Istituto Comprensivo di Crespellano

MANUALE PER LA PROTEZIONE DEI DATI PERSONALI REGOLAMENTO UE 679/2016 (GDPR)

Con riferimento ai principi dello standard BS 10012:2017
e della norma UNI EN ISO 27001:2014

☐	COPIA CONTROLLATA n° _____	CONSEGNATA A: NOME: _____ COGNOME: _____
☐	COPIA INFORMATIVA	CONSEGNATA A: NOME: _____ COGNOME: _____

Note:
Questo manuale è di proprietà dell'I.C. di Crespellano
Ogni divulgazione e/o riproduzione e/o cessione di contenuti a terzi deve essere autorizzata dalla società stessa.

N°	MOTIVAZIONE	DATA
00	EMISSIONE DEL MANUALE	24.08.18

INTRODUZIONE

PRESENTAZIONE			
RAGIONE SOCIALE	Istituto Comprensivo di Crespellano		
SEDE LEGALE/OPERATIVA	Via IV Novembre, 23 - 40053 Crespellano (BO)		
TEL	0516722325	*FAX*	051964154
E-MAIL	boic862002@istruzione.it	*P.IVA*	91235100376
SITO WEB	https://iccrespellano.gov.it/	*REFERENTE*	DS – Adriano Rovinazzi

CAPITOLO 1

SCOPO

Quanto descritto nel presente documento si applica a tutta l'organizzazione.

Tali prescrizioni sono approvate e, pertanto, rese obbligatorie a tutto il personale, da parte della Direzione che sottoscrive il presente documento e le sue successive modifiche.

CAPITOLO 2

RIFERIMENTI NORMATIVI

Regolamento Ue 679/2016 – GDPR (General Data Protection Regulation).

Per la redazione del Sistema si fa riferimento ai principi contenuti ne:

- BS 10012:2017 Data Protection - Sistemi di gestione per la sicurezza delle informazioni
- ISO 27001:2014 Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni

Per l'implementazione del Sistema sono state consultate anche le norme:

- GDPR – General Data Protection Regulation – Regolamento Ue 2016/679 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)
- ISO/IEC 29134 - Information technology — Security techniques — Guidelines for privacy impact assessment
- ISO/IEC 27000, Information security management systems — Overview and vocabulary
- ISO/IEC 27001, Information security management systems — Requirements —
- ISO/IEC 27002, Code of practice for information security controls —
- ISO/IEC 27003, Information security management system implementation guidance

CAPITOLO 3

TERMINI E DEFINIZIONI

Nel presente Manuale si applicano i termini e le definizioni fornite dalle norme di riferimento.

DEFINIZIONI DI INTERESSE

Definizioni da ISO 9000 - 27000

Alta direzione **Vertice dell'organizzazione**	Persona o gruppo di persone che, dal livello più elevato di un'organizzazione, la guidano e controllano.
Azione correttiva	Azione per eliminare la causa di una non conformità rilevata, o di altre situazioni indesiderabili rilevate.
Cliente	Organizzazione o persona che riceve un prodotto/servizio.
Correzione	Azione per eliminare una non conformità rilevata.
Documento	Informazioni con il loro mezzo di supporto.
Evidenza oggettiva	Dati che supportano l'esistenza o la veridicità di qualcosa.
Fornitore	Organizzazione o persona che fornisce un prodotto.
Ispezione / controllo / collaudo	Valutazione della conformità mediante osservazioni e giudizi, associati, quando opportuno, a misurazioni, prove e verifiche.
Miglioramento continuo	Attività ricorrente mirata ad accrescere la capacità di soddisfare i requisiti.
Non Conformità	Mancato soddisfacimento di un requisito.
Organizzazione	Insieme di persone e di mezzi con definite responsabilità, autorità ed interrelazioni.
Procedura	Modo specificato per svolgere un'attività o un processo.
Processo	Insieme di attività, correlate o interagenti, che trasformano elementi in entrata in elementi in uscita.
Prodotto	Risultato di un processo.
Progettazione e sviluppo	Insieme di processi che trasforma requisiti in caratteristiche specificate o nella specifica di un prodotto, di un processo o di un sistema.
Registrazione	Documento che riporta i risultati ottenuti o fornisce evidenza delle attività svolte.
Requisito	Esigenza o aspettativa che può essere espressa, generalmente implicita o cogente.
Riesame	Attività effettuata per riscontrare l'idoneità, l'adeguatezza, e l'efficacia di qualcosa per il conseguimento degli obiettivi stabiliti.
Rintracciabilità	Capacità di risalire alla storia, all'utilizzazione o all'ubicazione di ciò che si sta considerando.
Specifica	Documento che stabilisce i requisiti.
Struttura organizzativa	Articolazione di responsabilità, autorità e interrelazioni tra persone.

Validazione	Conferma, sostenuta da evidenze oggettive, che i requisiti relativi ad una specifica utilizzazione od applicazione prevista sono stati soddisfatti.
Valutatore	Persona che ha la competenza per effettuare una verifica ispettiva.
Verifica	Conferma, sostenuta da evidenze oggettive, del soddisfacimento di requisiti specificati.
Audit	Processo sistematico, indipendente e documentato per ottenere evidenze delle verifiche ispettive e valutarle con obiettività, al fine di stabilire in quale misura i criteri della verifica ispettiva siano stati soddisfatti.

Definizioni tratte dal Regolamento Ue 2016/679 - GDPR

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

Destinatario	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;
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;
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;
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;
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 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 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;
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;
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;

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;
Gruppo imprenditoriale	un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;
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; NDR: In Italia l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.
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;
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;
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;
Il 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;
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.

Relativamente alle funzioni vengono utilizzate le seguenti sigle:

DS/TT	= Dirigente Scolastico/Titolare del Trattamento
RSG	= Responsabile del sistema di gestione
DPO	= Responsabile della Protezione dei dati
IT/RSI	= Responsabile informatico – Responsabile della Sicurezza delle Informazioni
RT	= Responsabile del Trattamento
AT/I	= Addetto al Trattamento/ Incaricati

CAPITOLO 4

CONTESTO DELL'ORGANIZZAZIONE

4.1 SISTEMA DI GESTIONE

4.1.1 Requisiti Generali

La nostra organizzazione ha determinato:

- i processi necessari per il sistema di gestione e la loro applicazione;
- gli input necessari e gli output attesi da ciascun processo;
- la sequenza e l'interazione di questi processi;
- i rischi per la conformità della sicurezza delle informazioni;
- le risorse necessarie, assicurandone la disponibilità;

ha inoltre stabilito criteri, metodi, misure, e relativi indicatori di performance necessari per garantire il funzionamento, il controllo della loro efficacia e il miglioramento continuo; poi ha assegnato le responsabilità e le autorità per i processi.

CAPITOLO 5

LEADERSHIP

5.1 L'IMPEGNO DELLA DIREZIONE

La Direzione assicura la messa in atto, l'applicazione ed il miglioramento del sistema di gestione prescelto.
Si assume l'onere di manifestare detta scelta a tutte le funzioni dell'organizzazione curando che ognuna di queste sia informata e formata rispetto al sistema prescelto.
A questo fine:

- ⇒ Definisce le politiche di sicurezza delle informazioni dell'impresa;
- ⇒ Definisce gli obiettivi e si assicura che vengano adeguatamente diffusi;
- ⇒ Garantisce l'integrazione dei requisiti del Sistema di Gestione all'interno dei processi centrali dell'organizzazione;
- ⇒ Effettua i riesami almeno con cadenza annuale e ogni qualvolta sia reso necessario dal manifestarsi di problemi di grossa entità o che lo si ritenga opportuno;
- ⇒ Assicura la disponibilità di risorse umane, organizzative ed economiche per la messa in atto, l'applicazione ed il miglioramento continuo del sistema;
- ⇒ Comunica l'importanza di un Sistema di Gestione per la sicurezza delle informazione efficace e l'importanza di conformarsi ai suoi requisiti;
- ⇒ Si occupa di controllare con regolarità ed almeno una volta all'anno la conformità ed adeguatezza degli assets;
- ⇒ Definisce i criteri per il livello di rischio;
- ⇒ Effettua test ed esercitazioni per verificare la conformità ed adeguatezza del sistema.

5.2 POLITICA DELL'ORGANIZZAZIONE

Per rendere partecipi tutti i dipendenti e collaboratori degli **obiettivi** e dei **traguardi** che l'organizzazione si è posta e per indirizzare le attività per ciò che riguarda la protezione dei dati personali, la Nostra organizzazione ha definito il suo principale documento rappresentato dalla **Politica Protezione dei Dati Personali,** che deve contenere almeno:

a) **gli obiettivi relativi alla protezione dei dati personali;**

b) **l'impegno a raggiungere gli obiettivi;**

c) **l'impegno al miglioramento;**

d) **l'impegno al rispetto normativo ed ai requisiti applicabili;**

e) **il focus sui i clienti in materia di sicurezza delle informazioni;**

f) **la responsabilità nei confronti del personale e dei collaboratori;**

Tale politica deve essere adeguata alla natura e alla dimensione dell'organizzazione e deve essere periodicamente revisionata.

Nella nostra organizzazione **la Politica è definita ed approvata dall'Alta Direzione** che ne assicura la conformità ai requisiti delle norme di riferimento, ossia che:

a) sia **appropriata** agli scopi dell'organizzazione e coerente con le altre politiche dell'organizzazione;
b) sia **attinente** agli obiettivi dell'organizzazione;
c) sia **adeguata** alle aspettative e alle esigenze dei clienti e delle altre parti interessate;
d) sia **adeguata** alla natura e all'entità dei rischi per la sicurezza delle informazioni dell'organizzazione;
e) **comprenda** l'impegno al continuo miglioramento della gestione e delle prestazioni del Sistema;
f) **comprenda** l'impegno al rispetto della normativa cogente e degli altri requisiti che l'organizzazione ha sottoscritto;
g) sia **documentata**, implementata e mantenuta attiva;
h) sia **comunicata** e compresa a tutti i livelli dell'organizzazione, a tutte le persone che lavorano sotto il controllo dell'organizzazione o per conto di essa, con l'intento di renderli consapevoli dei loro obblighi individuali;
i) sia **disponibile** alle parti interessate;
j) sia **rivista** periodicamente per garantire che rimanga appropriata e coerente con l'organizzazione.

Affinché la **Politica Protezione dei Dati** sia comunicata alle persone che lavorano sotto il controllo dell'organizzazione o per conto di essa, al fine di rendere partecipi tutti degli obiettivi e dei traguardi che l'organizzazione si è posta il documento:
- viene esposto nella bacheca della sede dell'organizzazione;
- viene trasmesso ai fornitori critici.

Per quanto riguarda, invece, le parti interessate, l'organizzazione rende disponibile la propria Politica attraverso comunicazione apposita.

La **Politica Protezione dei Dati** indica l'impegno dell'organizzazione per la conformità con i requisiti di protezione dei dati

e con le buone pratiche, tra cui:

1) il trattamento delle informazioni personali solo ove ciò sia strettamente necessario ai fini di legge e regolamentari, o per scopi legittimi organizzativa;
2) il trattamento solo dei dati personali minimi richiesti per tali scopi;
3) fornire informazioni chiare alle persone fisiche (minori compresi) su come le loro informazioni personali possono essere utilizzate e da chi (vedi 8.2.1);
4) assicurare garanzie speciali per raccogliere dati direttamente da minori;
5) l'elaborazione solo delle informazioni personali pertinenti e adeguate;
6) il trattamento corretto e lecito delle informazioni personali;
7) il mantenimento di un inventario documentato delle categorie di dati personali elaborati dall'organizzazione (Vedi **M 6.1.1 REGISTRO DELLE ATTIVITA' DI TRATTAMENTO**)
8) la conservazione di informazioni personali accurate e, quando necessario, up-to-date;
9) conservare le informazioni personali solo per il tempo strettamente necessario per motivi legali o regolamentari o per scopi organizzativi legittimi e garantire lo smaltimento tempestivo e adeguato;
10) il rispetto dei diritti delle persone fisiche in relazione alle loro informazioni personali;
11) mantenere tutte le informazioni personali sicure;
12) il trasferimento di dati personali al di fuori dal territorio nazionale solo in circostanze in cui può essere adeguatamente protetto;
13) se del caso, la strategia per trattare con le autorità di regolamentazione in tutta l'UE, dove le merci e / o servizi sono offerti alle persone fisiche residenti in altri paesi dell'UE;
14) l'applicazione delle varie esenzioni consentite dalla legislazione sulla protezione dei dati;
15) sviluppare e attuare un Sistema di Gestione delle informazioni personale per implementare la **Politica** stessa;
16) se del caso, l'identificazione delle parti interessate interne ed esterne e il grado in cui essi sono coinvolti nel governo del Sistema di Gestione dell'organizzazione;
17) l'individuazione dei lavoratori aventi una funzione specifica e la responsabilità per il Sistema di Gestione;
18) tenere registri di trattamento dei dati personali (Vedi **M 6.1.1 REGISTRO DELLE ATTIVITA' DI TRATTAMENTO**).

La **Politica** copre l'intera organizzazione e non una parte identificata dell'organizzazione.

Documenti applicabili

M 6.1.1 Registro delle attività di trattamento
Allegato al MSG – Politica Protezione dei Dati Personali
Politiche Operative

5.3 RUOLO NELL'ORGANIZZAZIONE, RESPONSABILITÀ E AUTORITÀ

La direzione assicura che le responsabilità e le autorità siano definite e comunicate nell'ambito dell'organizzazione.

La direzione individua un soggetto che, **indipendentemente da altre responsabilità**, deve avere l'autorità per:

- assicurare che i processi necessari per il sistema di gestione dell'organizzazione siano stabiliti, attuati e tenuti aggiornati;

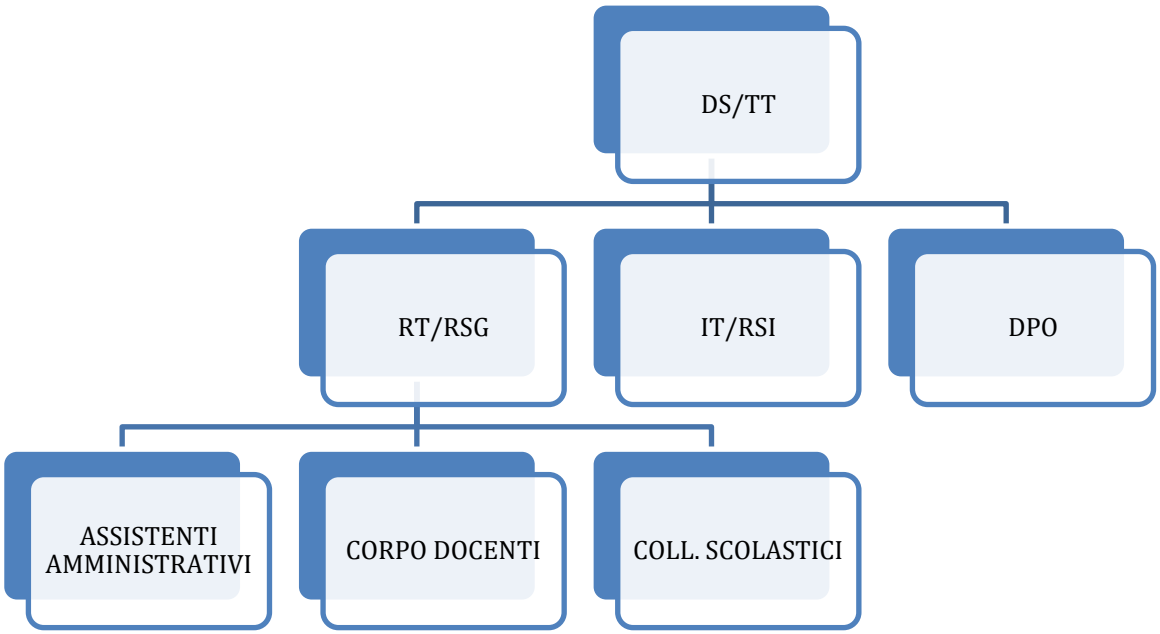
- **riferisce** all'alta direzione sulle prestazioni del sistema di gestione dell'organizzazione e su ogni esigenza di miglioramento;
- **assicurare** la promozione della consapevolezza dei requisiti del cliente nell'ambito di tutta l'organizzazione.

Sono definiti uno o più lavoratori adeguatamente qualificati o con esperienza per assumersi la responsabilità per la conformità QUOTIDIANA dell'organizzazione con la **Politica Protezione dei Dati Personali.**

(Il dirigente scolastico e il lavoratore responsabile della conformità quotidiana potrebbe essere la stessa persona)

La responsabilità della direzione può comprendere collegamenti con parti esterne su argomenti relativi al sistema di gestione per la sicurezza delle informazioni.

La nostra struttura organizzativa è illustrata nell'organigramma di seguito riportato e nel mansionario allegato al presente manuale.



La Direzione provvede ad informare i propri dipendenti e collaboratori circa la struttura organizzativa mediante:

- momenti di riunione verbalizzati;
- esposizione dell'organigramma nominativo nella bacheca dell'organizzazione;
- incontri personali di informazione.

5.4 INCORPORARE IL SISTEMA DI GESTIONE NELLA CULTURA DELL'ORGANIZZAZIONE

Per garantire che la gestione delle informazioni personali diventi una parte dei valori fondamentali dell'organizzazione e la gestione efficace, l'organizzazione provvede a:

a) Elevare, migliorare, testare e mantenere la **consapevolezza** del SG attraverso una formazione continua e un programma di sensibilizzazione per i lavoratori;
b) **Stabilire** un processo per valutare l'efficacia del metodo di sensibilizzazione del SG (mini test di fine corso formazione);

c) **Comunicare** ai lavoratori l'importanza di:
   1) raggiungere gli obiettivi del SG;
   2) essere conformi alla **Politica Protezione dei Dati Personali**;
   3) miglioramento continuo della **Politica Protezione dei Dati Personali**;
d) **Assicurare** che i lavoratori siano consapevoli di come loro stessi contribuiscono al raggiungimento degli obiettivi del Sistema di Gestione dell'organizzazione e le conseguenze di non conformità; e
e) **Conservare** le informazioni documentate di attività di formazione e di sensibilizzazione e la sua efficacia.

Documenti applicabili

P 5.1.1 Struttura e organizzazione del sistema
M 5.1.1 Organigramma
M 5.1.1 Mansionario
Allegato al MSG – Politica Protezione dei Dati Personali

CAPITOLO 6

PIANIFICAZIONE

6.1.1 ANALISI E VALUTAZIONE DI RISCHI E OPPORTUNITÀ

Nella fase di pianificazione del sistema sono stati presi in considerazione e determinati i rischi e le opportunità al fine di rispondere ai requisiti del Regolamento Ue 679/2016 – GDPR.

6.1.2 INVENTARIO DI DATI E FLUSSO DI DATI[1]

L'organizzazione ha definito una procedura di analisi dell'inventario dei dati e del flusso dati che:
1) stabilisce e mantiene un'analisi dell'inventario dei dati e del flusso dati che include l'identificazione di:
   a. processi chiave che utilizzano dati personali;
   b. fonti di dati personali;
   c. categorie di dati trattati, compresa l'individuazione di informazioni personali ad alto rischio;
   d. scopi per i quali i dati personali possono essere usati, inclusi scopi secondari successivi che vanno oltre lo scopo iniziale raccolto;
   e. potenziali destinatari delle informazioni personali, tra cui la divulgazione di informazioni personali a terzi, i responsabili di trattamento dei dati e il trasferimento ai fornitori;
   f. i flussi di dati personali di cui organizzazione agisce come titolare o come responsabile;

[1] *L'articolo 30 impone i titolari del trattamento per mantenere un **registro delle attività** di lavorazione per dimostrare il rispetto della GDPR. Esso specifica le informazioni che devono essere fornite nel record.*
*L'organizzazione dovrebbe prendere in considerazione il **mantenimento** di up-to-date informazioni documentate relative ai dati inventario e identificazione flusso di dati.*
L'organizzazione dovrebbe considerare se mantenere versioni superata della politica di conservazione dei dati e delle informazioni di inventario in conformità con il loro programma di conservazione.

g. i sistemi chiave e archiviazione di informazioni personali;
h. i flussi di dati personali in cui le informazioni personali vengono trasferite oltre i confini nazionali o soggetti a diverse leggi, regolamenti, norme o quadro;
i. requisiti di conservazione e smaltimento di dati personali, nonché i criteri per tali esigenze; e

2) assicura che ripetuti inventari di dati producono risultati coerenti, validi e confrontabili.

6.1.3 BASI LEGALI

6.1.3.1 Trattamento

L'organizzazione ha identificato, definito e documentato la base giuridica per il trattamento di tutte le informazioni personali, che deve essere selezionato da uno o più dei seguenti elementi:

- Il consenso[2] della persona fisica adeguato e inequivocabile in riferimento a scopi specifici;
- Sia necessario per l'esecuzione di un contratto in cui la persona fisica è una delle parti, o ad adottare misure per stipulare un contratto;
- Sia necessario per adempiere un obbligo legale al quale l'organizzazione è soggetta;
- Sia necessario per tutelare gli interessi vitali della persona fisica;
- Sia necessario per svolgere un compito di interesse pubblico o l'esercizio di pubblici poteri dell'organizzazione;
- Sia necessario per gli interessi legittimi[3] del titolare o di un terzo, a meno che a tali interessi prevalgano gli interessi o i diritti fondamentali e le libertà della persona fisica (non applicabile al trattamento effettuato da organismi pubblici nell'esercizio delle i loro compiti).

Documenti applicabili
M 6.1.1 Registro delle attività di trattamento

6.1.3.2 Categorie particolari

L'organizzazione ha individuato, definito e documentato, una base giuridica aggiuntiva per il trattamento dei dati personali, qualora si elaborino categorie particolari di dati personali.
Essa viene selezionata tra una o più delle opzioni seguenti:

- Il consenso esplicito della persona fisica per scopi specifici;
- Il trattamento sia necessario per diritti o obblighi di lavoro;
- Il trattamento sia necessario per tutelare gli interessi vitali della persona fisica;
- Il trattamento sia necessario per le attività legittime di una fondazione, associazione, o qualsiasi altra organizzazione senza scopo di lucro per uno scopo politico, filosofica, religioso o sindacale, date garanzie adeguate;
- Le informazioni deliberatamente rese pubbliche dalla persona fisica;
- Il trattamento sia necessario per costituire, esercitare o difendere un diritto per via giudiziaria;
- Il trattamento sia necessario per motivi di interesse pubblico;

[2] Si richiama l'attenzione l'articolo 7 del GDPR per dare e ritirare il consenso di una persona fisica.
[3] Per ulteriori dettagli di "interesse legittimo", vedi il considerando 47 della GDPR; disposizioni supplementari per l'elaborazione del tipo introdotto da leggi nazionali. Si richiama inoltre l'attenzione l'articolo 5 1 (b) del GDPR per la documentazione degli interessi legittimi dell'organizzazione

- Il trattamento sia necessario per la medicina preventiva e del lavoro, la valutazione della capacità di lavoro di un dipendente, diagnosi medica, la fornitura di assistenza sanitaria o di sistemi e servizi sociali;
- Il trattamento sia necessario per motivi di salute pubblica o di segreto professionale;
- Disposizioni supplementari per le elaborazioni di questo tipo introdotte da leggi nazionali in materia di trattamento di dati genetici, biometrici, o concernenti la salute della persona fisica.

6.1.4 VALUTAZIONE DEL RISCHIO

6.1.4.1 VALUTAZIONE DEL RISCHIO DELLA SICUREZZA DELLE INFORMAZIONI SULLA PROTEZIONE DEI DATI (DPIA – VALUTAZIONE D'IMPATTO)

L'organizzazione ha definito la procedura per implementare una *Valutazione D'impatto sulla Protezione dei Dati (Pia)* relativa al trattamento dei dati personali che:

a) **stabilisce** e mantiene aggiornati i criteri di rischio privacy, tra cui:
   - i criteri di accettazione del rischio;
   - i criteri per l'esecuzione di valutazione del rischio privacy (includendo se è stato assegnato esternamente); e
   - l'applicazione dei principi di protezione dei dati sui flussi di dati al fine di identificare i rischi privacy.

b) **garantisce** che le ripetute valutazioni d'impatto dei rischi privacy siano coerenti, valide e comparabili;

c) **individua** i rischi di protezione dei dati associati al processo di valutazione dei rischi privacy per identificare i rischi associati a:
   - leggi rilevanti, standard e frame quark concernenti la privacy;
   - l'impatto sui diritti e le libertà delle persone fisiche[4];
   - qualsiasi danno fisico, materiale o morale a persone fisiche[5]; e
   - l'impatto sull'organizzazione (tra cui, ma non solo reputazione, interventi normativi, perdite finanziarie, ecc);

d) **identifica** le informazioni personali ad alto rischio e i relativi processi ad alto rischio;

e) **identifica** i *risk owners*;

f) **analizza** i rischi privacy che:
   1) valutano le potenziali conseguenze che deriverebbero se i rischi per la privacy individuati nella valutazione del rischio dovessero concretizzarsi;
   2) valutano la probabilità realistica del verificarsi dei rischi identificati nella valutazione dei rischi privacy;
   3) determinano il livello di rischio.

---

[4] *Le persone fisiche vulnerabili sono coloro che, a causa della loro situazione personale, sono particolarmente soggetti a danno, in particolare quando un responsabile del trattamento non agisce con adeguati livelli di cura.*

[5] *Danno morale, fisico o non-materiale si verifica per esempio:*

• quando il trattamento potrebbe dare luogo a discriminazioni, il furto di identità o la frode, perdite finanziarie, danni alla reputazione, perdita di riservatezza delle informazioni personali protette dal segreto professionale, l'inversione non autorizzata di de-identificazione, o qualsiasi altro significativo svantaggio economico o sociale;

• le persone fisiche possono essere private dei loro diritti e delle libertà o impedito di esercitare il controllo sulle loro informazioni personali;

• qualora particolari categorie di informazioni o di dati personali relativi alle condanne penali e reati o misure di sicurezza connesse vengono elaborati;

• qualora gli aspetti personali vengono valutati, come ad esempio la profilazione;

• quando le informazioni personali delle persone fisiche vulnerabili, in particolare dei minori viene elaborato; o

• quando il trattamento comporta una grande quantità di informazioni personali e colpisce un gran numero di persone interessate.

g) **valuta** i rischi privacy, includendo:
   1) il confronto dei risultati delle analisi dei rischi con i criteri di rischio; e
   2) il dare priorità ai rischi analizzati per il trattamento del rischio.

L'organizzazione conserva informazioni documentate concernenti l'impatto della privacy e il processo di valutazione del rischio in **M 6.1.1 DPIA – Valutazione d'impatto**.[6]

6.1.5 TRATTAMENTO DEL RISCHIO PRIVACY

Il processo di valutazione del rischio privacy definito dall'organizzazione:

a) Seleziona opzioni di trattamento appropriato per il rischio privacy, tenendo conto dei risultati della valutazione dei rischi;
b) Determina tutti i controlli necessari per attuare l'opzione di trattamento prescelto per i(l) rischi(o) privacy;[7]
c) Formula un piano di trattamento per il rischio privacy; e
d) Ottiene l'approvazione del piano di trattamento per il rischio privacy dai *risk owners* e l'accettazione dei rischi privacy residui.

L'organizzazione conserva informazioni documentate concernenti processo di valutazione del rischio.[8]

Il controllo potrebbe includere, ad esempio, de-identificazione, pseudonominazione, minimizzazione dei dati, ridurre la portata e finalità del trattamento, periodo di archiviazione, accessibilità o misure tecniche e organizzative di sicurezza delle informazioni, come ad esempio quelli individuati nella BS EN ISO / IEC 27001

6.1.6 CONSULTAZIONE E AUTORIZZAZIONE PREVENTIVA RELATIVA ALLA PROTEZIONE DEI DATI PERSONALI

Qualora i rischi per la persona fisica derivati dal trattamento dei dati personali siano identificati dalla Valutazione d'impatto della protezione dei dati (PIA) di alto livello[9], e non possano essere mitigati, l'organizzazione ricerca la consultazione e l'autorizzazione preventiva da parte dell'autorità di vigilanza.

L'organizzazione conserva informazioni documentate sui criteri e i processi d'interazione con gli organi di controllo appropriati in materia di consultazione e di autorizzazione preventiva.

6.1.7 PRIVACY BY DESIGN E PRIVACY BY DEFAULT

---

[6] *Un esempio di un processo di valutazione del rischio (come applicato ai record) è incluso nel 18128 PD ISO /TR: 2014 Informazione e documentazione - Valutazione del rischio per i processi e sistemi di registrazione.*

[7] *Le imprese devono attuare misure tecniche ed organizzative per garantire ed essere in grado di dimostrare che il trattamento viene effettuato in conformità con la legge, quindi hanno bisogno di progettare i controlli come appropriato, o identificarli da qualsiasi fonte, compresi i codici di Autodisciplina emanati dalle autorità di regolamentazione competenti e le autorità di vigilanza.*

[8] *La valutazione del rischio privacy e processo di trattamento in questo British Standard allinearsi con i principi e le linee guida generali fornite nella BS ISO 31000.*

[9] *L'elaborazione ad alto rischio include estese attività di profiling, o l'assenza di controlli adottati dall'organizzazione per mitigare i rischi per la persona fisica. Si veda l'articolo (36) 3 del GDPR*

Nel progettare o apportare modifiche significative a:

a) Sistemi finalizzati all'utilizzo interno all'organizzazione o dagli elaboratori di dati; o
b) Prodotti e servizi finalizzati all'uso da parte di individui o di altre organizzazioni,

l'organizzazione assicura che il trattamento dei dati personali da parte di tali sistemi, prodotti o servizi:

1) venga minimizzato by default;
2) utilizzi informazioni de-identificate ove possibile; e
3) sia trasparente per quanto riguarda la funzione e l'elaborazione dei dati personali.

Ciò è realizzato seguendo azioni organizzative e tecniche adeguate:

i. disposte in relazione ai rischi individuati (vedi 6.1.4);
ii. che garantiscono controlli della privacy individuati (vedi 6.1.5) siano implementati a seconda dei casi protezione dei dati personali; e
iii. che mantengono appropriate informazioni documentate concernenti le attività e i risultati della privacy by design.

6.2 OBIETTIVI DEL SISTEMA DI GESTIONI E LA PIANIFICAZIONE PER LA LORO REALIZZAZIONE

L'organizzazione ha definito gli obiettivi in relazione alle pertinenti funzioni e livelli. Gli obiettivi del SG devono:

a) essere coerenti con la Politica di protezione dei dati personali;

b) essere misurabili (se possibile);

c) tener conto dei requisiti di privacy e dei risultati di valutazione dei rischi e dei trattamenti di rischio;

d) essere monitorati;

e) essere comunicati;

c) essere opportunamente aggiornati.

L'organizzazione conserva informazioni documentate relative ai propri obiettivi.

Nel pianificare come conseguire i propri obiettivi per la sicurezza delle informazioni, l'organizzazione deve determinare:

- cosa sarà fatto;
- quali risorse saranno necessarie;
- chi ne sarà responsabile;
- quando sarà completato; e
- come saranno valutati i risultati.

Documenti applicabili:
M 6.1.1 Valutazione d'Impatto – DPIA

CAPITOLO 7

STRUTTURA DELL'ORGANIZZAZIONE

7.1 RISORSE UMANE E INFRASTRUTTURALI

La nostra organizzazione individua e rende disponibili le risorse umane, mezzi e strumenti organizzativi con la finalità di attuare e tenere aggiornato il sistema di gestione e migliorare in modo continuo la sua efficacia.

7.2 GESTIONE DELLE COMPETENZE

La nostra organizzazione si assicura che il personale, inclusi i lavoratori temporanei, che esegue attività che hanno influenza sul presente sistema abbia la necessaria competenza sulla base di un idoneo grado di istruzione, addestramento, abilità ed esperienza.
La selezione e la gestione del personale avviene con le modalità descritte in **P 7.1.1 "Gestione delle Risorse".** Nella medesima procedura viene previsto il monitoraggio della soddisfazione del personale al fine di migliorarne la fidelizzazione e il senso di appartenenza all'organizzazione.

La nostra organizzazione considera la formazione del personale dell'organizzazione un aspetto di primaria importanza, ai fini di assicurare il raggiungimento degli obiettivi di sicurezza e protezione dei dati personali.

A tal fine si riconosce che per ottenere un'efficace ed efficiente applicazione del Sistema di Gestione, è necessario che ogni collaboratore arrivi a possedere:

- **autosufficienza** ed esperienza nello svolgimento della propria funzione;
- **conoscenza** della importanza della conformità del proprio operato rispetto alla politica dell'organizzazione, alle procedure, ai requisiti del Sistema e all'immagine che l'organizzazione ha verso l'esterno;
- **consapevolezza** degli eventuali effetti negativi causati dallo scostamento rispetto a quanto sopra indicato;
- **consapevolezza** del proprio ruolo nei casi in cui si verificano incidenti che determinano la discontinuità operativa.

Per assicurarsi che tutto il personale dell'organizzazione sia in possesso di tali competenze, professionalità e consapevolezza, relativamente al proprio ruolo, pianificando e definendo le modalità di selezione e di formazione del personale.
La formazione può essere per gruppi di persone con necessità omogenee, o individuale, tramite corsi teorici o affiancamento con personale esperto.

L'attuazione della **FORMAZIONE** può essere:

- *interna*: ovvero effettuata da personale interno all'organizzazione, anche avvalendosi dei dipendenti e collaboratori. La scelta del docente/istruttore, della durata del corso/affiancamento spetta, a seconda del tipo di formazione da eseguire, a DS con la collaborazione di RSG.

- *esterna*: ovvero effettuata da personale esterno all'organizzazione, quali ad esempio il Data Protection officer, in sedi interne od esterne con docenti scelti da DS con la collaborazione di RSG.

A seguito di ogni intervento formativo viene verificata l'efficacia dell'addestramento tramite interviste al personale interessato, verifiche ispettive supplementari o valutazione del miglioramento dei processi. Tutti risultati dell'attività formativa vengono registrati.

Documenti applicabili:
P 7.1.1 "Gestione delle Risorse"
P 7.2.1 "Formazione e Addestramento"

7.3 PARTECIPAZIONE, CONSULTAZIONE E CONSAPEVOLEZZA

L'organizzazione stabilisce, fornisce e mantiene attive procedure affinché le persone che lavorano sotto il suo controllo siano consapevoli:

- delle conseguenze, reali e potenziali, delle proprie attività lavorative, del proprio comportamento, e dei benefici derivanti dal miglioramento delle prestazioni personali;
- del proprio ruolo, delle proprie responsabilità e dell'importanza del raggiungimento della conformità alla politica, alle procedure e ai requisiti del Sistema di Gestione, inclusi i requisiti per la preparazione e la risposta alle emergenze;
- delle potenziali conseguenze derivanti da scostamenti dalle specifiche operative.

L'organizzazione assicura, quando è opportuno, la consultazione delle parti esterne interessate su aspetti pertinenti il Sistema di Gestione.

Tutto il personale, inclusi i lavoratori temporanei, deve segnalare malattie infettive rilevanti o compromissioni dello stato di salute.

7.4 GESTIONE DELLA COMUNICAZIONE

L'organizzazione ha definito un piano di comunicazione interna ed esterna che include le informazioni relative a:

COSA COMUNICARE;
QUANDO COMUNICARE;
CON CHI COMUNICARE.

Sono state definite procedure per gestire:

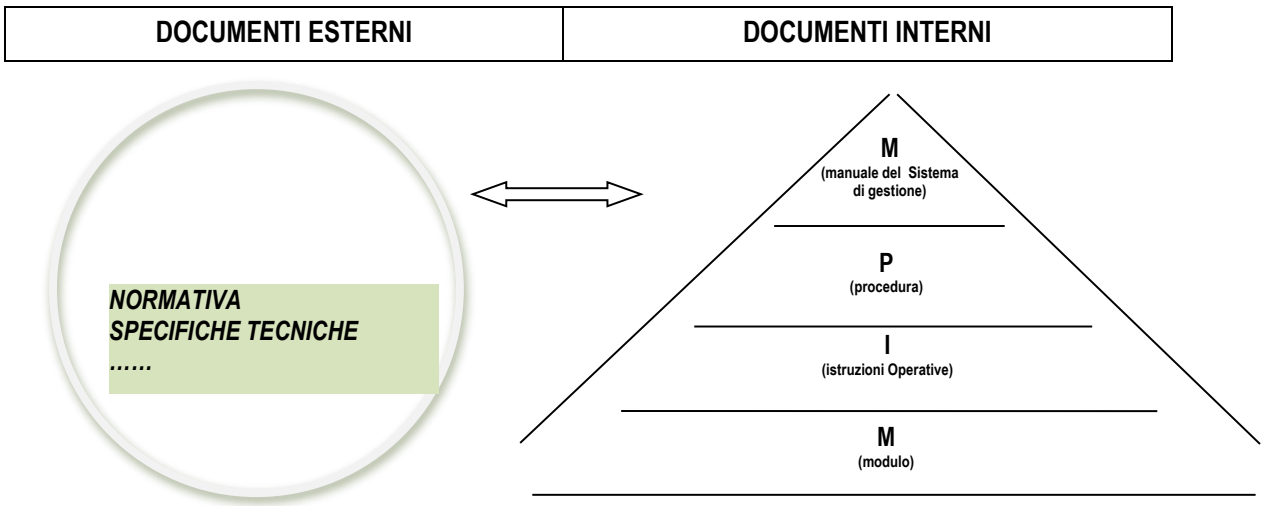
- comunicazioni interne tra le parti interessate ed i lavoratori all'interno dell'organizzazione
- comunicazioni esterne con clienti, partner, fornitori, comunità locali ed altre parti interessate, inclusi i Media
- comunicazioni in ingresso e le risposte
- il coinvolgimento di soggetti anche istituzionali se appropriato

Documenti applicabili:
P 7.2.1 Gestione della Comunicazione

7.5 GESTIONE DELLA DOCUMENTAZIONE

7.5.1 REQUISITI GENERALI

La documentazione del sistema di gestione include tutti i documenti necessari all'organizzazione per assicurare l'efficace funzionamento ed il controllo dei suoi processi. Tale documentazione, che include anche norme ed informazioni di origine esterna, è organizzata secondo il modello di seguito riportato:



7.5.2 DOCUMENTAZIONE E CONTROLLO

Il presente documento costituisce il Manuale del Sistema di Gestione predisposto dall'organizzazione. Il campo di applicazione del sistema di gestione è definito nel 4.3 del presente documento. Le procedure implementate al fine di dare attuazione a quanto definito nei diversi capitoli o paragrafi del presente manuale vengono richiamate nelle sezioni "Documenti applicabili" inserite al termine di capitoli e paragrafi. Nel capitolo 4 del manuale sono descritti i processi del sistema di gestione e ne sono rappresentate anche le loro interazioni.

CAPITOLO 8

CONTROLLO OPERATIVO

8.1 PIANIFICAZIONE E CONTROLLO

L'organizzazione, nella pianificazione delle proprie attività, valuta e controlla i cambiamenti, inclusi quelli non previsti, adottando le opportune correzioni per ridurne gli impatti, qualora necessario, e garantisce che le operatività in outsourcing che influenzano la sicurezza delle informazioni siano mantenute sotto controllo.

8.2 IMPLEMENTAZIONE DEL SISTEMA DI GESTIONE

8.2.1 Nomine Chiave

Obiettivo: garantire che l'organizzazione nomini i lavoratori responsabili appropriati, come specificato nella Politica dell'organizzazione.

8.2.1.1 Titolare del Trattamento – Alta direzione

Un membro dell'Alta direzione deve essere designato come responsabile per la gestione delle informazioni personali all'interno dell'organizzazione al fine di dimostrare il rispetto dei requisiti di protezione dei dati e delle buone pratiche.

8.2.1.2 Responsabile della protezione dei dati (DPO)

Qualora l'organizzazione decida di nominare un DPO sulla base della normativa, della richiesta di un'autorità di controllo o per una strategia di business, nomina un lavoratore qualificato a svolgere questo ruolo.

I dati di contatto del DPO sono segnalati all'autorità di vigilanza competente secondo la modulistica fornita dall'autorità garante.

Il DPO o un lavoratore qualificato garantisce che la Politica sia conforme ai requisiti delle leggi applicabili, dei regolamenti e del business.

Il DPO o un lavoratore qualificato garantisce che l'appropriata valutazione d'impatto sulla privacy e la valutazione dei rischi vengano eseguite ove necessario.

Il DPO o un lavoratore qualificato garantisce che venga effettuata la notifica all'autorità di vigilanza, ove necessario.

L'organizzazione coinvolge il DPO o il lavoratore adeguatamente qualificato in maniera tempestiva in tutte le questioni relative al trattamento dei dati personali.

8.2.1.3 Responsabilità quotidiane per la conformità con la Politica del SG

Uno o più lavoratori adeguatamente qualificati o con esperienza sono designati come responsabili della conformità quotidiana con la politica SG. Tale responsabile può essere designato sia full-time che part-time a seconda delle dimensioni dell'organizzazione e della natura del trattamento dei dati personali.

Se del caso, il lavoratore nominato presenta una relazione al DPO o ad un altro lavoratore qualificato ove necessario per adempiere alle proprie responsabilità.

Il lavoratore nominato avrà le seguenti responsabilità:

a) la responsabilità globale per monitorare il rispetto della **Politica**;

b) lo sviluppo e la revisione della **Politica**;

c) provvedere all'implementazione della **Politica**;

d) gestire la revisione della **Politica**;

e) la formazione e la continua sensibilizzazione come richiesto dalla **Politica**;

f) l'approvazione delle procedure in cui le informazioni personali sono trattate quali:

   1) la gestione e la comunicazione di informazioni sulla privacy ;

   2) la gestione delle richieste provenienti da persone fisiche ;

   3) la raccolta e il trattamento dei dati personali ;

   4) la gestione dei reclami ;

   5) la gestione di violazione della sicurezza; e

   6) outsourcing e off-shoring.

g) di intermediario con i responsabili della gestione dei rischi, dei problemi di sicurezza e delle funzioni di controllo all'interno dell'organizzazione;

h) la fornitura di informazioni, consulenza e orientamento in materia di protezione dei dati;

i) l'interpretazione e l'applicazione delle varie esenzioni applicabili al trattamento dei dati personali;

j) la fornitura di consulenza in relazione ai progetti di condivisione dei dati (inclusi i problemi di sicurezza quando i dati sono fuori sede);

k) garantire che l'organizzazione abbia accesso agli aggiornamenti legislativi e ad un' adeguata assistenza relativa ai requisiti di protezione dei dati, che la **Politica** venga continuamente rivista per conformarsi alle aggiornamenti legislativi; e

l) l'implementazione appropriata delle pratiche relative al trattamento dei dati personali delineata nei codice settoriali applicabili all'organizzazione obbligatori o consultivi.

8.2.1.4 Rappresentanti della Protezione dei dati

Qualora l'organizzazione comprenda più reparti o sistemi che trattano dati personali, l'organizzazione deve determinare se sarebbe opportuno istituire una rete di rappresentanti della protezione dei dati che:

a) rappresentano i reparti o sistemi che sono riconosciuti come ad alto rischio in relazione alla gestione delle informazioni personali; e
b) assistono il lavoratore con i compiti di responsabilità quotidiana per la conformità con la Politica.

8.2.2 identificare e registrare gli usi delle informazioni personali

Obiettivo: garantire che l'organizzazione comprenda le categorie di dati personali da essa trattate e il livello di rischio connesso al trattamento di tali informazioni.

8.2.2.1 inventario

L'organizzazione mantiene un inventario delle categorie di dati personali elaborati. L'inventario documenta inoltre gli scopi per i quali viene utilizzata ogni categoria di dati personali.

L'organizzazione ha documentato il flusso di informazioni personali in tutti processi dell'organizzazione.

Note: vedi allegato **ELENCO PC**

8.2.2.2 informazioni personali ad alto rischio

L'inventario consente l'individuazione esplicita e la documentazione delle categorie ad alto rischio delle informazioni personali elaborate dall'organizzazione.

8.2.3 Valutazione del rischio e del trattamento

L'organizzazione ha implementato un processo per la valutazione del livello[10] di rischio per le persone fisiche associato al trattamento dei dati personali con l'attuazione della PIA (vedi 6.1.4). Tali valutazioni comprendono l'elaborazione intrapresa da altre organizzazioni.

L'organizzazione ha inoltre attuato un piano di trattamento del rischio per gestire i rischi che sono stati identificati dalla valutazione dei rischi, al fine di ridurre la probabilità di una non conformità con la Politica.

Il processo di valutazione dei rischi deve comprende procedure in cui ogni trattamento dei dati personali che potrebbe causare danni e / o disagio alle persone fisiche possa essere sottoposto a revisione dai responsabili per la gestione delle informazioni personali

---

[10] *Categorie ad alto rischio di informazioni personali possono includere:*

a) la categoria particolare dati personali (vedi 3.1.30);
b) il conto bancario personale e altre informazioni finanziarie
c) gli identificatori nazionali, come ad esempio i numeri di assicurazione nazionali;
d) le informazioni personali relative ad adulti e minori vulnerabili;
e) i profili dettagliati delle persone fisiche (compresi i minori); e
f) le trattative sensibili che potrebbero influenzare negativamente le persone fisiche.

il livello di rischio può aumentare qualora venga elaborato un elevato volume di informazioni personali.

8.2.4 Formazione e sensibilizzazione

L'organizzazione assicura che il lavoratore con i compiti di responsabilità quotidiana possa dimostrare la conformità ai requisiti di protezione dei dati e buone pratiche:

- **essendo in grado di dimostrare** la competenza nella comprensione delle esigenze di protezione dei dati e di buone pratiche e di come queste dovrebbero essere attuate all'interno dell'organizzazione, e,
- **rimanga** informato sulle problematiche legate alla gestione dei dati personali, se del caso, attraverso il contatto con enti esterni.

L'organizzazione è in grado di dimostrare che i lavoratori comprendono la loro responsabilità di garantire che le informazioni personali siano protette e trattate secondo le procedure applicabili, tenendo conto dei relativi requisiti di sicurezza.

I lavoratori ricevono una formazione (Vedi **P 7.2.1 Formazione e Addestramento**) per consentire loro di elaborare i dati personali in conformità con le procedure applicabili.

Questa formazione deve essere rilevante per il ruolo che ciascun lavoratore svolge all'interno dell'organizzazione. In particolare si sottolinea l'esigenza dei lavoratori di aderire a procedure di sicurezza delle informazioni applicabili.

8.2.5 Mantenere aggiornato il Sistema di Gestione

Il lavoratore con i compiti di responsabilità quotidiana per la conformità con la Politica ad intervalli pianificati valuta se l'SG consente e continuerà a consentire la dimostrazione della conformità ai requisiti di protezione dei dati e buone pratiche, attuando cambiamenti, ove necessario.

Questa valutazione deve includere la revisione del SG quando si verificano dei cambiamenti nei requisiti e / o nella tecnologia dell'organizzazione.

8.2.6 Trattamento corretto, lecito e trasparente

Obiettivo: garantire che le informazioni personali sono trattati in modo corretto, lecito e trasparente, e per assicurare che i motivi legali per l'elaborazione dei dati personali siano state chiaramente identificate prima dell'inizio del trattamento.

8.2.6.1 Raccolta e trattamento dei dati personali

L'SG provvede, in conformità con quanto descritto sulla base giuridica per l'elaborazione in, che:

a) l'organizzazione elabori i dati personali in modo equo e conforme alla legge;

b) l'organizzazione elabori le informazioni personali solo quando ciò sia giustificato, in linea con i requisiti[11];

c) l'organizzazione elabori le informazioni personali ad alto rischio solo laddove ciò sia necessario per gli scopi dell'organizzazione, in linea con i requisiti;

d) l'organizzazione fornisca alle persone fisiche le informazioni in un formato appropriato, affinché comunichi in modo chiaro:

   1) l'identità dell'organizzazione e dei suoi rappresentanti, se del caso;

   2) gli scopi per cui le informazioni personali possono essere trattate;

[11] *L'articolo 6 della GDPR [1] definisce "Legittimità del trattamento"*

3) gli interessi legittimi dell'organizzazione o il trattamento dove essi sono la base giuridica utilizzata;
4) i tipi di dati personali raccolti (solo quando le informazioni sono raccolte da una fonte diversa dalla persona fisica);
5) l'origine dei dati personali e, se del caso, se provengano da fonti accessibili al pubblico (solo quando le informazioni vengono raccolte da una fonte diversa dalla persona fisica);
6) l'informazione sulla comunicazione di dati personali a soggetti terzi;
7) se le informazioni personali sono trasferite al di fuori del SEE e una spiegazione delle garanzie in essere, e come ottenere una copia di tali garanzie;
8) se l'organizzazione è basata al di fuori dell'UE (che sarà il caso se il Regno Unito non sia più essere un membro della UE) e della persona fisica che è nella UE, l'identità del rappresentante UE, ove ciò sia richiesto[12];
9) dettagli di eventuali tecnologie, come i cookies, utilizzati su un sito web per raccogliere informazioni personali su persone fisiche;
10) altre informazioni per rendere il trattamento equo e trasparente:
    I. il periodo di conservazione o i criteri utilizzati per impostare la ritenzione;
    II. le informazioni riguardanti i diritti della persona fisica di accesso e di rettifica, cancellazione e restrizioni di informazioni personali, così come il diritto alla portabilità dei dati
    III. il diritto di presentare una denuncia presso l'autorità di vigilanza;
    IV. se il trattamento si basa sul consenso, il diritto di ritirare il consenso;
    V. se la fornitura di informazioni è richiesta da requisiti legge o contrattuali, informare la persona fisica sul perché sia necessario e quali siano le conseguenze della mancata fornitura delle informazioni; e
    VI. informazioni su qualsiasi processo decisionale automatizzato e / o che le informazioni potrebbero essere utilizzate per la profilazione, tra cui la logica applicata e le conseguenze per la persona fisica.

Se le informazioni personali vengono raccolte per scopi di marketing o potrebbero essere utilizzate in futuro per scopi di marketing, l'SG provvede affinché i mezzi con cui una persona fisica può opporsi a tale commercializzazione siano chiaramente spiegati a tale persona fisica.

Dove viene utilizzata la profilatura con mezzi automatizzati per scopi di marketing, l'SG provvede affinché il diritto di opposizione e il meccanismo mediante il quale una persona fisica può opporsi a tali processi sia chiaramente spiegato a tale persona fisica.

L'SG garantisce che, quando il trattamento è stata basato sul consenso, vengano mantenuti dei record di consenso. Inoltre, qualora il consenso venga ritratto, garantisce che il trattamento basato su tale consenso sia cessato e gli atti del ritiro del consenso vengano conservati.

---

[12] *Nota 2 Articolo 3 (2) e 27 del GDPR specifica quando v'è un requisito per un rappresentante con sede nell'UE.*

Non influisce, ad esempio, le autorità pubbliche - vedi l'articolo 27 (2) di come contattare l'organizzazione con domande relative al trattamento dei dati personali, compresi i dati di contatti dei DPO (dove un tale funzionario è stato nominato);

Qualora altri requisiti settoriali o la legislazione richiedano un consenso esplicito per il marketing, l'SG provvede affinché dettagli di questo consenso siano raccolti.

Qualora le informazioni personali ad alto rischio vengano raccolte per un particolare scopo, l'SG assicura che le informazioni fornite sulla privacy affermino esplicitamente lo scopo per il quale tali informazioni personali ad alto rischio sono o potrebbero essere utilizzate.

L'SG assicura che i nuovi metodi di raccolta vengano esaminati e sottoscritti da un lavoratore adeguatamente qualificato o con esperienza per garantire che tali metodi possano essere dimostrati conformi ai requisiti di protezione dei dati e alle buone pratiche.

8.2.6.2 Registrazioni di qualsiasi informativa sulla privacy (ad esempio, le comunicazioni e le dichiarazioni)

L'organizzazione tiene registri delle informative sulla privacy fornite alle persone fisiche (come ad esempio l'informativa sulla privacy e le normative sulla privacy on-line). Queste registrazioni sono conservate almeno fintanto che le informazioni personali a cui si riferiscono vengono mantenute.

Inoltre sono mantenute le informazioni relative a quando una particolare informativa sulla privacy (o a versione della notificazione sulla privacy) era in uso.[13]

8.2.6.3 Tempistica informativa sulla privacy

L'SG garantisce che quando l'organizzazione raccoglie dati personali direttamente da una persona fisica, qualsiasi informazione che deve essere fornita alla persona fisica venga fornita o resa disponibile a tale persona fisica *prima* di ottenere qualsiasi dato personale.

Quando i dati personali non sono ottenuti direttamente dalla persona fisica, le informazioni sono fornite dopo la raccolta dei dati o:

a) al più tardi entro un mese, tenuto conto delle circostanze specifiche in cui le informazioni vengono elaborate, oppure;

b) se il dato è utilizzato per comunicare con la persona fisica, al momento della prima comunicazione; o

c) se il dato è destinato ad essere comunicato a un altro destinatario, almeno quando tale dato viene divulgato per la prima volta.

8.2.6.4 Accessibilità della privacy informazioni

L'SG provvede affinché le informative presentate a persone fisiche siano presentate in un modo che permetta che siano facilmente accessibili e comprensibili per i destinatari.[14]

[13] Questo assicura che ci sia un record delle condizioni alle quali sono state raccolte particolari informazioni personali
[14] Tale informativa viene utilizzata per la raccolta di dati personali di adulti vulnerabili, persone con difficoltà di apprendimento o minori dovrebbero essere presentati e in una lingua e il formato facilmente comprensibile e accessibile a loro.

8.2.6.5 Raccolta da terzi

L'SG provvede affinché, qualora le informazioni personali vengano raccolte da terzi, siano raccolte lealmente e legalmente.

Qualora le informazioni personali vengano raccolte da terzi, l'SG provvede affinché, se necessario, le persone fisiche identificate siano informate entro un mese dalla raccolta, a meno che la persona fisica sia già stata informata e / o comporti uno sforzo sproporzionato[15].

8.2.7 Trattamento per scopi legittimi specifici

Obiettivo: assicurare che le informazioni personali siano ottenute solo per uno o più scopi specificati e che non siano ulteriormente elaborate in alcun modo incompatibili con tali scopi.

8.2.7.1 Basi per il trattamento

L'SG garantisce che le informazioni personali siano ottenute solo per uno o più scopi specificati e che non vengano ulteriormente elaborate in alcun modo incompatibile con tale scopo o con tali scopi.

L'SG garantisce che il trattamento dei dati personali non avvenga in modo tale da violare o potenzialmente violare gli obblighi legali o le condizioni contrattuali.

L'SG garantisce che le informazioni personali raccolte per scopi specificati non vengano utilizzate per un altro scopo incompatibile, a meno che:

a) sia applicabile una esenzione pertinente dalla legislazione; o

b) le persone fisiche le cui informazioni personali devono essere elaborate per il nuovo scopo abbiano acconsentito al trattamento per tale nuovo scopo.

L'SG garantisce che, laddove le informazioni personali ad alto rischio debbano essere utilizzate per un nuovo scopo incompatibile, il consenso esplicito della persona fisica sia ottenuto prima dell'elaborazione, a meno che un'esenzione pertinente non sia applicabile.

8.2.7.2 Consenso per scopi incompatibili

Qualsiasi trattamento è compatibile con lo scopo originale. Se le informazioni personali vengono utilizzate per scopi aggiuntivi o diversi rispetto allo scopo originariamente specificato, il nuovo uso non deve essere inatteso e deve essere equo.

L'SG garantisce che qualsiasi consenso per qualsiasi scopo incompatibile sia dato e informato liberamente.

---

[15] *"Sforzo sproporzionato" in questo contesto non significa semplicemente "uno sforzo considerevole", come all'organizzazione potrebbe essere richiesto di andare a lunghezze considerevoli per fornire informazioni quando il trattamento rischia di avere un effetto pregiudizievole alla persona fisica. Si richiama l'attenzione l'articolo 14, 5 (b) del GDPR.*

Non v'è alcun obbligo di fornire informative qualora le informazioni personali siano state ottenute o divulgate come espressamente consentito dalla legge o v'è un obbligo di riservatezza previsto dalla legge.

L'SG garantisce che:

a) si ottengano indicazioni positive del consenso di una persona fisica all'utilizzo delle proprie informazioni personali per uno scopo; e

b) vengano mantenute le registrazioni del consenso ottenuto per un nuovo scopo

8.2.7.3 Elaborazione delle informazioni dei minori

Laddove vengono elaborate informazioni personali relative ai minori[16], in particolare con l'intenzione di creare un profilo e / o per la commercializzazione, l'SG include un meccanismo per ottenere il consenso del titolare della responsabilità genitoriale, salvo nei casi in cui il servizio si riferisce a servizi di consulenza o di prevenzione.

8.2.7.4 Condivisione dei dati

L'SG garantisce che, laddove l'organizzazione condivida le informazioni personali con un'altra organizzazione, le responsabilità di entrambe le parti riguardo alle informazioni personali siano formalmente documentate in un accordo o contratto scritto, a seconda dei casi.

L'SG garantisce che, laddove l'altra organizzazione stia utilizzando le informazioni personali per i propri scopi:

a) l'accordo o contratto scritto descriva sia le finalità per le quali le informazioni possano essere utilizzate sia eventuali limitazioni o restrizioni sull'ulteriore utilizzo delle informazioni personali per altri scopi; e

b) l'altra organizzazione fornisca un'iniziativa o altra prova del proprio impegno a trattare le informazioni in un modo che non contravvenga alla legislazione sulla protezione dei dati.

L'SG garantisce che, ove possibile, ogni nuovo trattamento che comporta la condivisione di informazioni personali con terzi sia compatibile con i termini delle informazioni forniti alla persona fisica.

Laddove ciò non è possibile, l'organizzazione ha:

1) una base legale per la condivisione dei dati;

2) fornito un'adeguata comunicazione di condivisione alla persona fisica, a seconda dei casi;

3) valutato l'osservanza del principio di limitazione delle finalità; e

4) se richiesto, il consenso della persona fisica alla condivisione dei dati.

[16] *Non esiste un limite di età definito per "minori". L'articolo 8 del GDPR afferma che "le persone fisiche non sono più minori una volta che hanno raggiunto l'età di 16 anni". Se il minore ha meno di 16 anni, l'elaborazione in relazione ai servizi della società dell'informazione è lecita solo se e nella misura in cui il consenso è concesso o autorizzato dal titolare della responsabilità genitoriale sul minore. Gli stati membri potrebbero prevedere una legge per un'età inferiore a 16 anni, ma non può essere inferiore a 13.*

Laddove la condivisione dei dati con terze parti è consentita senza il consenso della persona fisica, l'SG garantisce che sia documentata una registrazione verificabile dei protocolli e dei controlli per questa condivisione dei dati.

Laddove è richiesta la condivisione dei dati con una terza parte, ad esempio, per legge, l'SG garantisce che i protocolli e i controlli per la condivisione dei dati siano documentati.

8.2.7.5 Open Data

Laddove le informazioni personali siano pubblicate come parte di un'iniziativa di "dati aperti", le informazioni personali saranno de-identificate in modo che le persone fisiche non siano identificabili, a meno che non vi siano motivi per rendere pubbliche le informazioni personali.

Quando viene utilizzata la de-identificazione, si tiene conto di tutti i mezzi ragionevoli che possono essere utilizzati per re-identificare una persona fisica.

8.2.7.6 L'abbinamento dei dati (*Data matching*)

Qualora le informazioni personali siano abbinate con altre informazioni personali per creare, ad esempio, un profilo più dettagliato di una persona fisica identificabile, l'SG provvede affinché le informazioni personali abbinate vengano utilizzate solo

- per scopi notificati e compatibili;
- come richiesto dalla legge; o
- qualora sia stato ottenuto il consenso.

Qualora i dati abbinati si riferiscano alle informazioni personali sui minori, misure di protezione specifiche sono state incluse nel SG. Tali misure tengono conto di:

- rischi potenziali e conseguenze;
- requisiti per le garanzie; e
- diritti specifici dei minori.

8.2.8 ADEGUATI, PERTINENTI E IN LINEA CON I PRINCIPI DI MINIMIZZAZIONE DEI DATI

Obiettivo: garantire che le informazioni personali siano adeguate, pertinenti e non eccedenti.

8.2.8.1 Adeguatezza

L'SG assicura che le informazioni personali raccolte dall'organizzazione siano adeguate per gli scopi dell'organizzazione.

Inoltre l'SG salvaguarda che siano effettuate le revisioni regolari (ad esempio annualmente) di tecnologia e dei processi di trattamento di dati personali al fine di assicurare che le informazioni personali continuino ad essere adeguate per tali scopi.

8.2.8.2 Pertinenza e non eccedenza

L'SG provvede affinché:

a) l'organizzazione elabori la quantità minima di dati personali richiesta per conseguire l'obiettivo legittimo;

b) le informazioni personali che non sono rilevanti o sono eccessive per gli scopi dichiarati non vengano trattate, a meno che la fornitura di tali informazioni sia facoltativa e siano utilizzate con il consenso della persona fisica;

c) nuovi sistemi e processi di trattamento dei dati personali vengano esaminati al fine di garantire che le informazioni in lavorazione siano pertinenti e non eccessive.

Qualora non sia pertinente o necessario elaborare le informazioni personali per scopi dell'organizzazione, l'SG garantisce che le informazioni personali non vengano elaborate.[17]

8.2.9 Precisione

Obiettivo: garantire che le informazioni personali siano accurate e, se necessario, tenute aggiornate.

8.2.9.1 Accuratezza e aggiornamento

L'SG garantisce il mantenimento dell'integrità e della precisione delle informazioni personali trattate.

L'SG assicura che le persone fisiche abbiano la possibilità di contestare l'esattezza dei propri dati personali e di ottenerne la rettifica laddove necessario. Qualora le informazioni personali siano imprecise e incapaci di essere corrette, per esempio in relazione a un record storico, l'SG documenta l'inesattezza riportata e, se del caso, le informazioni personali accurate.

L'SG dispone di processi approvati e documentati per verificare se presunte imprecisioni siano davvero imprecise. Nel caso in cui questo processo di verifica concluda che la presunta imprecisione sia erronea e i dati siano, di fatto, accurati, l'SG conserva le prove del caso.

L'SG provvede affinché i lavoratori siano informati dell'importanza delle registrazioni delle informazioni personali in modo accurato e la necessità di utilizzare solo informazioni personali aggiornate per prendere decisioni importanti circa le persone fisiche.

Il Sistema di Gestione in atto:

a) informa i terzi con i quali l'organizzazione ha condiviso informazioni personali imprecise o out-of-date che tali informazioni sono imprecise e / o out-of-data e non devono essere utilizzate per informare le decisioni circa la persona fisica interessata; e

b) condivide eventuali correzioni alle informazioni personali con la terza parte quando ciò è richiesto.

L'SG riesamina i nuovi sistemi e processi che comportano il trattamento dei dati personali, al fine di:

[17] *L'organizzazione ha bisogno di esaminare se sia opportuno utilizzare la forma anonima o un altro tipo di de-identificazione dei dati personali prima del trattamento con il fine di salvaguardare ulteriormente i dati e di documentare i risultati delle considerazioni*

1) confermare che questi sistemi o processi prevengano, per quanto possibile, la registrazione di informazioni personali inesatte o out-of-date, e

2) consentire correzioni da apportare a informazioni personali inesatte o out-of-date.

8.2.10 Conservazione ed eliminazione

Obiettivi: garantire che le informazioni personali non vengano conservate per più di quanto sia necessario.

8.2.10.1 Programmi di conservazione

L'SG ha definito e implementato dei programmi di conservazione per l'identificazione dei periodi di conservazione delle informazioni personali. Tali programmi:

a) includono qualsiasi periodo minimo richiesto dalla legge, nonché i periodi di conservazione stabiliti dall'organizzazione; e

b) rendono chiara e documentata la giustificazione e la base per i periodi di conservazione.

Al termine del periodo di conservazione, l'SG garantisce che tutte le copie delle informazioni personali non più richieste dall'organizzazione vengano smaltite, sulla base delle procedure di smaltimento con le quali sono gestite[18]:

1) utilizzando processi approvati;

2) con un livello di sicurezza adeguato alla sensibilità dei dati personali; e

3) in linea con la valutazione del rischio sicurezza delle informazioni dell'organizzazione.

Qualora le informazioni personali debbano essere trasferite per la conservazione a lungo termine (ad esempio, in cui è di valore per scopi di archiviazione di interesse pubblico, scopi di ricerca scientifica o storica o fini statistici), allora esse sono soggette ad adeguate misure tecniche e organizzative[19] al fine di salvaguardare i diritti e le libertà della persona fisica.

L'SG garantisce l'attuazione del programma di conservazione e la comunicazione dei programmi a tutti i lavoratori interessati.

8.2.11 I problemi relativi alla sicurezza

Obiettivo: assicurare che le informazioni personali siano protette contro il trattamento non autorizzato o illecito e contro perdite, distruzioni o danni esterni, utilizzando adeguate misure e controlli tecnici e organizzativi

8.2.11.1 Le misure di sicurezza

L'SG definisce le misure di sicurezza adeguate, tenendo conto dello stato dell'arte, il costo di implementazione e la natura, la portata, il contesto e le finalità del trattamento dei dati personali.

Nota: tali misure di sicurezza possono includere:

[18] *Le procedure di smaltimento comprendono le copie detenute sui sistemi di backup / media.*
[19] *Si veda l'articolo 5 (1 sexies) del GDPR*

a) la pseudonominazione e / o la crittografia dei dati personali;

b) la capacità di garantire in corso la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi;

c) la capacità di ripristinare l'accesso alle informazioni personali in caso di incidente fisico e / o tecnico; e

d) la sperimentazione e la valutazione dell'efficacia delle misure di sicurezza individuate.

8.2.11.2 Controlli di sicurezza

L'SG attua le misure di sicurezza appropriate definendo e implementando controlli di sicurezza sulla base:

a) del tipo di informazioni personali trattate;

b) del rischio di danno o disagio alla persona fisica nel caso l'informazione venga compromessa ; e

c) del rischio di danni operativi e reputazionali per l'organizzazione[20].

Qualora si elaborino informazioni personali ad alto rischio, l'SG assicura che i controlli di sicurezza previsti e realizzati siano appropriati ai rischi identificati e valutati, e che rimangano così.

N.B. Se del caso, l'organizzazione potrebbe prendere in considerazione la conformità con BS EN ISO / IEC 27001. La certificazione BS EN ISO / IEC 27001 da parte di un organismo esterno al fine di dimostrare la conformità è anche una possibilità.

8.2.11.3 Stoccaggio e movimentazione

L'SG assicura che le informazioni personali siano immagazzinate e manipolate in modo sicuro, con precauzioni adeguate alla loro riservatezza e sensibilità.

L'SG garantisce una particolare attenzione per la memorizzazione di informazioni personali su supporti rimovibili, dispositivi portatili (soprattutto se il dispositivo portatile viene utilizzato nell'ambito di una politica "portare il proprio dispositivo") e sistemi di storage di terze parti (ad esempio, il cloud storage) .

8.2.11.4 Trasferimento

L'SG garantisce che, qualora le informazioni personali siano trasferite elettronicamente o manualmente all'interno dell'organizzazione o ad altre organizzazioni, questa trasmissione sia fissata con mezzi appropriati definiti dalla struttura al fine di salvaguardare le informazioni durante la trasmissione.[21]

8.2.11.5 Controllo degli accessi

[20] *La valutazione del rischio (8.2.3) stabilisce un adeguato livello di controllo. Over-specificare i requisiti di sicurezza può essere dannosi o tanto come sotto-specificare*
[21] *Per i trasferimenti elettronici, la crittografia deve essere utilizzata.*

L'SG provvede affinché, qualora sia consentito l'accesso dei lavoratori alle informazioni personali, questo accesso sia limitato a quei lavoratori che necessitano di tale accesso, come parte del loro ruolo.

L'SG provvede inoltre affinché sia chiaro ai lavoratori che, dove l'accesso è legittimamente concesso, questo è limitato allo scopo lavorativo e che le informazioni saranno accessibili solo per scopi legittimi.

Qualora vengano elaborate informazioni personali ad alto rischio, l'SG assicura che i controlli di accesso riflettano la sensibilità di tali informazioni.

L'SG assicura inoltre che gli accessi alle informazioni personali vengano monitorati e valutati in linea con la valutazione del rischio sicurezza delle informazioni dell'organizzazione.

8.2.11.6 Valutazioni di sicurezza

L'SG garantisce che le valutazioni di sicurezza siano regolarmente eseguite.

Tali valutazioni stabiliscono se i controlli di sicurezza esistenti sono adeguati e formulano raccomandazioni per miglioramenti ove necessario.

Tali valutazioni tengono conto del rischio di danni e / o difficoltà per le persone fisiche in caso di violazione della sicurezza.

8.2.11.7 Gestione delle violazioni della sicurezza

L'SG ha implementato una procedura (vedi **Politica Gestione degli Incidenti di Sicurezza delle Informazioni** e **Modulo Segnalazione Data Breach**) che:

a) valuta, gestisce e documenta le violazioni della sicurezza che coinvolgono informazioni personali, incluse le procedure per mitigare il danno causato da qualsiasi violazione della sicurezza;

b) informa l'autorità di vigilanza (con le informazioni richieste entro 72 ore dalla presa di coscienza della violazione) di eventuali violazioni della sicurezza che costituiscono una violazione che potrebbe comportare un rischio per i diritti e le libertà di qualsiasi persona fisica. Tali notifiche comprendono:

   1) una descrizione delle informazioni personali coinvolte;

   2) i dettagli delle categorie delle informazioni personali e il numero approssimativo di *records* coinvolti;

   3) i dettagli di contatto per il responsabile della protezione dei dati o di altri punti di contatto all'interno dell'organizzazione;

   4) una descrizione delle probabili conseguenze della violazione;

   5) una descrizione delle misure adottate o proposte per affrontare la violazione e per mitigare eventuali effetti negativi;[22]

c) qualora la violazione possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, notifica alle persone fisiche interessate senza indebito ritardo:

   1) la violazione della sicurezza;

[22] *Si richiama l'attenzione sull'articolo 33, paragrafo 3, del GDPR*

2) la natura della violazione; e

3) eventuali raccomandazioni per le loro azioni riguardanti la mitigazione di eventuali rischi avversi;

d) documenta ogni violazione della sicurezza, compresa una valutazione del modo in cui si è verificata la violazione, quali azioni correttive sono state intraprese e cosa può essere appreso dalla violazione;

e) prende decisioni in merito all'eventualità che una violazione della sicurezza venga indirizzata a qualsiasi autorità di regolamentazione pertinente e

f) conserva le registrazioni di tali notifiche rilasciate.

8.2.11.8 Trasferimento di informazioni personali al di fuori del territorio nazionale

Qualora l'organizzazione trasferisca informazioni personali al di fuori del territorio nazionale[23], l'SG garantisce che i diritti delle persone fisiche siano tutelati:

a) nel caso in cui lo Stato non sia membro dell'UE o del SEE al momento del trasferimento:

1) per il trasferimento in un paese o territorio che è membro del SEE stabilendo se il SEE è stato valutato dall'Italia come dotato di adeguata protezione;

2) per il trasferimento in altri paesi o territori, stabilendo se il paese o il territorio di destinazione è stato valutato dall'Italia come dotato di adeguata protezione;

b) nel caso in cui l'Italia sia membro dell'Unione europea o del SEE al momento del trasferimento, stabilendo se il paese o il territorio sia stato valutato dalla Commissione europea come "adeguato";

c) includendo nei contratti condizioni specifiche che garantiscano la protezione delle informazioni personali e il trattamento, ad es. impiegando, basandosi su o rispecchiando clausole standard stabilite o contratti tipo;

d) ponendo in essere regole interne vincolanti d'impresa (BCR) quando il trasferimento è verso un'altra entità all'interno della stessa organizzazione;

e) rispettando un codice di condotta approvato o un meccanismo di certificazione approvato insieme a impegni vincolanti ed esecutivi sull'organizzazione di destinazione;

f) per gli enti pubblici ottemperando ad uno strumento o ad un accordo amministrativo giuridicamente vincolante;

g) mediante trasferimento in linea con una deroga applicabile.

L'SG garantisce che l'alta direzione e il/i lavoratore/i responsabile/i per la conformità ai requisiti di protezione dei dati e alle buone pratiche rivedano tutte le nuove iniziative che coinvolgono:

i. il trasferimento di informazioni personali tra il Regno Unito e il SEE; e

[23] *Nota personale: Le informazioni sui trasferimenti di dati al di fuori dell'UE sono disponibili su http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm*

ii. il trasferimento di informazioni personali al di fuori del Regno Unito.

Questo riesame deve stabilire se possa essere fornita una protezione adeguata per tali trasferimenti.

L'SG garantisce che i responsabili del trattamento dei dati e gli eventuali sub-responsabili esterni al Regno Unito che trattano le informazioni personali per conto dell'organizzazione operino secondo termini contrattuali appropriati (ad esempio clausole standard o contratti tipo, come quelli approvati dalla Commissione europea per garantire un'adeguata protezione delle informazioni personali), a meno che non siano state concordate altre procedure adeguate per proteggere le informazioni personali.

8.2.11.9 Divulgazione a richieste di terzi

L'SG garantisce che i terzi forniscano la prova di:

a) il loro diritto di richiedere una copia delle informazioni personali specificate; e

b) se necessario, la loro identità.

L'SG garantisce che venga effettuato un controllo per garantire che vi siano motivi legali per divulgare informazioni a terzi. Solo la quantità minima di informazioni personali necessarie sarà comunicata a terzi.

L'SG conserva le registrazioni delle divulgazioni di informazioni personali. Questi registri dimostrano la legalità della divulgazione e consentono all'organizzazione di tenere traccia di dove siano state divulgate le informazioni personali.[24]

8.2.11.10 Trattamento di informazioni subappaltate

L'SG garantisce che, qualora le informazioni personali siano trattate per suo conto da altre organizzazioni:

a) vengano selezionate solo le organizzazioni che agiscono come responsabili del trattamento dei dati in grado di fornire sicurezza tecnica, fisica e organizzativa che soddisfi i requisiti dell'organizzazione per tutte le informazioni personali che trattano per conto di questa organizzazione;

b) sia stata intrapresa una valutazione dell'adeguata sicurezza nell'ambito della dovuta diligenza prima che un organismo che agisce come responsabile del trattamento dei dati sia assunto e, se ritenuto necessario a causa della natura delle informazioni personali da trattare o in ragione delle particolari circostanze del trattamento, sia stata intrapresa anche una verifica delle disposizioni sulla sicurezza dell'organizzazione che agisce come responsabile del trattamento dei dati prima di stipulare il contratto;

c) sia stata effettuata la due diligence sull'organizzazione che agisce in qualità di responsabile del trattamento dei dati (*data processor*);

d) una volta selezionata l'organizzazione che agisce in qualità di responsabile del trattamento dei dati, l'organizzazione mette in atto un accordo scritto vincolante o un contratto che:

[24] *Quando l'accesso alle informazioni personali da parte di terzi è concesso in base a una legge come il Freedom of Information Act 2000 [4], la verifica dell'identità e la minimizzazione delle informazioni divulgate potrebbero non essere necessario*

1) definisce l'oggetto e la durata del trattamento, la natura e le finalità del trattamento, il tipo di informazioni personali e le categorie di persone fisiche, nonché gli obblighi e i diritti dell'organizzazione;
2) stabilisce che l'organizzazione che agisce in qualità di responsabile del trattamento dei dati elabori le informazioni personali solo sotto istruzioni documentate;
3) stabilisce che, per quanto riguarda i trasferimenti di informazioni personali verso un paese terzo o un'organizzazione internazionale, a meno che non sia richiesto dal diritto dell'Unione o dello Stato membro a cui è soggetta l'organizzazione che agisce in qualità di responsabile del trattamento, l'organizzazione che agisce come responsabile del trattamento informa questa organizzazione di qualsiasi requisito giuridico prima del trattamento, a meno che tale legge non vieti tali informazioni per importanti motivi di pubblico interesse;
4) garantisce che i lavoratori autorizzati a trattare le informazioni personali si siano impegnati a mantenere la riservatezza o siano soggetti ad un obbligo legale di riservatezza;
5) richiede all'organizzazione che agisce come responsabile del trattamento dei dati di assistere l'organizzazione nel rispetto dei diritti delle persone fisiche;
6) introduce una richiesta specifica di conformità con i requisiti legali di notifica all'organizzazione per qualsiasi violazione della sicurezza senza alcun ritardo indebito;
7) richiede all'organizzazione che agisce come responsabile del trattamento dei dati di fornire adeguata sicurezza per le informazioni personali che elaborerà;
8) attiva audit regolari delle disposizioni sulla sicurezza dell'organizzazione che agisce come responsabile del trattamento dei dati durante il periodo in cui l'organizzazione che agisce come responsabile del trattamento dei dati ha accesso alle informazioni personali;
9) richiede all'organizzazione che agisce come responsabile del trattamento dei dati di ottenere il permesso dell'organizzazione prima di utilizzare ulteriori subappaltatori per elaborare le informazioni personali;
10) richiede che i contratti con subappaltatori dell'organizzazione che agiscono in qualità di responsabili del trattamento richiedano ai subappaltatori di rispettare almeno le stesse norme di sicurezza e di altro genere di quelle implementate dall'organizzazione che agisce come responsabile del trattamento dei dati;
11) richiede che i contratti con l'organizzazione che agisce come i responsabili del trattamento dei dati (che sono trasmessi a qualsiasi subappaltatore) specifichino che, al termine del contratto, le informazioni personali correlate saranno distrutte o passate ad un'altra organizzazione che agisce come un elaboratore di dati come specificato da questa organizzazione; e
12) richiede all'organizzazione che agisce come responsabile del trattamento di mettere a disposizione dell'organizzazione prove di conformità con l'accordo / contratto.

8.2.12 Diritti delle persone fisiche

Obiettivo: assicurare che i diritti delle persone fisiche siano presi in considerazione e rispettati laddove appropriato.

8.2.12.1 Rispondere ai diritti

L'SG comprende procedure che garantiscono

- il rispetto dei diritti delle persone fisiche in relazione alle loro informazioni personali
- che le richieste di esercitare tali diritti siano trattate senza indebito ritardo (o in ogni caso entro un mese dal ricevimento della richiesta da parte della persona fisica).

L'SG garantisce che le persone fisiche siano informate, in caso di eventuali proroghe, al termine di un mese per soddisfare le richieste e per fornire le informazioni in formato elettronico o cartaceo come richiesto dalla persona fisica. L'SG garantisce che qualsiasi proroga al periodo di un mese per soddisfare una richiesta di una persona fisica non sia più lunga di altri due mesi.

NOTA Tali diritti comprendono l'accesso alle informazioni, l'opposizione al trattamento, la rettifica di informazioni inesatte, la cancellazione e / o la limitazione dell'uso delle informazioni, la portabilità dei dati e il diritto di non essere sottoposti a trattamento automatizzato laddove tale elaborazione si riferisce alla profilazione o influisce in modo significativo la persona naturale.

L'SG garantisce che le procedure comprendano l'eventuale applicazione di deroghe o esenzioni.

8.2.12.2 Accesso alle informazioni

L'SG garantisce che la persona fisica sia in grado, su richiesta, di ottenere la conferma dell'esistenza o meno di informazioni personali che la riguardano e, in tal caso, di avere accesso alle informazioni personali, di ricevere una copia delle informazioni personali e le seguenti informazioni, a meno che non si applichi una deroga specifica:

a) le finalità del trattamento;

b) le categorie di informazioni personali interessate;

c) i destinatari o le categorie di destinatari a cui sono state comunicate le informazioni, in particolare i destinatari in paesi terzi o organizzazioni internazionali;

d) ove possibile, il periodo previsto per il quale saranno archiviate le informazioni personali o, se non possibile, i criteri utilizzati per determinare tale periodo;

e) l'esistenza del diritto di chiedere la rettifica o la cancellazione di informazioni personali o la limitazione del trattamento di dati personali relativi alla persona fisica o di opporsi a tale trattamento;

f) l'esistenza del diritto di presentare un reclamo all'autorità di controllo;

g) qualora le informazioni personali non siano state raccolte dall'interessato, eventuali informazioni disponibili sulla fonte delle informazioni;

h) esistenza di processi decisionali automatizzati, inclusa la profilazione (cfr. 8.2.12.8) e informazioni significative sulla logica coinvolta, nonché sul significato e le conseguenze di tale trattamento per la persona fisica; e

i) se le informazioni personali sono trasferite a un paese terzo o ad un'organizzazione internazionale, quali sono le misure di sicurezza appropriate che sono state messe in atto.

8.2.12.3 Rettifica

L'SG garantisce che la persona fisica sia in grado, senza indebito ritardo, di ottenere la rettifica di dati personali inesatti che la riguardano in conformità al 8.2.9. Queste procedure assicurano inoltre che la persona fisica sia in grado di completare le informazioni personali incomplete.

8.2.12.4 Cancellazione

L'SG garantisce che le richieste provenienti da persone fisiche soggette al principio del "diritto all'oblio" siano gestite in modo appropriato.

L'SG garantisce che una persona fisica abbia il diritto di ottenere la cancellazione di informazioni personali su di esse senza indebito ritardo se:

a) i dati personali non sono più necessari in relazione agli scopi per i quali sono stati originariamente raccolti o altrimenti trattati;

b) il trattamento è stato basato sul consenso, la persona fisica ritira il proprio consenso e non vi è altra base legale per continuare a elaborare le informazioni;

c) la persona fisica ha contestato il trattamento in questione e non vi sono motivi legittimi per il trattamento, o la persona fisica ha obiettato al marketing;

d) i dati personali sono stati trattati illecitamente;

e) le informazioni personali devono essere cancellate per essere conformi ad un obbligo legale;

f) le informazioni personali sono state raccolte per offrire servizi della società dell'informazione.

L'SG garantisce che, laddove le informazioni siano state rese pubbliche, siano prese misure appropriate per informare altre organizzazioni che potrebbero trattare le informazioni personali di cui la persona fisica ha richiesto la cancellazione delle informazioni.

8.2.12.5 Restrizione del trattamento

L'SG garantisce che la persona fisica abbia il diritto di ottenere la restrizione del trattamento delle informazioni personali laddove:

a) l'accuratezza delle informazioni personali è stata contestata dalla persona fisica, per un periodo che consente all'organizzazione di verificare l'esattezza delle informazioni personali;

b) il trattamento è illegale e la persona fisica si oppone alla cancellazione di informazioni personali e richiede invece la limitazione del suo utilizzo;

c) l'organizzazione non ha più bisogno delle informazioni personali ai fini del trattamento, ma è richiesta dalla persona fisica per l'istituzione, l'esercizio o la difesa di reclami legali; o

d) la persona fisica ha obiettato al trattamento e la restrizione rimane in sospeso in attesa di verificare se i motivi legittimi dell'organizzazione prevalgono su quelli della persona fisica.

L'SG garantisce che quando una limitazione sta per essere revocata, la persona fisica viene informata prima che ciò avvenga.

8.2.12.6 Portabilità dei dati

L'SG garantisce che, qualora la persona fisica abbia il diritto alla portabilità dei dati e le informazioni siano trattate con mezzi automatizzati, la persona fisica è in grado di avere tali informazioni trasmesse a loro o ad un'altra organizzazione da esse nominata, a titolo gratuito e in un formato strutturato, comunemente usato e leggibile da una macchina.[25]

8.2.12.7 Obiezione

L'SG garantisce che siano in atto procedure per prendere in considerazione e rispondere alle richieste di una persona fisica che si oppone al trattamento di dati personali.

Quando una persona fisica si oppone al trattamento di dati personali ai fini del marketing diretto, l'SG garantisce che il trattamento venga cessato per quella persona fisica.

8.2.12.8 Decisioni automatizzate, inclusa la profilazione

L'SG garantisce che ci siano procedure per l'identificazione del trattamento delle informazioni personali risultanti da un processo decisionale automatizzato, inclusa la profilazione, che potrebbe influire in modo significativo su una persona fisica.

L'SG garantisce almeno che qualsiasi decisione automatizzata possa comportare un intervento umano quando richiesto dalla persona fisica.

8.2.12.9 Reclami e ricorsi

L'SG include una procedura di reclamo che assicuri che i reclami relativi al trattamento dei dati personali siano gestiti correttamente. Ciò include le procedure per considerare i ricorsi da parte di persone fisiche sul modo in cui i loro reclami sono stati gestiti.

8.2.13 Manutenzione

Obiettivo: assicurare che i sistemi tecnologici siano appropriatamente mantenuti.

L'SG garantisce che le procedure e i componenti tecnologici siano mantenuti per assicurare il loro corretto e appropriato funzionamento. Queste procedure assicurano che tale manutenzione sia pianificata ed eseguita su base regolare e programmata.

Documenti applicabili

[25] *Vedi articolo 20 del GDPR*

M 6.1.1. Registro delle attività di trattamento
M 6.1.1. DPIA – Valutazione d'Impatto
P 7.2.1 Formazione e Addestramento
Allegato a MSG – Politica della protezione dei dati personali
Allegato a MSG – Politiche operative
P 8.1.1. Diritti dell'interessati
Modulo Segnalazione Data Breach
Modello di esercizio diritti in materia di protezione dei dati personali

CAPITOLO 9

VALUTAZIONE DELLE PERFORMANCE

9.1 MISURAZIONE DELLE PRESTAZIONI E CONTROLLO

Il responsabile dell'analisi dei dati è RSG che, congiuntamente alla Direzione, individua, raccoglie ed analizza i dati appropriati, provenienti dalle varie fonti, allo scopo di:

- Valutare le prestazioni a fronte degli obiettivi stabiliti.
- Individuare le aree per il miglioramento.

Il momento di elezione per l'analisi dei dati è rappresentato dal Riesame della Direzione.

Al fine di migliorare con continuità l'efficacia del sistema di gestione la nostra organizzazione utilizza i dati e le informazioni, provenienti da

- obiettivi;
- verifiche ispettive interne/Audit;
- analisi dei dati;
- analisi delle non conformità;
- sviluppo di azioni correttive;
- politica dell'organizzazione.

Le informazioni raccolte, sono oggetto di valutazione nel corso delle periodiche riunioni di riesame da parte della Direzione. L'esito delle azioni attivate viene verificato in occasione dei successivi incontri di riesame, che costituiscono quindi il momento in cui valutare se il sistema di gestione per la qualità, risulta efficace per il conseguimento degli obiettivi pianificati e di conseguenza, per il miglioramento continuo.

Per eliminare le cause delle non conformità e per prevenire il loro ripetersi vengono attivate delle **azioni correttive** adeguate all'impatto dei problemi riscontrati.

Ove fosse necessario l'utilizzo di attrezzature per la misurazione e il controllo delle prestazioni, l'organizzazione dovrà istituire e mantenere procedure per calibrare e mantenere queste attrezzature. I dati delle attività e dei risultati di calibrazione e manutenzione dovranno essere conservati.

9.2 AUDIT

E' stata predisposta la **P 9.2.1"Audit"** al fine di descriverne le modalità di pianificazione, esecuzione e registrazione.
Le verifiche ispettive interne/Audit hanno lo scopo di verificare l'attuazione delle disposizioni definite dal Sistema di gestione, al fine di migliorarne in modo continuo l'efficacia.
Le verifiche ispettive interne sono periodicamente pianificate, in occasione dei periodici riesami del sistema di gestione per la qualità, da parte di RSG e della Direzione.
La pianificazione tiene conto delle aree più critiche, ma assicura che ogni funzione venga esaminata almeno una volta all'anno.

Le verifiche vengono effettuate principalmente da RSG o comunque da personale designato dalla direzione, indipendente da chi è diretto responsabile delle attività sottoposte a verifica.

Possono essere incaricati di effettuare gli Audit interni anche professionisti esterni purché adeguatamente qualificati.
Nella **P 9.2.1"Audit"** sono stati definiti i requisiti minimi per poter essere designati a condurre le verifiche ispettive interne/Audit sul sistema di gestione.

Con sufficiente anticipo, il verificatore, che deve rispondere a requisiti di indipendenza rispetto al settore oggetto dell'Audit, concorda con il responsabile della funzione interessata, le date e gli orari degli Audit.
Gli Audit interni vengono condotti mediante colloqui, osservazioni dirette del sistema di gestione, esame delle evidenze oggettive documentate.[26]

Nel corso della conduzione degli Audit, l'incaricato effettua una valutazione sulla conformità riscontrata in riferimento a quanto indicato nella documentazione del Sistema (MSG,P,I). Tale valutazione viene sintetizzata in un verbale riassuntivo della verifica.

Sono previsti metodi adeguati per monitorare e misurare i processi del Sistema di gestione in modo da controllare la capacità dei processi stessi ad ottenere i risultati pianificati.
Qualora tali risultati non siano raggiunti, vengono adottate correzioni ed intraprese azioni correttive, come indicato nel presente manuale.

Tutte le informazioni utili a seguire l'andamento delle prestazioni, dei controlli operativi appropriati e della conformità agli obiettivi, vengono opportunamente registrate e gestite come indicato dalla parte di sistema relativa alla gestione dei documenti e delle registrazioni. I controlli sulle attività vengono condotti secondo i risultati del Risk Assessment e della Valutazione d'impatto.

Nel caso di rilevazione di non conformità devono essere apportate correzioni opportune prima di proseguire nell'attività di trattamento, salvo diversa indicazione di DS.

Il programma di audit include esplicitamente qualsiasi trattamento di informazioni personali ad alto rischio (cfr. 8.2.2.2) e include qualsiasi trattamento di dati personali da parte di subappaltatori (responsabili del trattamento dei dati) (cfr. 8.2.11.10).

[26] *Controlli regolari da parte di soggetti esterni dovrebbero essere presi in considerazione da organizzazioni più grandi e da quelle che elaborano informazioni personali ad alto rischio (vedere 8.2.2.2).*

*Le relazioni di audit che specificano qualsiasi distacco significativo dalla **Politica** SG e / o le procedure stabilite sono fornite alla direzione.*
Le relazioni di audit devono anche identificare le questioni relative alla tecnologia o ai processi che potrebbero influire sulla conformità alla **Politica Protezione dei dati**.

Documenti applicabili

P 9.2.1 Audit
P 6.1.1 DPIA – Valutazione d'impatto

9.3 RIESAME DELLA DIREZIONE

Il **Riesame della direzione** valuta l'eventuale necessità di cambiare la politica, gli obiettivi e gli altri elementi del sistema di gestione, alla luce dei risultati provenienti dalle Verifiche interne del sistema stesso, da cambiamenti della situazione e dall'impegno al miglioramento continuo.

Gli elementi in ingresso per la conduzione del riesame sono:

⇒ Risultati degli Audit
⇒ Prestazioni e conformità dei prodotti e dei processi
⇒ Stato delle azioni correttive
⇒ Azioni a seguire di precedenti riesami
⇒ Avanzamento delle modifiche pianificate che, per una serie di fattori quali: mutamenti legislativi, condizioni economico-sociali, condizioni finanziarie ecc.., potrebbero avere influenza sul sistema
⇒ Cambiamenti che potrebbero influenzare il sistema di gestione del sistema
⇒ Raccomandazioni e proposte per il miglioramento
⇒ Gli obiettivi

Gli elementi in uscita dal riesame sono:

⇐ Azioni relative al miglioramento del SG e dei suoi processi;
⇐ Azioni relative al miglioramento dei prodotti/servizi connessi ai requisiti del cliente;
⇐ Obiettivi misurabili e relativi indici numerici;
⇐ Necessità di risorse;
⇐ Eventuale variazione della politica;
⇐ Variazioni del sistema e del campo di applicazione;
⇐ Obblighi contrattuali e normativi;
⇐ Revisione dei rischi;
⇐ Revisione dei budget;

Le registrazioni dei riesami sono conservate **M 9.3.1 Riesame del Sistema**.
I riesami sono condotti con l'obiettivo di essere concretamente rivolti alle esigenze dell'impresa

Nel riesame vengono presi in considerazione gli aspetti relativi alle infrastrutture, alle attrezzature e ai bisogni degli ambienti di lavoro per il raggiungimento degli obiettivi.

a) rischi identificati e intensificati dai lavoratori;
b) registrazioni di revisioni procedurali;
c) risultati degli aggiornamenti tecnologici e / o delle sostituzioni;
d) richieste formali di valutazione da parte di organismi di regolamentazione;
e) trattamento dei reclami; e
f) violazioni della sicurezza / incidenti di sicurezza delle informazioni verificatisi.

I risultati del riesame della direzione comprendono le decisioni relative alle opportunità di miglioramento continuo e qualsiasi necessità di modifiche al SG, ad esempio l'identificazione di modifiche alla politica, alle procedure e / o alla tecnologia SG che potrebbero influire sulla conformità.
L'organizzazione deve conservare le informazioni documentate come prova dei risultati dei riesami della direzione.
Laddove vengono apportate modifiche importanti ai SG, una verifica deve essere completata al più presto possibile dopo l'attuazione.

Documenti applicabili
M 9.3.1 Riesame del Sistema
P 9.3.1 Riesame della Direzione

CAPITOLO 10

MIGLIORAMENTO

10.1 NON CONFORMITÀ E AZIONI CORRETTIVE

La nostra organizzazione ha individuato, nell'ambito dei propri processi, opportune attività di misurazione e di monitoraggio.
Tutta l' attività di controllo e monitoraggio è volta a migliorare in modo continuativo l'organizzazione.
Le attività sopra elencate sono descritte nel dettaglio nelle procedure e di seguito riassunte.
Ove opportuno tali controlli permettono di eseguire elaborazioni a supporto del riesame del sistema da parte della direzione.
Le **non conformità** possono riguardare il Sistema, i processi, oltre a servizi/prodotti forniti o ricevuti. Le NC possono essere accidentali, quindi determinate da eventi fortuiti, oppure possono essere strutturali e quindi riconducibili, in linea generale, al sistema organizzativo e di qualità dell'organizzazione.
La gestione delle non conformità, ovverosia dei problemi che si presentano, include i seguenti aspetti:

- identificazione e il controllo dei servizi e dei prodotti non conformi ai requisiti
- comunicazione alle funzioni interessate
- correzione delle non conformità rilevate
- verifica della efficacia della correzione
- registrazioni

La metodologia da adottare, le responsabilità, le autorità, nonché i moduli di registrazione delle NC e le relative modalità di gestione, sono dettagliatamente descritti nella procedura **P 10.1.1 "Gestione delle Non Conformità"**. Essa ha lo scopo di impedire che le difformità possano evolvere in modo non controllato.

La nostra organizzazione prende in considerazione sia **Reclami** scritti, che Reclami di natura verbale da parte dei Clienti.
Qualora i reclami pervengano in forma verbale vengono registrati con la modulistica prevista in **P 10.1.1 "Gestione delle Non Conformità"**. Successivamente RSG ne valuta la sussistenza ed eventualmente compila la relativa modulistica.
I Reclami scritti, che pervengono all'organizzazione, sono identificati e opportunamente conservati da RSG che individua le azioni più opportune con il supporto di DS.
A seguito di un reclamo pervenuto in forma scritta, DS, coadiuvato da RSG ha la responsabilità di predisporre una comunicazione di risposta da inviare al cliente.
RSG ha il compito di tenere correttamente aggiornato il "Registro dei problemi" come descritto in **P 10.1.1 "Gestione delle non conformità"**.

La procedura **P 10.1.2 "Azioni correttive"** definisce i seguenti requisiti per le azioni correttive intraprese:
1. identificazione e registrazione delle non conformità (compresi i reclami dei clienti);
2. individuazione e registrazione delle cause delle non conformità (relative al prodotto, ai processi, al sistema);
3. valutazione delle esigenze di adottare azioni per evitare il ripetersi delle non conformità;
4. individuazione ed attuazione delle azioni correttive necessarie;
5. registrazione dei risultati delle azioni adottate;
6. effettuazione del riesame delle azioni correttive adottate al fine di verificarne l'efficacia.

L'esito e l'efficacia delle azioni correttive intraprese viene discusso nel corso del riesame periodico del sistema di gestione da parte della Direzione.
La valutazione del rischio è condotta a intervalli regolari, per determinare se la posizione è cambiata, e qualsiasi non conformità deve essere corretta (vedere 8.2.3).
L'organizzazione garantisce che tutti i nuovi rischi identificati per le informazioni personali (sia all'interno dell'organizzazione che nella più ampia prospettiva nazionale) siano valutati utilizzando procedure proattive come le PIA (vedi 6.1.4).
Tutte le modifiche e / o i miglioramenti proposti sono valutati prima dell'implementazione per garantire che i requisiti della **Politica** siano soddisfatti.
Le modifiche che potrebbero influire sulla capacità di dimostrare la conformità con i requisiti di protezione dei dati e le buone pratiche (come la conversione delle informazioni personali in un nuovo formato di file di archiviazione) sono riviste per determinare se incidono sulla conformità.
Le modifiche derivanti da azioni correttive sono documentate e conservate conformemente al programma di conservazione.
L'organizzazione conserva inoltre le informazioni documentate come prova:

- della natura delle non conformità e delle eventuali azioni successive;
- dei risultati di qualsiasi azione correttiva.

Documenti applicabili
P 10.1.1 Gestione delle non conformità
P 10.1.2 Azioni correttive
Allegato – Politiche protezione dei dati personali

10.3 MIGLIORAMENTO

Per monitorare la **soddisfazione del cliente** è tato predisposto un questionario di **customer satisfaction** per acquisire le informazioni in merito alla soddisfazione del cliente, anche in materia di trattamento dei dati. Il questionario viene somministrato a tutti i clienti. I risultati vengono raccolti ed elaborati da RSG.
Altri dati utili a percepire la soddisfazione dei clienti sono:

- ✓ i reclami pervenuti dai clienti;
- ✓ le insolvenze.

I dati raccolti dalle indagini sono elaborati da RSG e valutati con la direzione, nelle periodiche riunioni di riesame in cui vengono definite opportune azioni di miglioramento e la loro priorità.

Documenti applicabili
P 9.3.1 Riesame della direzione
Allegato – Politiche protezione dei dati personali