorità di controllo, il Titolare del trattamento comunica:

- le responsabilità proprie del titolare e, ove presenti, dei contitolari e dei responsabili, in particolare quando l'organizzazione è strutturata come gruppo imprenditoriale;
- le finalità del trattamento e le modalità con cui viene svolto;
- le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del Regolamento UE 2016/679;
- ove applicabile, i dati di contatto del Responsabile della Protezione dei Dati (DPO);
- la valutazione d'impatto sulla protezione dei dati;
- ogni altra informazione richiesta dall'Autorità di controllo.

7 SUPPORTO

7.1 RISORSE, COMPETENZE E CONSAPEVOLEZZA

DOMUSMEDIA. mette a disposizione le risorse necessarie, sia umane che infrastrutturali, per attuare, mantenere e migliorare il presente Manuale Privacy.

7.1.1 Gestione delle Risorse Umane

DOMUSMEDIA. assicura che le risorse umane siano a conoscenza delle loro responsabilità in tema di sicurezza dei dati personali e siano idonee ai ruoli loro assegnati, attraverso la definizione di opportuni termini contrattuali.

In fase di assunzione di nuove risorse, ***DOMUSMEDIA.*** pone attenzione alla corretta gestione dei dati personali nei processi di selezione in ottemperanza la Regolamento Europeo UE 2016/679.

La Direzione di ***DOMUSMEDIA.*** richiede a tutti i dipendenti/collaboratori di rispettare ed attuare le misure di sicurezza definite nel presente documento e di utilizzare i beni condivisi e/o loro assegnati secondo quanto definito dalle relative policy.

Inoltre, si impegna ad attuare politiche adeguate in materia di protezione dei dati personali dei suoi dipendenti (di cui è "Titolare del trattamento") garantendone i diritti in base alle normative vigenti.

Ove necessario, viene fornita formazione, addestramento o altra azione per acquisire le competenze necessarie. La funzione relativa, inoltre, è responsabile direttamente e/o indirettamente della valutazione dell'efficacia degli addestramenti effettuati.

Il Responsabile del trattamento, su input del Titolare, deve assicurare la presenza delle competenze necessarie a ***DOMUSMEDIA.*** prevedendo:

- possibili esigenze future, collegate ai piani ed agli obiettivi strategici e operativi;
- piani di formazione specifici per personale neo-assunto;
- la necessità di ottemperare a requisiti e norme cogenti;
- specifico addestramento per il personale che ricopre ruoli di responsabilità nell'ambito dei processi operativi.

Al fine di mantenere alto il coinvolgimento di tutto il personale, ***DOMUSMEDIA.*** si adopera per assicurare che ogni persona, di ogni livello, sia consapevole della rilevanza e dell'importanza della sua mansione, delle sue attività e di come esse contribuiscano a conseguire gli obiettivi per la gestione dei dati personali e la tutela dei diritti dell'interessato.

7.1.2 Gestione dei Fornitori

DOMUSMEDIA. garantisce gli aspetti di sicurezza inerenti gli accessi ai beni e alle informazioni da parte dei fornitori esterni (con particolare rilievo alla tutela dei dati personali).

Al fine di indirizzare gli aspetti di sicurezza nell'ambito dei rapporti di servizio con i fornitori esterni, ed evitare quindi eventuali violazioni dei dati personali, ***DOMUSMEDIA.*** ha stabilito che i contratti di fornitura con le terze parti prevedano opportune clausole a tutela della privacy.
Vengono altresì definite le responsabilità, sia dell'organizzazione che dei fornitori, nel raggiungere e soddisfare i requisiti della Sicurezza e Protezione dei Dati Personali, tenendo in considerazione:

- la natura delle informazioni e relative modalità di accesso o fornitura delle stesse;
- eventuali requisiti legali e normativi (ad es. sulla protezione delle informazioni, su marchi, copyright o qualunque altro diritto di proprietà intellettuale ed industriale, ecc.);
- gli obblighi di ciascuna parte per l'implementazione dei controlli di sicurezza e di protezione dei dati personali definiti nell'accordo contrattuale di fornitura (ad es. sul controllo degli accessi, sulle modalità di monitoraggio e auditing, ecc.);
- le regole stabilite per l'utilizzo dei dati personali a cui si ha accesso;

- eventuali liste di distribuzione di persone/collaboratori autorizzati ad accedere o ricevere le informazioni oggetto dell'accordo, o specifiche procedure per gestire l'aggiunta o la rimozione di persone/collaboratori a tali liste di distribuzione;
- ulteriori politiche di Tutela dei Dati Personali definite nel contratto di fornitura;
- requisiti e processi per la gestione degli incidenti relativi alla violazione dei Dati Personali;
- eventuali esigenze formative in ambiti privacy per il personale che accede alle informazioni e ai servizi oggetto di fornitura;
- le responsabilità di eventuali subfornitori, inclusi i controlli necessari che devono essere implementati;
- la possibilità per l'organizzazione di effettuare audit sui fornitori;
- i requisiti e le modalità di rescissione delle parti coinvolte;
- l'obbligo per le terze parti di fornire report periodici sull'efficacia dei controlli;
- l'obbligo per i fornitori di essere conformi ai requisiti di sicurezza dell'organizzazione ed a quelli prescritti dal Regolamento EU per la protezione dei dati personali.

Gli accordi con i fornitori prevedono inoltre i requisiti per indirizzare i possibili rischi alla Sicurezza dei Dati Personali derivanti dall'accesso e dalla comunicazione delle informazioni (e dei dati personali in particolare) di ***DOMUSMEDIA.*** durante la filiera di fornitura.

DOMUSMEDIA. assicura che le informazioni condivise con i fornitori abbiano un adeguato livello di protezione in linea con la loro importanza per l'organizzazione (§ 7.3).

7.2 COMUNICAZIONE

L'organizzazione di ***DOMUSMEDIA.***, grazie ai processi di comunicazione e consultazione, incoraggia la partecipazione alle buone prassi in materia di organizzazione, sicurezza e protezione dei dati personali, fornendo un supporto alla corretta applicazione della sua politica e dei suoi obiettivi.

Obiettivo principale della comunicazione in ambito privacy è quello di aiutare le parti interessate a comprendere le problematiche inerenti la protezione dei dati personali e le politiche dell'organizzazione.

La comunicazione deve essere:

- chiara, utilizzando un linguaggio adeguato e comprensibile ai destinatari della comunicazione;
- trasparente, trasmettendo ai destinatari informazioni accessibili e verificabili;
- credibile, veicolando informazioni accurate;
- appropriata, assicurandosi di comunicare informazioni importanti e rilevanti per i destinatari.

Per la comunicazione, sia interna che esterna, sono stati realizzati e messi a disposizione dei dipendenti diversi strumenti informatici di gestione, condivisione e archiviazione delle informazioni.

Per comunicazione esterna si intende la comunicazione da e verso le parti interessate esterne, come i clienti e i fornitori. ***DOMUSMEDIA.*** gestisce le informazioni necessarie alla sua attività tramite lo scambio di moduli di registrazione e report.

7.2.1 Notifiche all'Autorità di controllo delle Violazioni dei Dati Personali

L'art. 33 del Regolamento UE 2016/679 disciplina che, in caso di violazioni dei dati personali che possano compromettere le libertà e i diritti dei soggetti interessati (data breach), è obbligo del Titolare del trattamento notificarlo senza ingiustificato ritardo all'Autorità di controllo, ove possibile entro **72 ore** dal momento in cui ne è venuto a conoscenza.

La notifica al Garante Privacy si effettua compilando il documento pdf sul sito del Garante al link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524

Il modello, opportunamente compilato in ogni sua parte e firmato digitalmente, va inviato tramite posta elettronica al Garante Privacy, seguendo le istruzioni di spedizione presenti sul sito del Garante.

Il Titolare del trattamento, oltre alla notifica, tiene una documentazione su qualsiasi violazione dei dati personali, comprese le circostanze ad essa relative, le sue conseguenze, i provvedimenti adottati per porvi rimedio, ecc.

La documentazione è conservata e resa disponibile per eventuali verifiche dell'Autorità di controllo.

7.2.2 Comunicazione della Violazione all'Interessato

Il Titolare del trattamento, in caso di rischio elevato per i diritti e le libertà della persona fisica, è inoltre tenuto a comunicare all'Interessato la violazione dei dati personali, al fine di consentirgli di prendere le precauzioni necessarie.

La comunicazione deve contenere la natura della violazione dei dati personali e le raccomandazioni che la persona fisica interessata dovrebbe adottare al fine di attenuare i potenziali effetti negativi.

DOMUSMEDIA. ha stabilito, in conformità agli orientamenti impartiti dal Garante Privacy e dal Regolamento UE 2016/679 (art. 34), che le comunicazioni agli Interessati siano effettuate tempestivamente o, qualora si volesse indagare per risalire al trasgressore, in maniera differita.

7.3 CLASSIFICAZIONE E GESTIONE DELLE INFORMAZIONI

DOMUSMEDIA. ha stabilito che le informazioni, i dati personali, i documenti e i beni/asset devono essere classificati tenendo conto dei requisiti legali e di business.

Oltre all'attenzione nei riguardi del valore e della criticità per l'attività aziendale, ***DOMUSMEDIA.*** classifica i dati in base alla loro sensibilità in materia di privacy in ottemperanza a quanto disposto dal nuovo Regolamento UE 2016/679, al fine di garantire i diritti dell'interessato e la liceità del trattamento (in qualità di Titolare e/o Responsabile) su tali dati.

DOMUSMEDIA. adotta una classificazione degli asset in base alle informazioni che contengono mentre, in merito ai dati personali trattati nell'esercizio della propria attività, ***DOMUSMEDIA.*** classifica i dati personali in base alle tipologie definite nel Regolamento UE 2016/679.

I livelli di classificazione stabiliti da ***DOMUSMEDIA.*** garantiscono la disponibilità, l'integrità e la riservatezza delle informazioni e dei dati personali. La classificazione delle informazioni in ottica privacy consente a ***DOMUSMEDIA.*** di poter ottemperare, in modo migliore, al rispetto dei diritti dell'interessato sul controllo dei propri dati personali (art. da 15 a 20 del Regolamento UE 2016/679) facilitandone la rintracciabilità.

È responsabilità del Titolare manutenere ed aggiornare lo schema di classificazione delle informazioni, riportato di seguito.

Livello di Classificazione	Descrizione
Strettamente riservato	Le informazioni e gli asset con questo livello di classificazione sono quelli con il livello di riservatezza più elevato. Essi devono essere disponibili ed accessibili ad un ristretto numero di utenti, in quanto la loro distribuzione deve essere opportunamente autorizzata e controllata per le ripercussioni rilevanti sia sul piano della competitività che sul piano legale. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).

Livello di Classificazione	Descrizione
Confidenziale	Le informazioni e gli asset con questo livello di classificazione devono essere condivisi solamente con un gruppo di utenti esplicitamente identificati e definiti. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).
Uso interno	Le informazioni e gli asset con questo livello di classificazione devono essere condivisi e disponibili solamente con i dipendenti/collaboratori di ***DOMUSMEDIA.*** e con le eventuali terze parti autorizzate (in questo caso gli accessi, i privilegi e le attività eseguite devono essere controllate in maniera adeguata).
Pubblico	Le informazioni e gli asset con questo livello di classificazione comprendono tutti quelli con una definizione di livello diversa da quelle precedentemente descritte e per cui non sono necessarie misure di sicurezza particolari per la loro conservazione ed archiviazione; anche la loro trasmissione non deve essere soggetta a protezioni particolari e può essere fatta liberamente.

In relazione al nuovo Regolamento Europeo per la protezione dei dati personali, vi è una ulteriore classificazione dei dati come segue:

Livello di Classificazione	Descrizione
Dati Identificativi (DPI)	Dati personali che permettono l'identificazione diretta dell'interessato. Laddove la categoria dei dati personali si riferisce ad una serie di informazioni che possono essere messe in relazione ad un soggetto, questi sono i dati che lo individuano immediatamente, ad esempio: il nome ed il cognome. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).
Dati Particolari (DPP)	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati genetici, i dati biometrici, i dati relativi alla salute e i dati relativi alla vita sessuale o all'orientamento sessuale della persona. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).
Dati Giudiziari (DPG)	Dati personali che riguardano il casellario giudiziario, o l'eventualità di una sentenza penale di condanna. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).

Livello di Classificazione	Descrizione
Dati Genetici (DGN)	Dati personali relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica, che risultino dall'analisi di un campione biologico della persona fisica in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) o dell'acido ribonucleico (RNA), ovvero dall'analisi di un altro elemento che consenta di ottenere informazioni equivalenti. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).
Dati Biometrici (DBM)	Dati personali 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. La conservazione, archiviazione e trasmissione delle informazioni con questo livello di classificazione, siano esse in formato elettronico che cartaceo, devono essere protette attraverso opportune misure di sicurezza (autenticazione con password, firma elettronica, crittografia, armadi chiusi a chiave, controllo accessi ad archivi con lettore badge o scansioni biometriche, ecc.).

L'adozione di tale schema da parte di tutti i dipendenti/collaboratori e delle terze parti autorizzate permette di avere un approccio sistematico nel trattare le informazioni e di applicare una metodologia comune a tutta l'organizzazione (agevolando anche il diffondersi della consapevolezza); inoltre, i soggetti interessati avranno più fiducia nella liceità del trattamento dei propri dati personali.

7.3.1 Gestione dei documenti

Per documento si intende un supporto cartaceo o elettronico in cui sono riportati dati e informazioni riconosciuti ed autorizzati.

I documenti sono prodotti/utilizzati da tutte le funzioni aziendali durante lo svolgersi dei diversi processi aziendali.

La documentazione di ***DOMUSMEDIA.*** relativa alla privacy, oltre al presente manuale, include anche i Modelli per la tutela dei dati personali.

Le registrazioni costituiscono le dimostrazioni del conseguimento dell'applicazione e dell'efficacia del MP applicato, fornendo evidenza oggettiva di attività eseguite e/o di risultati ottenuti.

I documenti di origine esterna sono rappresentati da eventuali informazioni e dati non direttamente prodotti nell'ottica del Manuale Privacy, ma che risultano funzionali alla corretta erogazione dei prodotti/servizi. Esempi di documenti di origine esterna possono essere normative di settore in vigore, manuali o documenti tecnici, ecc.

I documenti di origine esterna, prodotti e/o consegnati dal Cliente o proveniente da altre entità esterne e destinati ad essere integrati nelle forniture, sono identificati attraverso un codice alfanumerico così strutturato:

Nome cliente_EXT_NN

dove:

- EXT indica che si tratta di un documento di origine esterna;
- NN indica il numero progressivo di identificazione del documento.

8 ATTIVITÀ OPERATIVE

8.1 PIANIFICAZIONI E CONTROLLI OPERATIVI

DOMUSMEDIA. ha pianificato, sviluppato e tiene costantemente sotto controllo tutti i processi necessari per soddisfare i requisiti di protezione dei dati personali (anche quelli affidati all'esterno). Inoltre ***DOMUSMEDIA.*** mette in atto le opportune misure di controllo per la riduzione degli impatti, monitora le eventuali modifiche e attua i piani per conseguire gli obiettivi per la gestione dei dati personali.

8.1.1 Gestione della Privacy By Design

Il principio della "Privacy by Design" prevede che i dati degli utenti siano tutelati nei sistemi di trattamento per impostazione predefinita: questo significa che la privacy deve essere inclusa, in modo nativo, nei processi di trattamento (raccolta dati, analisi, modifica, elaborazione, ecc.) e nei prodotti e nei servizi offerti. La tutela della privacy viene quindi attuata fin dalla fase iniziale di progettazione dei sistemi di trattamento e per tutto il ciclo di vita del dato.

Non è sufficiente dimostrare di aver implementato le misure minime o qualche misura idonea di sicurezza, ma, in ossequio al principio di accountability, si deve garantire e essere in grado di dimostrare, di aver applicato al trattamento i principi di "protezione dei dati fin dalla progettazione" e di "protezione per impostazione predefinita" (art. 25 del Regolamento UE 2016/679). In altre parole, si ha la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del Regolamento UE 2016/679 e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

L'approccio adottato da ***DOMUSMEDIA.*** è basato sulla valutazione del rischio, nella quale si determina il livello di rischio del trattamento, dopo aver valutato la gravità e la probabilità di accadimento per i diritti e le libertà delle persone.

La "Privacy by Design" sottintende la necessità di prevedere, già in fase di progettazione dei sistemi informatici e delle procedure aziendali, la tutela dei dati sensibili/particolari che vengono trattati (ad esempio limitando il trattamento a quelli effettivamente necessari o adottando sistemi di anonimizzazione dei dati stessi), riducendo così i rischi legati al loro trattamento.

Il Titolare del trattamento deve fare riferimento alle necessità di tutela dei dati personali sin dalla fase di progettazione, sviluppo, selezione e utilizzo di applicazioni, servizi e prodotti.

DOMUSMEDIA. integra la privacy by design nelle proprie procedure interne, garantendo la protezione dei dati personali attraverso l'adozione di misure sia tecniche che organizzative. Nel far questo si tiene conto di:

- obblighi e adempimenti in materia di sicurezza;
- obblighi e adempimenti di garanzia nei confronti dei diritti dell'Interessato;
- collaborazione con soggetti preposti al controllo.

L'approccio alla protezione dei dati personali adottato da ***DOMUSMEDIA.*** recepisce il principio della privacy by design con modalità proattive e non più solo reattive; ciò prevede necessariamente configurazioni, modalità operative, e misure di sicurezza in grado di salvaguardare la riservatezza, l'integrità e la disponibilità dei dati personali (RID) nel momento in cui essi "entrano" nell'organizzazione.

Tutte le principali funzioni aziendali forniscono, per quanto di loro competenza, il proprio contributo alla revisione ed integrazione, dei processi e delle tecnologie in uso.

La Privacy By Design, nella definizione del sistema per la conformità al Regolamento UE 2016/679, deve inoltre considerare che il dato personale deve essere tutelato sempre e comunque, quindi anche quando non è in formato digitale. Vengono previste quindi opportune linee guida per la

gestione di documenti cartacei contenenti informazioni personali, per l'adozione di schedari, portadocumenti, contenitori, ecc. tutti dotati di serratura, per l'archiviazione sicura dei documenti cartacei riportanti dati personali.

Oltre alle misure tecniche (ad es. pseudonimizzazione) e organizzative (ad es. gestione dei data breach), in fase di progettazione di prodotti e servizi devono essere anche adottate ulteriori misure che riguardano:

- le autorizzazioni relative all'accesso ai dati;
- le opportune nomine per il trattamento di dati personali;
- ulteriori misure organizzative funzionali a custodire e controllare i dati.

L'obiettivo del Titolare del trattamento è anche quello di impedire l'accesso e l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento (Considerando 39 del Regolamento UE 2016/679).

La presenza di mansionari e lettere di nomina alle persone autorizzate al trattamento (già "incaricati") diventano necessarie in quanto definiscono i profili di autorizzazione e impongono ai Responsabili del trattamento di attenersi alle istruzioni impartite dal Titolare, evitando così possibili incidenti per la tutela e le libertà delle persone impattate. Le designazioni consentono di distribuire, già in fase di progettazione e quindi prima che avvenga l'effettivo trattamento, le responsabilità tra tutte le figure coinvolte.

8.1.2 Gestione degli Asset

DOMUSMEDIA. gestisce in maniera appropriata i propri asset, classificandoli in:

1. Asset primari: processi/attività, informazioni e dati personali;
2. Asset di supporto: hardware, software, reti, personale, sito, struttura organizzativa.

Gli asset assumono le tipologie di:

- Information asset: dati (personali e di business) digitali e non digitali, sistemi operativi, software applicativo, beni intangibili (conoscenza, marchi, brevetti, …).
- Asset fisici: infrastruttura IT, Hardware, Sistemi di controllo, Servizi IT.
- Risorse Umane: dipendenti, collaboratori esterni e consulenti.

Tutti gli asset di ***DOMUSMEDIA.,*** associati alle informazioni (personali e di business) e alle strutture di elaborazione delle informazioni, sono identificati.

I dipendenti/collaboratori di ***DOMUSMEDIA.*** devono utilizzare gli asset esclusivamente per lo svolgimento delle attività lavorative, rispettando le politiche del presente documento e i manuali di utilizzo specifici di strumenti, dispositivi, ecc.

È vietata qualsiasi attività che possa recare danni agli asset o che risulti in contrasto con le regole contenute nel MP o con le norme vigenti.

Particolare attenzione è posta per gli asset che sono utilizzati per il trattamento di dati personali.

Tutto il personale che svolge attività all'interno di ***DOMUSMEDIA.*** è formato in merito ai trattamenti che può effettuare sui dati ed in merito agli accessi che può eseguire sulle banche dati presenti nell'infrastruttura.

Tutte le attività del personale (interno ed esterno) sono esplicitate in lettere di incarico personali e soggette ad accordi di non divulgazione e riservatezza.

I dipendenti/collaboratori, al termine del periodo di impiego, del contratto o dell'accordo stipulato con il titolare, sono tenuti a restituire gli asset in dotazione, salvo differenti accordi tra le parti.

DOMUSMEDIA. previene la divulgazione, la modifica, la rimozione o la distruzione non autorizzate delle informazioni e dei dati personali con misure opportune in relazione alle tipologie di supporto sulle quali esse sono archiviate.

I supporti non più utilizzabili sono dismessi/eliminati con una procedura che prevede la cancellazione non reversibile delle informazioni memorizzate (ad es. smagnetizzazione) e la distruzione fisica del supporto (incenerimento, trapanatura o altri metodi).

Per rispettare le norme di sicurezza e di tutela ambientale, lo smaltimento di tali supporti è demandato a ditte specializzate esterne, inserite nell'"Albo dei Fornitori Qualificati".

DOMUSMEDIA. garantisce la sicurezza nell'uso di dispositivi portatili prevedendo che:

- gli assegnatari di dispositivi portatili siano istruiti e formati circa i rischi derivanti dal loro utilizzo e dei controlli applicati;
- sui dispositivi siano installati applicativi di protezione dal malware;
- sia attivo un sistema di controllo da remoto per la disabilitazione, cancellazione o blocco degli accessi;
- siano attive opportune procedure di backup automatico delle informazioni;
- siano attivi dei sistemi di autenticazione e di autorizzazione per il controllo degli l'accessi e l'utilizzo dei servizi web;
- siano adottate opportune misure di controllo fisico ai fini di evitarne il furto (ad es. mediante sistemi di blocco fisico);
- siano stipulate polizze assicurative a copertura di eventi di furto;
- i dati privati siano separati da quelli aziendali;
- si utilizzino esclusivamente connessioni wireless protette da protocolli di sicurezza.

8.1.3 Backup delle Informazioni

Al fine di proteggersi dalla perdita di informazioni ***DOMUSMEDIA.***:

- documenta ed attua opportune procedure di backup;
- effettua copie di backup delle informazioni e dei software;
- testa il buon esito delle attività di backup;
- testa i dispositivi/supporti di memorizzazione ad intervalli di tempo regolari.

Per i dati aziendali, eventualmente contenuti su macchine virtuali e NAS, è pianificato un backup con cadenza settimanale.

Non è permessa dalla policy aziendale la conservazione di dati in locale.

Vengono effettuati periodicamente test di ripristino, sia per i dati dei database sia per le VM.

8.1.4 Controllo degli accessi logici

L'organizzazione registra, conserva, protegge e riesamina periodicamente i log degli eventi relativi alle attività degli utenti, alle eccezioni, ai malfunzionamenti e agli eventi relativi alla sicurezza delle informazioni.

Le informazioni contenute nei log devono comprendere:

- gli ID degli utenti;
- le attività dei sistemi;
- data, ora e dettagli degli eventi principali (ad es. log-on, log-off, ecc.),
- ove possibile, identificativo o ubicazione dei dispositivi;
- registrazione dei tentativi di accesso al sistema, sia avvenuti con successo che falliti;
- registrazione dei tentativi di accesso alle informazioni e ad altre risorse, sia avvenuti con successo che falliti;

- cambiamenti nella configurazione del sistema;
- utilizzo dei privilegi;
- utilizzo di servizi ed applicazioni di sistema;
- file acceduti e tipo di accesso (ad es. lettura, aggiornamento, copia, cancellazione, ecc.);
- indirizzi e protocolli di rete;
- allarmi generati dal sistema di controllo degli accessi;
- attivazioni e disattivazioni dei sistemi di protezione (ad es. sistemi antivirus, sistemi di anti-intrusione e controllo);
- registrazione delle attività eseguite dagli utenti tramite applicazioni.

Per i log contenenti dati personali, sono applicate opportune misure di protezione per il rispetto della privacy.

L'organizzazione garantisce la protezione delle registrazioni dei log e dei file stessi di log da:

- manomissioni dei tipi di messaggi registrati;
- modifiche o alterazioni dei file;
- criticità della capacità di memorizzazione dei file di log, che potrebbe comprometterne la registrazione stessa o la sovrascrittura di precedenti eventi.

8.1.5 Controllo degli accessi fisici

La procedura di controllo degli accessi fisici alle sedi/uffici prevede che ogni **dipendente/collaboratore**, successivamente all'assunzione, e le terze parti autorizzate siano dotate di un badge elettronico che li abilita ad accedere alle aree pertinenti in funzione del ruolo ricoperto e delle necessità operative.

Gli accessi dei **visitatori** vengono gestiti nell'area di reception da apposito personale che, previa autorizzazione da parte del dipendente/collaboratore interno che necessita di ricevere l'ospite, è tenuto a consegnare al visitatore stesso apposito badge e a registrare le seguenti informazioni:

- Id del badge assegnato
- nome e cognome del visitatore
- società di appartenenza
- tipo documento
- numero documento
- nome e cognome del dipendente interno
- data
- orario di ingresso
- orario di uscita

Il Visitatore provvederà a riconsegnare il badge in reception al momento dell'uscita.

Espletate le attività di riconoscimento, autorizzazione e registrazione, il visitatore viene informato sui comportamenti minimi da seguire per salvaguardare la sicurezza dell'organizzazione e fatto accomodare in un'apposita area controllata in attesa del dipendente interno che lo ospita. Quest'ultimo è responsabile del visitatore ed è tenuto ad accompagnarlo durante l'intera permanenza presso la sede.

Al termine dell'orario di lavoro, il personale della reception effettua un controllo sui badge ospiti e, in caso di mancata riconsegna di uno di essi, previe le opportune verifiche, provvede ad informare il Titolare.

Tutti i dipendenti/collaboratori/visitatori, durante la loro permanenza nelle sedi di ***DOMUSMEDIA.***, sono tenuti ad indossare ed esporre in maniera visibile il badge; qualora si dovesse rilevare la

presenza di persone sprovviste, questi sono tenuti a segnalare immediatamente l'evento al Titolare o, nel caso di visitatore, alla persona interna che lo ospita.

I diritti di accesso di tutto il personale interno/esterno, e gli accessi stessi, sono periodicamente riesaminati ed aggiornati.

8.1.6 Video Sorveglianza

DOMUSMEDIA. si è dotata di un sistema di video sorveglianza al fine di potenziare gli strumenti in suo possesso per il controllo e la sorveglianza degli accessi, per ragioni di sicurezza. La video sorveglianza è uno strumento di prevenzione e di razionalizzazione dell'azione e degli interventi di chi è preposto a tutelare le esigenze di sicurezza ed è regolamentato mediante il **"Regolamento Video Sorveglianza"[1].**

Rimuovere questo paragrafo se non si effettuano le attività di Video Sorveglianza, così come il punto la relativa informativa nel seguente paragrafo

8.1.7 Gestione informative e consensi

DOMUSMEDIA., al fine di ottemperare alle disposizioni previste dall'art. 13 del Regolamento EU 2016/679 in merito alle informazioni da fornire all'interessato al momento della raccolta dei suoi dati personali, ha predisposto due tipologie di modelli:

1. Mod_IDP "Informativa sul trattamento dei dati personali"
2. Mod_IDD "Informativa sul trattamento dei dati personali dei dipendenti"
3. Mod_IVS "Informativa sul trattamento dei dati personali mediante Video Sorveglianza"

Gli uffici/responsabili preposti, preventivamente rispetto al trattamento, sottopongono l'informativa all'interessato, rendendosi disponibili a chiarire eventuali dubbi.

L'interessato può esprimere il proprio **consenso**, sottoscrivendo il modulo dell'informativa.

Nel caso in cui vengano sottoscritti accordi o contratti, nonché prestati servizi, la concessione del consenso può essere intrinseca nel contratto/accordo stesso.

8.1.8 Gestione delle Violazioni (Data Breach)

DOMUSMEDIA. garantisce una gestione coerente ed efficace delle violazioni dei dati personali. Ciò prevede precise modalità di comunicazione delle violazioni stesse e l'insieme delle attività necessarie ad aumentare il grado di consapevolezza tra i dipendenti/collaboratori e le terze parti interessate. ***DOMUSMEDIA.*** assicura inoltre che le violazioni siano immediatamente gestite, al fine di evitare l'insorgenza o l'aggravamento di danni fisici, materiali o immateriali alle persone fisiche.

DOMUSMEDIA. ha definito i ruoli e le responsabilità delle figure coinvolte, i cui obblighi sono opportunamente definiti nelle specifiche lettere di nomina, e procedure atte a garantire risposte rapide ed efficienti in caso di violazioni dei dati personali.

Gli eventi relative alla sicurezza dei dati personali ed eventuali vulnerabilità rilevate, devono essere segnalati in maniera tempestiva al Titolare e/o al Responsabile del trattamento.

Esempi di eventi di sicurezza che devono essere segnalati sono:

- misure di sicurezza non efficienti;
- compromissione di disponibilità, integrità o riservatezza;
- errori umani;
- non conformità rispetto a politiche, procedure o linee guida;
- falle nella sicurezza fisica;
- cambiamenti non gestiti o controllati;
- malfunzionamenti software o hardware;

[1] Allegato al presente manuale

- violazioni degli accessi;
- violazione dei dati personali.

A ciascun evento segnalato e classificato come violazione dei dati personali viene assegnato un Livello di Criticità adeguato tenendo conto dei seguenti fattori:

a) gravità, in funzione del valore strategico dei dati personali direttamente coinvolti nell'incidente occorso (servizi, sistemi, applicazioni, processi, dati, informazioni, ecc.)
b) impatto, in funzione dell'estensione dell'incidente stesso (numero di persone, processi e servizi/sistemi coinvolti).

In base alle informazioni disponibili sulla gravità e sulle conseguenze che la violazione ha arrecato, i Livelli di Criticità adottati sono quindi:

1. Basso: normale svolgimento delle attività;
2. Medio: incidente rilevante potenzialmente in grado di degenerare in violazione;
3. Elevato: situazione di emergenza;
4. Molto Elevato: situazione di crisi.

Infine viene definito il Livello di Priorità di intervento, utilizzando una scala di valori da 1 (Molto Basso) a 5 (Molto Alto).

Nel caso in cui, a seguito della sua valutazione, l'evento di sicurezza sia classificato come una violazione dei dati personali, il Titolare del trattamento deve:

- registrare l'evento e tutte le informazioni necessarie a definire e classificare la violazione dei dati personali, con i relativi livelli di criticità e priorità e valutazione economica;
- notificare la violazione all'Autorità di controllo competente (Garante Privacy) entro **72** ore dal momento in cui ne è venuto a conoscenza mediante il link https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835;
- quando richiesto, provvedere a comunicarlo anche all'Interessato.

A seguito di ciascuna violazione, devono essere svolte, laddove opportuno, ulteriori e più approfondite indagini per identificare le cause della stessa.

Obiettivo primario della gestione delle violazioni dei dati personali è quello di ripristinare un "normale livello di sicurezza e protezione" e successivamente di attuare le opportune azioni di recupero dei dati personali.

8.1.9 Gestione della richiesta di Esercizio dei Diritti dell'Interessato

L'informativa sul trattamento dei dati personali predisposta da ***DOMUSMEDIA.*** descrive in modo chiaro ed esaustivo i diritti dell'interessato e le modalità per esercitarli.

Il Titolare del trattamento ha predisposto un opportuno canale di comunicazione (definire tale canale di comunicazione) attraverso il quale l'interessato può far richiesta di esercizio dei propri diritti.

DOMUSMEDIA. risponde ad una richiesta di esercizio dei diritti da parte di un interessato attraverso processi comunicati e diffusi all'interno dell'organizzazione.

I diritti dell'interessato vengono definiti agli artt. 7, comma 3, 15, 16, 17, 18, 20 e 21 del Regolamento UE 2016/679 e sono:

- Diritto di revoca del consenso;
- Diritto di accesso;
- Diritto di rettifica;

- Diritto di cancellazione (“diritto all’oblio”);
- Diritto di limitazione del trattamento;
- Diritto di portabilità dei dati;
- Diritto di opposizione.

DOMUSMEDIA. risponde ad una richiesta di esercizio dei diritti con le tempistiche riportate nella seguente tabella:

Tempi	Diritti
48 ore	Diritto di accesso
72 ore	Diritto di revoca del consenso
	Diritto di rettifica
	Diritto di cancellazione (“diritto all’oblio”)
	Diritto di limitazione del trattamento
	Diritto di opposizione
7 giorni	Diritto di portabilità dei dati

Il dipendente/collaboratore che deve prendere in carico tale richiesta è debitamente formato ed istruito sulle modalità operative predisposte da ***DOMUSMEDIA.***

Per ottemperare alle richieste di esercizio dei diritti è stato implementato un processo che, attraverso l’inserimento del nominativo dell’interessato all’interno della banca dati, mostri tutti i dati che lo riguardano. Il solo personale autorizzato può rispondere alla richiesta di diritto e avviare, quindi, i flussi di controllo affinché tali modifiche diventino operative.

I dati riguardanti l’interessato contenuti all’interno dei backup effettuati da ***DOMUSMEDIA.*** prima della richiesta di esercizio dei diritti verranno sovrascritti completamente nell’arco di 2 mesi, in quanto effettuare tale modifica manualmente su tutti i backup sarebbe troppo oneroso per l’organizzazione.

Alla ricezione di una richiesta di esercizio dei diritti il sistema archivia la stessa in un database specifico.

Qualora fosse necessario effettuare un ripristino dei dati da un backup precedente alla richiesta, il sistema invia un alert che informa il dipendente/collaboratore sulle nuove richieste di esercizio dei diritti, così che possa controllare e/o gestire nuovamente la modifica.

Nel caso in cui i dati siano trattati anche in maniera cartacea, ***DOMUSMEDIA.*** ottempera alla richiesta di esercizio dei diritti inserendo manualmente le opportune modifiche o distruggendo il documento.

DOMUSMEDIA., dopo aver ricevuto la richiesta, si impegna a controllare che la modifica sia correttamente applicata a tutti i sistemi e, se presenti, anche a tutti i documenti cartacei.

Fa eccezione il diritto di portabilità per cui, a seguito della ricerca dei dati dell’interessato all’interno della banca dati, l’art. 20, paragrafo 2 del Regolamento UE 2016/679, obbliga il Titolare a trasmettere i dati direttamente a un Titolare diverso se “tecnicamente fattibile”. Per adempiere a questa direttiva ***DOMUSMEDIA.*** ha:

- instaurato, quando possibile, una comunicazione sicura fra i sistemi dei Titolari.
- deciso di utilizzare uno strumento automatizzato che consenta l’estrazione dei dati pertinenti. Questo approccio permette di estrarre le parti di set di dati che sono pertinenti per l’interessato nel contesto della sua specifica richiesta.

Per implementare questi approcci, al fine di fornire la portabilità dei dati, sono state previste varie metodologie:

- L’utilizzo di messaggistica sicura;

- L'utilizzo di un server SFTP;
- L'utilizzo di una WebAPI;
- L'utilizzo di un WebPortal sicuro.

Come previsto dal Regolamento UE 2016/679, ***DOMUSMEDIA.*** fornisce i dati personali portabili in un formato che ne consenta il riutilizzo.

8.2 GESTIONE DEI RISCHI PRIVACY

DOMUSMEDIA. effettua la valutazione del rischio relativo al trattamento dei dati personali a intervalli regolari (almeno una volta l'anno) o quando si verificano cambiamenti significativi (pianificati o meno). Sono presi in considerazione i criteri stabiliti al § 6.1 del presente Manuale e i risultati di tali valutazioni sono conservati come informazioni documentate**,** utilizzando il **Mod_GRP "Gestione dei Rischi Privacy"**.

8.3 GESTIONE DELLA SICUREZZA DEI DATI PERSONALI

DOMUSMEDIA., in quanto Titolare del trattamento, attua misure tecniche ed organizzative adeguate a garantire, ed essere in grado di dimostrare, che il trattamento dei dati venga effettuato in modo conforme al Regolamento EU 2016/679.

In tal modo, il Titolare del trattamento dimostra:

- di essersi dotato di regole proprie in linea con i requisiti definiti nel Regolamento EU 2016/679;
- di attuarle e averne il controllo;
- di essere in grado di motivare le scelte effettuate.

Tendendo conto del contesto, delle finalità del trattamento, dei rischi per i diritti e le libertà delle persone fisiche e delle opzioni di trattamento selezionate, il Titolare e/o il Responsabile del trattamento mettono in atto misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio.

Le misure tecniche ed organizzative comprendono:

- la pseudonimizzazione e la cifratura dei dati personali;
- procedure per garantire la disponibilità delle informazioni;
- procedure per la gestione dei dati personali in attuazione delle misure per la sicurezza fisica e logica;
- politiche e procedure per il trasferimento delle informazioni e dei dati personali;
- procedure operative per il backup, la raccolta di log e monitoraggio, la sicurezza della rete, ecc;
- procedure per la gestione delle violazioni della privacy (data breach);

9 VALUTAZIONE DELLE PRESTAZIONI

9.1 ANALISI E MIGLIORAMENTO

DOMUSMEDIA. valuta costantemente l'efficacia del MP avendo determinato:

- cosa è necessario monitorare e misurare e i metodi per assicurare risultati validi;
- quando il monitoraggio e le misurazioni devono essere effettuati e chi deve farlo;
- chi deve analizzare e valutare questi risultati e quando deve farlo.

9.2 AUDIT INTERNO

DOMUSMEDIA. conduce ad intervalli pianificati audit interni per determinare se il MP:

- è conforme ai requisiti della norma e a quanto stabilito;
- è efficacemente attuato e mantenuto.

L'analisi dei risultati di tali verifiche permette di adottare opportune azioni correttive e di miglioramento, in grado di ridurre l'esposizione ai rischi connessi al trattamento dei dati personali.

Tutti i risultati emersi vengono registrati e mantenuti. I responsabili delle funzioni sottoposte ad audit assicurano che ogni azione correttiva, necessaria per eliminare le NC rilevate e le loro cause, venga implementata senza indebito ritardo. Le attività successive vengono comunque riverificate.

9.3 RIESAME

Il Titolare e/o il Responsabile del trattamento, ad intervalli pianificati, effettuano un riesame sulla gestione e la sicurezza dei trattamenti dei dati personali, prendendo in considerazione:

- i risultati della valutazione del rischio, della valutazione degli impatti privacy (DPIA) e lo stato di attuazione del "Piano delle Misure di Controllo";
- i cambiamenti dei fattori esterni e interni, degli stakeholder o dei trattamenti effettuati che hanno impatti sulla sicurezza dei dati;
- lo stato delle azioni derivanti dai precedenti riesami;
- eventuali feedback delle parti interessate;
- le opportunità per il miglioramento continuo.

Gli elementi in uscita dal riesame comprendono sia le decisioni prese a seguito della valutazione del rischio e dell'eventuale valutazione degli impatti, sia la valutazione delle opportunità per il miglioramento della privacy.

10 MIGLIORAMENTO

DOMUSMEDIA. individua le opportunità di miglioramento e attua opportune azioni al fine di soddisfare i requisiti definiti dal presente documento e dal Regolamento EU 2016/679 e di migliorare le prestazioni e l'efficacia del MP.

10.1 NON CONFORMITÀ AL SISTEMA E AZIONI CORRETTIVE

DOMUSMEDIA. intraprende opportune azioni al fine di eliminare le cause delle NC e il loro ripetersi. Le AC sono appropriate agli effetti delle NC riscontrate.

Le NC riscontrabili nell'ambito della tutela dei dati personali possono derivare dal mancato adempimento dei principi legati al trattamento dei dati personali: liceità, correttezza, trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza, responsabilizzazione (§ 5.2.1).

10.2 MIGLIORAMENTO CONTINUO

DOMUSMEDIA. si impegna a migliorare in continuo l'efficacia del suo MP, utilizzando i risultati degli audit, l'analisi dei dati, le AC e i Riesami della Direzione.