MANUALE DELLA PRIVACY

Elaborato in base al D.Lgs 30 giugno 2003, n. 196

in

"MATERIA DI PROTEZIONE DEI DATI PERSONALI"

PRESENTAZIONE MANUALE

0.1. **SCOPO DEL MANUALE**

0.2. **STRUTTURA E GESTIONE DEL MANUALE**

0.3. **IL TESTO UNICO IN MATERIA DI TRATTAMENTO DEI DATI PERSONALI –**

D. LSG. 30/06/2003 N. 196

0.4. **PRINCIPALI DEFINIZIONI**

0.5. **ALLEGATI**

VERIFICA				ATTUAZIONE		
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

0.1. SCOPO DEL MANUALE

Il presente MANUALE sul trattamento dei dati personali è stato redatto sulla base del disposto del 19° comma del Disciplinare tecnico del Nuovo Testo Unico in materia di trattamento di dati personali del 30.6.2003 n.196 ed è stato elaborato a seguito di una dettagliata analisi dei rischi del trattamento potenzialmente presenti e ciò per individuare, analizzare ed applicare un complesso di contromisure di diverso genere per l'abbattimento dei rischi e per garantire la massima sicurezza in ordine al trattamento dei dati personali.

Il documento è stato compilato dal Titolare unitamente al Responsabile del Trattamento in adempimento di quanto previsto dall'art.29 del D.Lgs. 196/2003 in ordine all'esperienza, capacità ed affidabilità del citato soggetto e dalla idonea garanzia da esso fornita del pieno rispetto delle vigenti disposizioni in materia di trattamento, "ivi compreso il profilo relativo alla sicurezza".

Il presente documento deve essere aggiornato ogni anno e sottoposto a revisione entro e non oltre il 31 marzo di ogni anno e, comunque, tempestivamente modificato a cura del Titolare del Trattamento e del Responsabile del Trattamento qualora nel corso del trattamento annuale

dovessero insorgere anomalie applicative delle misure di sicurezza adottate o qualora dovessero ravvisarsi inadeguatezze protettive derivanti anche da nuovi rischi.

Al fine della migliore applicazione della legge sulla Privacy, il Titolare ed il Responsabile del Trattamento dei dati personali hanno individuato un organo non previsto dalla legge ma ritenuto utile ed opportuno per il raggiungimento dell'effettiva applicazione pratica della legge in considerazione della peculiare organizzazione amministrativa interna e dei vari ruoli presenti nella specifica realtà .

Tale organo è stato chiamato "Gruppo Privacy" e, nel caso in cui venga nominato, è stato preventivamente ritenuto come garantista della maggiore tutela degli interessati cui si riferiscono i dati in possesso dell’Ente nonché per creare e sostenere la cultura della privacy tra tutti coloro che trattano dati personali per ragioni connesse al raggiungimento delle

finalità stesse.

Tali finalità sono evidenziate nel presente manuale che descrive e definisce:

- le Responsabilità, nonché le istruzioni impartite ai soggetti preposti al Trattamento (Responsabili del trattamento, incaricati del trattamento, eventuali componenti del Gruppo Privacy, ecc.);
- le azioni per la gestione dei rischi e per l'adozione delle misure di sicurezza, ai sensi del disciplinare tecnico del D.Lgs n.196/2003;
- gli adempimenti necessari, sia a rilevanza cd. interna che esterna;
- individua le procedure per la tutela della riservatezza dei dati personali in rapporto all'assetto organizzativo dell'Ente.

Riferimenti normativi

Articolo	Norma	Descrizione
Art. 11	D.Lgs. 196/03	Modalità di raccolta e requisiti dei dati personali
Art. 15	D.Lgs. 196/03	Danni cagionati per effetto del Trattamento
Art. 31-36	D.Lgs. 196/03	Misure di Sicurezza dei dati
Art. 169	D.Lgs. 196/03	Omessa adozione di misure minime di sicurezza
Disciplinare Tecnico in materia di Misure Minime di Sicurezza (Allegato B D.Lgs.196/03)		

0.2. STRUTTURA E GESTIONE DEL MANUALE

Il presente Manuale è strutturato in sezioni. Ogni sezione presenta degli allegati, che sono contrassegnati con la sigla **MAS.** Le Sezioni sono numerate in ordine progressivo: da 01 a "0X". Gli Allegati sono individuati in modo univoco con la sigla **MAS** seguita da due coppie di numeri (es. **MAS04.01**):

- la prima coppia indica la Sezione del Manuale di riferimento;
- la seconda coppia il numero progressivo del documento, qualora una sezione presenti più di un allegato.

Sulla copertina di ogni sezione oltre all'indice è riportata una tabella che evidenzia lo stato delle verifiche, fatte dall'eventuale ***Gruppo Privacy*** e l'approvazione delle eventuali modifiche da adottarsi dal:

- Titolare per l'adozione o la modifica del presente manuale;
- Responsabile pro - tempore del trattamento dei dati personali con riferimento agli aspetti organizzativi, tra questi compresi i provvedimenti tendenti all'adozione delle misure minime di sicurezza.

Il presente manuale deve essere tenuto ed aggiornato dal Responsabile del Trattamento e, in caso di nomina, dal Gruppo Privacy.

Tali soggetti hanno l'obbligo di curare:

- la revisione periodica, formulando le proposte di modificazione e integrazione al Titolare ed al Responsabile del Trattamento che potranno approvare;
- la corretta applicazione e conservazione del manuale;
- la distribuzione del medesimo, anche per via telematica.

Lo stato di revisione del documento è riportato in basso a sinistra, nella griglia di intestazione, contraddistinto da un numero progressivo e dalla data di approvazione. Il manuale è uno strumento indispensabile per la corretta gestione dei processi di Trattamento dei dati personali e per l'individuazione delle azioni correttive da adeguare a futuri trattamenti di dati ed in particolare all'ambito di comunicazione dei dati personali medesimi.

0.3. IL TESTO UNICO IN MATERIA DI TRATTAMENTO DI DATI PERSONALI

D.Lgs. 30 giugno 2003 n.196

La nuova disciplina relativa al trattamento dei dati personali è stata interamente modificata ed è attualmente disciplinata dal D.Lgs. 30 giugno 2003 n.196, cd. Testo Unico in materia di trattamento di dati personali o altrimenti conosciuto come legge sulla privacy che accorpa in un'unica disposizione normativa la complessa materia dei dati personali e di quella concernente le misure minime di sicurezza.

Tale nuova legge evidenzia la maturata sensibilità e la crescente attenzione alla materia e soprattutto alla protezione dei dati personali nell'ottica della maggiore tutela dei diritti degli interessati al trattamento.

Quanto sopra è altresì sancito dall'art. 1 del D.lgs 196/2003 secondo il quale Chiunque ha diritto alla protezione dei dati personali che lo riguardano nonché dal successivo Art. 2 che garantisce che il trattamento dei dati personali si deve svolgere nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali nel pieno rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte dei titolari del trattamento.

0.4. PRINCIPALI DEFINIZIONI

Per la maggiore comprensione del manuale si ritiene opportuno riportare le principali seguenti definizioni di ordine generale così contraddistinte:

a) Definizioni generali della materia della PRIVACY previste dal D.Lgs. n.196/2003:

"trattamento", qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati;

"titolare del trattamento dei dati personali", la persona fisica, la persona giuridica, la pubblica

amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

"dato personale", qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale;

"dati identificativi", i dati personali che permettono l'identificazione diretta dell'interessato;

"dati sensibili", i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;

"dati giudiziari", i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del d.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale;

"responsabile del trattamento dei dati personali", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali;

"incaricati del trattamento dei dati personali", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"interessato", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

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

"diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

"dato anonimo", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"blocco", la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento;

"banca di dati", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

"Garante", l'autorità di cui all'articolo 153, istituita dalla legge 31.12.1996 n. 675.

b) Definizioni tecniche della materia della PRIVACY previste dal D.Lgs. n. 196/2003:

"comunicazione elettronica", ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un abbonato o utente ricevente, identificato o identificabile;

"chiamata", la connessione istituita da un servizio telefonico accessibile al pubblico, che consente la comunicazione bidirezionale in tempo reale;

"reti di comunicazione elettronica", i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e altre risorse che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, incluse le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi

sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui sono utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

"rete pubblica di comunicazioni", una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico;

"dati relativi all'ubicazione", ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;

"posta elettronica", messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

c) Definizioni sulle misure minime di sicurezza della materia della PRIVACY previste dal disciplinare tecnico allegato al D.Lgs. n. 196/2003:

"misure minime", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31;

"strumenti elettronici", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"autenticazione informatica", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"credenziali di autenticazione", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

"parola chiave", componente di una credenziale di autenticazione associata ad una persona ed a questa nota,

costituita da una sequenza di caratteri o altri dati in forma elettronica;

"profilo di autorizzazione", l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti;

"sistema di autorizzazione", l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente.

Per quanto riportato emerge che i dati personali non sono però solo le informazioni cd. alfanumeriche, ma tutte quelle che si riferiscono ad un soggetto, comunque identificabile: la nozione è volutamente molto ampia e tra questa debbono ricomprendersi anche le immagini ed i suoni (si pensi alla videosorveglianza e alle audio registrazioni, che costituiscono forme di Trattamento di dati personali).

La legge detta una serie di regole procedurali per garantire la tutela delle persone e di altri soggetti da questa attività. Il manuale tiene presenti ed individua trattamenti specifici in relazione alla natura dei dati trattati ed in considerazione della maggiore o minore invasività della sfera più intima degli interessati.

0.5. ALLEGATI

- Elenco allegati Manuale Privacy

Codifica	**Oggetto**
MAS01.01	Nomina Gruppo Privacy (nomina eventuale)
MAS02.01	Scheda operatore/operatori
MAS02.02	Scheda tecnica
MAS02.03	Scheda processo
MAS03.01	Nomina del Responsabile del Trattamento
MAS03.02	Nomina degli incaricati del Trattamento
MAS03.03	Nomina responsabili di area quali incaricati del trattamento
MAS04.01	Documento programmatico sulla sicurezza
MAS04.02	Gestione dei rischi aree e locali
MAS04.03	Gestione dei rischi integrità dei dati
MAS04.04	Gestione rischi trasmissione dati
MAS04.05	Gestione rischi strumenti non automatizzati
MAS04.06	Registro di carico e scarico documentazione
MAS04.07	Dichiarazione di conformità dell'installatore esterno delle misure minime di sicurezza
MAS04.08	Dichiarazione ai sensi dell'art. 180, comma 2, del D.Lgs. n.196/2003 (misure minime di sicurezza) – conservare con data certa -
MAS04.09	Procedura per la gestione delle richieste degli interessati
MAS04.10	Modulo per l'esercizio dei diritti da parte degli interessati
MAS04.11	Nomina responsabile accesso ai locali
MAS04.12	Report Virus
MAS04.13	Report annuale rischi hardware

MAS04.14	Report annuale rischi nelle applicazioni
MAS04.15	Report annuale rischi sistemi operativi
MAS04.16	Report annuale rischio luoghi ove vengono trattati i dati
MAS05.01	Modelli per le informative agli interessati
MAS06.01	Richiesta di azioni correttive e preventive
MAS06.02	Rapporto di non conformità
MAS06.03	Pianificazione di azioni correttive e preventive

3.1. **SCOPO**

3.2. **RIFERIMENTI NORMATIVI**

3.3. **RESPONSABILITÀ**

3.4. **DESCRIZIONE**

3.4.1. La nomina dei Responsabili

3.4.2. Individuazione degli incaricati

3.4.3. Modalità di nomina dei Responsabili

3.4.4. Modalità per l'individuazione degli incaricati del Trattamento

3.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

3.1. SCOPO

Delineare gli adempimenti necessari e le modalità per la nomina dei Responsabili del Trattamento e per l'individuazione degli incaricati per lo svolgimento delle singole operazioni di Trattamento.

3.2. RIFERIMENTI NORMATIVI

Articolo	Norma	Descrizione
Art. 29	D.Lgs n.196/2003	Responsabile del Trattamento dei dati personali
Art. 30	D.Lgs n.196/2003	Incaricati del Trattamento dei dati personali
Art. 11	D.Lgs n.196/2003	Modalità del Trattamento
Art. 17	D.Lgs n.196/2003	Trattamento che presenta rischi specifici
Art. 24	D.Lgs n.196/2003	Fattispecie di Trattamento senza consenso

3.3. RESPONSABILITÀ

Il D.Lgs 30 giugno 2003 n.196 dispone che il responsabile è designato dal titolare facoltativamente e che se designato deve essere individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

L'art. 29 del citato Testo Unico precisa che se necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti e che qualora affidati al responsabile debbono essere analiticamente specificati per iscritto dal titolare.

Il responsabile che effettua il trattamento deve attenersi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, ha l'obbligo di vigilare sulla puntuale osservanza delle disposizioni di legge.

Se designati, i Responsabili del trattamento possono incaricare per iscritto i soggetti che materialmente hanno l'onere di effettuare le operazioni di Trattamento: questi devono operare sotto la loro diretta autorità, attenendosi alle istruzioni impartite.

Titolare e Responsabile devono verificare che gli incaricati abbiano accesso ai soli dati particolari (ossia sensibili o giudiziari), per i quali è stato autorizzato l'accesso che, come tale, deve essere strettamente limitato alle operazioni necessarie e sufficienti allo svolgimento delle operazioni loro affidate.

3.4. DESCRIZIONE

3.4.1. Nomina dei Responsabili

L'art. 29 comma 3 del D.Lgs n.196/2003 consente al Titolare di nominare uno o più Responsabili del Trattamento anche con suddivisione di compiti. Qualora si voglia procedere alla nomina occorrerà designare soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, ivi compreso il profilo relativo alla sicurezza.

Conseguentemente alla nomina il Responsabile dovrà procedere al Trattamento attenendosi alle istruzioni impartite dal Titolare il quale, anche attraverso verifiche periodiche conserva una sorta di corresponsabilità del trattamento da esercitarsi mediante la vigilanza sulla puntuale osservanza delle disposizioni di cui al comma 1 e delle proprie istruzioni.

3.4.2. Individuazione degli incaricati

Il problema delle comunicazioni di dati si pone nei confronti di qualsiasi soggetto che conosca dati personali, e sia diverso dall'interessato, trovandosi, quindi, in posizione di terzietà rispetto al rapporto Titolare - interessato. La legge sulla privacy prevede che non si considera comunicazione la conoscenza dei dati personali da parte delle persone incaricate per iscritto di compiere le operazioni del Trattamento dal Titolare o dal Responsabile o che operano sotto la loro diretta autorità. L'art. 30 comma 1 del D.Lgs. n.196/2003 precisa che "le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare del Trattamento o del responsabile,attenendosi alle istruzioni impartite".

Si rileva comunque che il Responsabile del Trattamento è una figura facoltativa e che, viceversa, **l'individuazione degli**

incaricati è obbligatoria.

3.4.3. Modalità di nomina dei Responsabili

L'atto di nomina del Responsabile (MAS 03.01) costituisce parte integrante del presentemanuale. Allo scopo è stata predisposta idonea documentazione con la specificazione analitica, per iscritto, dei compiti assegnati al Responsabile di cui l'originale deve essere conservato in allegato ed una copia consegnata al Responsabile del Trattamento.

La nomina deve essere espressamente accettata dal soggetto che assumerà tale qualifica. Anche a tali Responsabili esterni, definibili anche Responsabili del Trattamento in Out-sourcing, deve essere consegnata la lettera con la specificazione analitica dei compiti assegnati e delle istruzioni relative (MAS 03.02), costituenti parte integrante dell'atto di conferimento. Periodicamente, l'RdT, coadiuvato dai membri del Gruppo Privacy qualora lo stesso sia stato nominato, oppure da personale all'uopo delegato, deve procedere al controllo sulle attività svolte dagli Incaricati.

Inoltre, è previsto che sempre periodicamente il Responsabile debba presentare una relazione sulle attività svolte, segnalando non conformità, necessità di modificazioni o di integrazioni dei compiti e delle istruzioni impartite, nonché le necessità sotto il profilo dell'adozione di misure di sicurezza idonee, ai sensi degli artt. da 34 a 36 del Testo Unico in materia di trattamento di dati personali. **3.4.4. Modalità per l'individuazione degli incaricati.**

- favorire la consapevolezza dei soggetti, cercando di renderli edotti sugli obblighi loro assegnati;
- responsabilizzare i medesimi soggetti per applicare tutte le precauzioni e le cautele necessarie per un legittimo Trattamento dei dati personali. Quanto detto serve a far maturare la cultura del rispetto dell'interessato e della sua riservatezza ed anche a far sì che ogni incaricato deve conoscere e trattare i dati strettamente necessari all'assolvimento dei compiti assegnati. In particolare il Nuovo Testo Unico in materia di trattamento dei dati personali ha dato maggior risalto al principio del "need to know", il definendo quali informazioni un operatore deve "conoscere", limitando con ciò l'accesso e quindi, la conoscenza dei dati. Quanto precede necessita l'assunto che maggiore è il numero di soggetti che hanno accesso ai dati, maggiori sono i rischi di identificazione dell'interessato e, pertanto, delle potenziali violazioni della riservatezza del medesimo.

  In tale ottica si ritiene necessaria la seguente disposizione:

1. L'accesso alle diverse tipologie di dati è consentito ai soli incaricati del Trattamento, preposti alle specifiche fasi dell'attività amministrativa, secondo il principio della pertinenza dei dati di volta in volta trattati.
2. Gli incaricati del trattamento sono individuati come appresso:

a) creazione di profili dei soggetti preposti alle operazioni di Trattamento, mediante l'utilizzo delle informazioni raccolte con la scheda operatore/operatori (MAS 02.01);
b) una volta delineati i profili, si dovrà compilare la modulistica per l'individuazione e la nomina degli incaricati (MAS 03.03 e MAS 03.04);
c) Ogni soggetto incaricato dovrà essere consegnata la lettera di incarico, redatta in duplice copia, di cui una deve essere restituita al Responsabile, opportunamente firmata per ricevuta e da conservarsi agli atti.

3.5. ALLEGATI

MAS 03.01 - Modulo per la nomina dei Responsabili del Trattamento

MAS 03.02 - Modulo per la nomina di Responsabili esterni del Trattamento

MAS 03.03 - Nomina degli incaricati del Trattamento

MONITORAGGIO DEL PROCESSO DI TRATTAMENTO

2.1. **SCOPO**

2.2. **RIFERIMENTI NORMATIVI**

2.3. **RESPONSABILITÀ**

2.4. **DESCRIZIONE**

2.4.1. Le fasi del processo

2.4.2. Le schede per il monitoraggio

2.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

2.1. SCOPO

Scopo della presente sezione è descrivere le fasi del processo di Trattamento dei dati personali e le azioni di monitoraggio dello stesso, al fine della predisposizione degli adempimenti necessari aventi rilevanza sia interna che esterna.

2.2. RIFERIMENTI NORMATIVI

Articolo	Norma	Descrizione

Art. 2D.Lgs.n196/2003Finalità e definizioni Art. 11D.Lgs.n196/2003 Modalità di trattamento dei dei dati personali Art. 22 D.Lgs.n196/2003Principi applicabili al trattamento di dati sensibili D.P.R.

2.3. RESPONSABILITÀ

L'attività di monitoraggio è svolta in via prioritaria dal Responsabile del Trattamento e, in caso di nomina unitamente, al Gruppo Privacy.

Le risultanze del Trattamento dei dati personali posti in essere dal Responsabile/i dovranno essere regolarmente comunicate a cadenza periodica al Gruppo Privacy.

Rimane salvo il diritto di ogni Responsabile chiedere al Titolare la convocazione del Gruppo Privacy qualora rinvenisse anomalie nel Trattamento dei dati affidati alla sua Responsabilità e/o qualora si verificassero situazioni di eccezionali gravità che ne impongono l'immediata convocazione.

2.4. DESCRIZIONE

Il procedimento di Trattamento dei dati personali è caratterizzato da tre fasi:

1. **INPUT** - raccolta dati presso l'interessato o richiesta di comunicazione di dati personali a enti o persone giuridiche;
2. **BLACK-BOX** - (ossia il complesso delle operazioni di Trattamento interne);
3. **OUTPUT** - è la fase della comunicazione e/o della diffusione.

2.4.1. Le fasi del processo

La legge definisce il Trattamento di dati come qualunque operazione o complesso di operazioni svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la: Raccolta; Registrazione; Organizzazione; Conservazione; Elaborazione; Modificazione; Selezione; Estrazione; Raffronto; Utilizzo; Interconnessione; Blocco; Comunicazione; Diffusione; Cancellazione; Distruzione dati. La raccolta dei dati può essere effettuata o direttamente presso l'interessato o presso terzi, che conferiscono dati relativi a interessati diversi dalla propria persona. Al momento della raccolta dei dati occorre fornire all'interessato, o al terzo, presso il quale i dati sono raccolti, una informativa, secondo quanto previsto dall'art. 13 del Testo Unico in materia di trattamento di dati personali di cui al D.Lgs. n.196/2003 che specifica, infatti, che "'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa le finalità e le modalità del trattamento cui sono destinati i dati"..;

L'attività di monitoraggio è finalizzata ad ottenere l'insieme di tutti gli elementi e le fasi caratterizzanti l'intero Trattamento tenendo ben presente che la legge sulla privacy prevede due regimi di legittimazione diversi, a seconda della natura dei soggetti titolari del Trattamento:

- se a procedere al Trattamento è un soggetto privato (cui sono equiparati gli enti pubblici economici), questo deve chiedere preliminarmente il consenso all'interessato, salvo i casi di esclusione espressamente previsti dal legislatore;
- per i soggetti pubblici**,** vige il principio di finalità istituzionale: essi possono trattare solo i dati che siano necessari per lo svolgimento di funzioni istituzionali.

Questa scelta è una conseguenza del principio di legalità, che caratterizza l'attività amministrativa, per cui si è voluto evitare di condizionare l'azione al consenso degli interessati. Peraltro questa scelta, fatta dal nostro legislatore, appare pienamente compatibile con quanto previsto, in sede comunitaria, dall'art. 7 della direttiva 95/46/CE.

1) Per quanto riguarda **l'input** non ci sono particolari problemi, atteso che le informazioni pervergano da fonti istituzionali e /o direttamente dagli interessati.

2) Per quanto riguarda la **black-box** sono due le specie di operazioni, che interessano il Trattamento interno:

- **quelle statiche:** registrazione, conservazione, organizzazione, blocco, cancellazione, distruzione;
- **quelle dinamiche:** elaborazione, modificazione, selezione, estrazione, raffronto, utilizzo, interconnessione.

La differenza riguarda la circostanza che:

- **le operazioni statiche** non alterano il dato che, nel suo insieme, rimane inalterato;
- **le operazioni dinamiche** comportano, invece, un intervento sulle informazioni, che perdono la loro originaria

forma dando vita ad informazioni cd. di secondo livello, che possono essere profondamente diverse da quelle raccolte. Ed è per tale ultima fattispecie che la legge riconosce i diritti dell'interessato (ai sensi degli articoli 7, 8 e 9 del D.Lgs. 196/2003) finalizzando il controllo sul Trattamento avente ad oggetto i propri dati.

3) Infine le operazioni di **output**, si individuano nella:

- **comunicazione,** che riguarda il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;
- **diffusione,** ossia il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

La differenza fra queste due operazioni è data dalla determinatezza o meno del soggetto destinatario delle informazioni e nella specifica fattispecie la legge prevede che:

1. l'interessato deve essere informato sulle categorie di soggetti ai quali i dati possono essere comunicati e sull'ambito di diffusione dei dati medesimi;

2. se i dati (di natura comune) sono trattati da un **soggetto privato o da un Ente pubblico economico** per poter essere trasferiti ad un terzo occorre il consenso dell'interessato, salvo i casi di esclusione, previsti dalla legge;
3. se i dati (sempre di natura comune) sono trattati da un **soggetto pubblico** per essere comunicati o diffusi a soggetti privati (come destinatari) **occorre una previsione specifica di legge o di regolamento;**
4. se i dati trattati sono di natura **sensibile** per poter essere trasferiti a terzi non previsti istituzionalmente occorre rispettivamente il consenso scritto dell'interessato, quando il Titolare sia un soggetto privato; **una espressa autorizzazione di legge, nel caso dei soggetti pubblici.**

Si rinvia comunque alla sezione 05 per maggiori approfondimenti al riguardo.

2.4.2. Le schede per il monitoraggio

Data la complessità gli adempimenti previsti dal Testo Unico n.196/2003 in materia di trattamento di dati personali è stato ritenuto indispensabile procedere ad una azione di monitoraggio delle attività di Trattamento svolte al fine dell'ottenimento di un quadro generale dei trattamenti e della successiva verifica della compatibilità della situazione reale con le previsioni normative.

In particolare il Responsabile del Trattamento dei dati personali ed in caso di nomina il Gruppo Privacy, dovrà vagliare tre schede di monitoraggio:

1. scheda operatore/operatori (MAS 02.01);
2. scheda tecnica (MAS 02.02);
3. scheda di processo (MAS 02.03).

- **scheda operatore/operatori**: con questa scheda vengono raccolti i dati nominativi, l'area di appartenenza, la funzione e i compiti esercitati da ogni soggetto in seno o per conto dell'Ente. Lo scopo è raccogliere una serie di dati e di informazioni, al fine della creazione dei profili degli incaricati del Trattamento (sezione 03);

- **scheda tecnica**: con questa scheda vengono monitorate le risorse informatiche e telematiche utilizzate, in

modo da avere il quadro completo degli strumenti utilizzati. Inoltre sono state monitorate le banche dati costituite e detenute in seno all'Ente, sia con strumenti elettronici, sia in archivi cartacei. Lo scopo è quello di avere un quadro ben definito per l'adozione delle misure di sicurezza (sezione 04);

- **scheda di processo**: questa scheda riguarda le tre fasi del Trattamento (input - black-box e output). Si tratta di una ricognizione scrupolosa, mediante scheda individuata dal Garante e resa nota con provvedimento del 17.01.2002, al fine di individuare:

- **la finalità del Trattamento**, ossia gli scopi, per cui i dati vengono raccolti e successivamente trattati. Si ricorda che il citato Testo Unico prevede che i fini devono essere determinati, espliciti e legittimi. Inoltre i dati possono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati e che l'art.2 del Testo Unico garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali;

- **la modalità di Trattamento**, ossia gli strumenti che vengono utilizzati per trattare i dati (elettronici o comunque automatizzati, oppure cartacei) e la logica del Trattamento;

- **la natura dei dati trattati** (comuni, sensibili o giudiziari): si è già detto, e sarà approfondito nel corso della sezione 05 del presente manuale, come la tipologia dei dati trattati influisca sulle specifiche regole di legittimazione al Trattamento;

- **l'ambito di comunicazione e diffusione**. In questo caso lo scopo è duplice: verificare il flusso informativo dall'Ente verso l'esterno, monitorando le categorie di soggetti destinatari ovvero l'ambito di diffusione; monitorare le coperture normative, per le operazioni di output.

Per quanto sopra descritto ed al fine di adempiere ai vari obblighi previsti dal D.Lgs. n.196/2003 è stata posta particolare attenzione a questa fase "preliminare" per conseguire più agevolmente gli obiettivi imposti.

Dall' attività di monitoraggio scaturiscono i seguenti benefici:

1 la possibilità di avere sempre sotto controllo, nei limiti del possibile, il processo di Trattamento e di potere rispondere alle richieste dell'interessato che eserciti i diritti che la Legge gli riconosce e al Garante per la Privacy in caso di controlli e ispezioni;

2 cogliere il valore aggiunto della legge in termini di organizzazione e di verifica dei flussi informativi interni all'Ente e da questo verso l'esterno;

3 infine il coinvolgimento di tutto il personale che acquisisce e consolida una cultura del rispetto della riservatezza degli interessati e, quindi, il sicuro miglioramento dei rapporti con la propria utenza e con quanti verranno in contatto con l'Ente.

2.5. ALLEGATI

MAS 02.01 - Scheda operatore/operatori
MAS 02.02 - Scheda tecnica
MAS 02.03 - Scheda processo

GRUPPO PRIVACY

1.1. **SCOPO**

1.2. **RIFERIMENTI NORMATIVI**

1.3. **RESPONSABILITÀ**

1.4. **DESCRIZIONE**

1.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

1.1. SCOPO

Delineare compiti e responsabilità dell'eventuale Gruppo Privacy.

1.2. RIFERIMENTI NORMATIVI

Il Gruppo Privacy non è un organo previsto dal Nuovo Testo Unico in materia di protezione dei dati personali di cui al D.Lgs. n.196/2003. Tuttavia, considerati gli obblighi della Legge sulla Privacy e la necessità di procedere al meglio ad una serie di adempimenti, sia a rilevanza cd. interna, sia esterna, Il Titolare del trattamento dati ha ritenuto opportuno delineare i tratti ed i requisiti al fine della sua eventuale costituzione.

1.3. RESPONSABILITÀ

Qualora nominato, spetterà al Titolare del Trattamento, ai sensi dell'art. 4 lett. f) del D.Lgs. n. 196/2003, anche attraverso un suo delegato, presiedere, coordinare, controllare e convocare il Gruppo Privacy.

1.4. DESCRIZIONE

In caso di nomina, la costituzione del Gruppo Privacy sarà effettuata dal RdT dopo l'approvazione del presente manuale in considerazione del fatto che occorre innanzitutto procedere ad una operazione di monitoraggio delle attività di Trattamento di dati personali.

Qualora venga nominato il gruppo dovrà essere costituto da soggetti aventi diverse professionalità:

1.personale amministrativo: soggetti che hanno una qualificata formazione giuridica e che possiedono competenze gestionali della legge sul trattamento dei dati personali e delle problematiche giuridiche ad essa sottese. A tali soggetti sono stati assegnati incarichi particolari in relazione all'applicazione D.Lgs. n.196/2003 che costituiscono parte integrante di questo manuale

negli appositi allegati;

2.personale con competenze gestionali: trattasi di soggetti a cui è demandata la revisione delle procedure gestionali degli adempimenti ed il monitoraggio dei flussi informativi interni e verso l'esterno. In questa ottica, fanno parte del Gruppo privacy i Responsabili incaricati delle diverse posizioni organizzative e/o settori di intervento.

3.personale tecnico-informatico: è il Responsabile dei servizi informatici e automatizzati che possiede una idonea formazione tecnica ed apporta il proprio contributo soprattutto in relazione alla valutazione dei rischi e all'adozione delle misure di sicurezza.

4.rappresentanti dei settori:

a)SAISH per la coordinazione delle attività di sostegno per lo svolgimento delle funzioni assistenziali.

b) SAS per la coordinazione delle attività di sostegno per lo svolgimento delle funzioni assistenziali

5. **rappresentanti del settore formazione per le attività di formazione previste.**

Al Gruppo Privacy eventualmente nominato vengono assegnati i seguenti compiti:

1. predisposizione delle schede da utilizzare per il monitoraggio delle attività di trattamento, di cui alla sezione 02 del presente manuale;
2. elaborazione dei dati raccolti presso il settore SAISH con le schede, di cui al punto precedente;
3. segnalazione agli organi competenti delle azioni SAS Formazione;
4. valutazione delle misure di sicurezza ritenute necessarie, che vengono proposte al Titolare del Trattamento che provvederà alla eventuale adozione;

5. predisposizione dei moduli per le informative agli interessati e per il consenso al Trattamento (sezione 05);
6. programmazione di attività di formazione diretta e di informazione del personale preposto allo svolgimento delle operazioni di Trattamento;
7. cura e aggiornamento del presente manuale;
8. predisposizione delle condizioni per la consultazione e per l'eventuale distribuzione del manuale e degli aggiornamenti, utilizzando anche strumenti telematici;
9. segnalazione delle innovazioni di carattere normativo e delle necessarie modificazioni da apportare al presente manuale e alla modulistica allegata;
10. vigilanza sull'attività svolta dai soggetti incaricati del Trattamento e sul rispetto delle istruzioni loro impartite;
11. effettuazione di attività di audit e di controllo sulla rispondenza delle attività svolte rispetto a quanto previsto dalla legge e dalla documentazione dell'Ente;
12. attività di report sulle non conformità riscontrate;
13. revisione periodica della modulistica;
14. raccolta di quesiti di interesse sulla materia della privacy;
15. relazione periodica sulle attività di Trattamento con particolare riferimento al problema del rapporto tra diritto di accesso e tutela della riservatezza ai sensi degli articoli 59, 60 e 61 del D.Lgs n.196/2003;

Per quanto sopra, l'eventuale nomina del Gruppo Privacy garantirebbe la migliore gestione degli adempimenti per l'osservanza della legge sulla Privacy.

1.5. ALLEGATI

MAS 01.01 Nomina Gruppo Privacy

AZIONI CORRETTIVE E DI MIGLIORAMENTO

6.1. **SCOPO**

6.2. **RIFERIMENTI NORMATIVI**

6.3. **RESPONSABILITÀ**

6.4. **DESCRIZIONE**

6.4.1. Attività di vigilanza e ispettive

6.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

6.1. SCOPO

Descrivere le modalità per lo svolgimento delle operazioni di vigilanza, al fine del controllo del rispetto delle disposizioni di legge e delle istruzioni impartite ai Responsabili e agli incaricati.

Descrivere altresì le azioni per apportare misure correttive, per perseguire il miglioramento continuo del sistema di Trattamento dei dati in seno all' Ente e per la programmazione degli interventi di formazione.

6.2. RIFERIMENTI NORMATIVI

Articolo	**Norma**	**Descrizione**
Art. 29	D.Lgs. n.196/2003	Responsabile del trattamento
Art. 11	D.Lgs. n.196/2003	Modalità di trattamento e requisiti dei dati
Art. 30	D.Lgs. n.196/2003	Incaricati del Trattamento

6.3. RESPONSABILITÀ

Il Titolare del trattamento, qualora venga nominato, delega il Gruppo Privacy a svolgere le attività di vigilanza sull'operato degli incaricati del Trattamento.

Tale gruppo unitamente al responsabile ha l'obbligo di riferire in sede di conferenza sul rispetto delle istruzioni impartite e sulla necessità di apportare modifiche al presente Manuale e alla modulistica in uso.

I singoli Responsabili devono:

- ottemperare alle eventuali problematiche conseguenti alle richieste avanzate dall'interessato ai sensi dell'art. 7, riferendo poi al Titolare del trattamento o, in caso di nomina al Gruppo Privacy, nella relazione periodica sull'andamento delle attività di Trattamento e sulle correlative azioni correttive che si rendessero necessarie. (In caso di nomina sarà cura del Gruppo Privacy riferire al RdT);
- programmare iniziative periodiche di formazione degli incaricati.

6.4. DESCRIZIONE

Secondo la norma ISO 8402 per azione correttiva (AC) si intende un'azione intrapresa per eliminare le cause di non conformità, difetti o altre situazioni non desiderate, al fine di eliminarne il ripetersi.

Le AC possono comportare modifiche di procedure e di sistemi al fine di ottenere un miglioramento della qualità del processo (nel nostro caso del Trattamento dei dati personali).

Occorre distinguere però tra correzione e azione correttiva:

- il termine correzione si riferisce ad azioni quali riparazione, rilavorazione o ripristino e riguarda il Trattamento di una non conformità;
- l'AC si riferisce all'eliminazione delle cause che hanno generato una non conformità.

Le azioni preventive (AP) sono intraprese per eliminare le cause di potenziali non conformità, difetti o altre situazioni non desiderate, al fine di prevenirne il verificarsi.

Tali AP possono comportare modifiche di procedure e di sistemi al fine di ottenere un miglioramento della qualità in ogni fase del processo.

L'apertura di una AC-AP (MAS 06.01) si può avere in seguito alle informazioni derivanti dai rapporti delle verifiche ispettive interne, delle non conformità, dei reclami e delle indagini conoscitive, dell'analisi dei processi e del riesame della direzione.

In caso di nomina il Gruppo Privacy si riunisce periodicamente e deve provvedere alla verifica delle attività connesse al Trattamento riferendo al RdT su eventuali non conformità riscontrate (MAS 06.02).

Sarà quindi compito del Gruppo Privacy segnalare le eventuali necessità di adottare delle AC o delle AP, secondo le modalità, che sono definite in apposita procedura.

6.4.1. Attività di vigilanza e ispettive

Il Responsabile del Trattamento o, in caso di nomina il Gruppo Privacy, all'inizio di ogni anno scolastico programma l'attività stabilendo gli obiettivi da perseguire nell'anno.

Inoltre, in occasione delle riunioni del Gruppo Privacy, o, in assenza di tale organo, da parte del responsabile del trattamento, dovrà essere redatto un rapporto sull'andamento delle attività svolte, segnalando in particolare le non conformità riscontrate e le azioni correttive e preventive che si intendono intraprendere. (MAS 06.03)

Le azioni devono essere comunicate, comunque, al Titolare del RdT, esaminate ed eventualmente approvate.

Spetterà al Responsabile o all'eventuale Gruppo Privacy individuare, analizzare e predisporre gli interventi correttivi necessari. (MAS 06.03)

In sede di conferenza periodica del Gruppo Privacy vengono esaminate e discusse le non conformità riscontrate e segnalate le azioni necessarie intraprese o da intraprendere. (MAS 06.02)

I Responsabili ai quali sono state effettuate le segnalazioni, devono a loro volta programmare le attività di controllo sull'operato degli incaricati, verificando in particolare modo:

- il rispetto delle istruzioni, anche mediante visite ispettive a sorpresa, opportunamente programmate;
- il rispetto delle misure di sicurezza, sia minime, sia idonee.

6.5. ALLEGATI

MAS 06.01 Richiesta di azioni correttive e preventive

MAS 06.02 Rapporto di non conformità

MAS 06.03 Pianificazione di azioni correttive e preventive

ADEMPIMENTI A RILEVANZA INTERNA

4.1. **SCOPO**

4.2. **RIFERIMENTI NORMATIVI**

4.3. **RESPONSABILITÀ**

4.4.1. **ADOZIONE DI MISURE DI SICUREZZA**

4.4.2. **CONTROLLO DEL PROCESSO DEL TRATTAMENTO**

4.4.3. **IL CONTROLLO DELLA QUALITA' E DELLA QUANTITA' DEI DATI TRATTATI**

4.4.4. **ADOZIONE DI PROCEDURE PER FAVORIRE L'ESERCIZIO DEI DIRITTI DA PARTE DELL'INTERESSATO.**

4.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz	Firma
	GP	Vedi Relazione n°			TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

4.1. SCOPO

Scopo della presente sezione è descrivere gli adempimenti necessari cd. a rilevanza interna e le azioni che l'Ente pone in essere.

4.2. RIFERIMENTI NORMATIVI

Articolo	Norma	Descrizione

Art. 11D.Lgs. 196/2003Modalità del trattamento e requisiti dei dati personali Art. 7D.Lgs. 196/2003Diritti dell'interessato Art. 31D.Lgs. 196/2003Obblighi di Sicurezza dei dati Art. 15D.Lgs. 196/2003Danni cagionati per effetto del Trattamento di dati personali Art. 33D.Lgs. 196/2003 Misure minime di sicurezza Art.2050Codice civile Responsabilità oggettiva Art. 34D.Lgs. 196/2003Trattamenti con strumenti elettronici Art. 35D.Lgs. 196/2003Trattamenti senza l'ausilio di strumenti elettronici Art. 36D.Lgs. 196/2003

Adeguamento Allegato B D.Lgs. 196/2003 Disciplinare tecnico per l'individuazione e l'applicazione delle misure minime di sicurezza per il Trattamento dei dati personali.

4.3. RESPONSABILITÀ

Gli adempimenti previsti dal D.Lgs. n.196/2003 debbono essere adottati dal Titolare del Trattamento per conto dell'Ente. In adempimento di quanto sopra il Titolare nomina i Responsabili del trattamento ai quali è demandata l'adozione delle misure minime di sicurezza e la valutazione delle misure idonee da proporre. Inoltre, sempre ai Responsabili sono assegnati compiti di verifica dei profili qualitativi e quantitativi dei dati oggetto di Trattamento e di controllo del "processo" di Trattamento, con obbligo di riferire, con revisione periodica, in sede di conferenza del Gruppo Privacy (se nominato).

Nel caso di mancata nomina del Gruppo Privacy o di revoca dello stesso, la relazione periodica dovrà essere presentata al Titolare.

Nonostante la possibilità di designare i Responsabili, il Titolare non può delegare a questi i poteri che la legge gli riconosce, e di conseguenza non può dirsi completamente deresponsabilizzato, con particolare riferimento all'obbligo di adozione di misure di sicurezza.

4.4. DESCRIZIONE

Gli adempimenti definiti a rilevanza interna riguardano:

1. l'adozione di misure di sicurezza;
2. il controllo del processo di Trattamento;
3. il controllo della qualità dei dati personali trattati;
4. l'adozione di procedure per favorire l'esercizio dei diritti da parte dell'interessato.

4.4.1. Adozione di misure di sicurezza

Gli articoli da 33 a 36 del D.Lgs. n.196/2003 evidenziano le misure minime di sicurezza ed il conseguente obbligo di adozione delle dette misure di sicurezza a protezione di dati e informazioni.

In precedenza la legge 547/93, in tema di computer crimes, introducendo nel codice penale alcune fattispecie a tutela di beni informatici e telematici, aveva previsto l'adozione di misure di sicurezza non come obbligo, ma come condizione di punibilità:

- l'art. 615-ter del c.p. punisce la condotta della violazione del cd. domicilio informatico, a condizione che il sistema sia protetto da misure di sicurezza;
- l'art. 615-quater invece sanziona la condotta della detenzione e diffusione abusiva di codici di accesso a sistemi protetti da misure di sicurezza.

Il nuovo Testo Unico in materia di trattamento di dati personali prevede l'obbligo di adozione di idonee misure di sicurezza anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del Trattamento, in modo da ridurre al minimo i rischi:

1 di distruzione o perdita, anche accidentale, dei dati stessi;
2 di accesso non autorizzato;
3 di Trattamento non consentito o non conforme alle finalità della raccolta.

Si tratta di un obbligo che deve essere assolto dal Titolare, il quale può nominare uno o più Responsabili, che devono fornire, ai sensi dell'art. 29 del D.Lgs. n.196/2003, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di Trattamento, compreso il profilo relativo alla sicurezza.

La norma in oggetto deve essere letta congiuntamente all'art. 15 della medesima legge sulla Privacy che, per i casi in cui si cagioni un danno ad altri per effetto del Trattamento (leggasi anche a seguito della mancata adozione di idonee misure di sicurezza), prevede l'obbligo di risarcire il danno ai sensi dell'art. 2050 c.c.

Il richiamo dell'art. 2050 (attività pericolosa) comporta un'inversione dell'onere della prova, per cui in caso di lesione al danneggiato spetterà solo provare il danno e il nesso di causalità tra questo e la mancata adozione di misure idonee.

Ai sensi dell'art. 2050 del c.c. il danneggiante dovrà provare, invece, di aver adottato tutte le misure idonee ad evitare il danno stesso.

Per essere esentato da responsabilità al soggetto titolare del trattamento non basterà fornire la prova negativa di non aver commesso alcuna violazione delle norme di legge o di comune prudenza, ma, viceversa, quella ancora più ardua detta anche positiva consistente nella dimostrazione di aver impiegato ed adottato ogni cura, accorgimento o misura atta ad impedire in concreto l'evento dannoso.

Gli articoli da 33 a 36 del Testo Unico prevedono l'obbligo di adozione delle misure minime di sicurezza che sono ulteriormente individuate dal Disciplinare tecnico di cui all'allegato B del Testo Unico citato: la mancata adozione delle predette misure comporta la responsabilità penale ai sensi dell'art. 169 del D.Lgs. n.196/2003.

Per quanto sopra **sussiste un duplice obbligo per il Titolare e i Responsabili del Trattamento:**

1. adozione di misure idonee di sicurezza in considerazione delle conoscenze tecniche, della natura dei dati, delle specifiche caratteristiche del Trattamento, al fine di ridurre al minimo i rischi connessi al trattamento die dati

personali;

2. adozione delle misure minime di sicurezza la cui omissione comporta sanzioni penali ed amministrative.

Al fine di verificare quali misure siano necessarie, l'Associazione ha provveduto ad adottare una serie di azioni, secondo uno schema logico e una serie di tecniche derivate dal risk-management che si sono concretizzate in una dettagliata individuazione e valutazione dei rischi connessi al Trattamento dei dati personali.

Le fasi, che caratterizzano questo processo, sono tre:

1. **analisi:** attraverso l'uso di apposite check-list (MAS 04.02, MAS 04.03, MAS 04.04, MAS 04.05) sono stati monitorati i rischi per le informazioni trattate, ma anche quelli relativi alle aree e ai locali e alle modalità di Trattamento, in particolare ai collegamenti in rete;
2. **valutazione:** una volta evidenziati i rischi, presenti in ogni unità di Trattamento si è provveduto ad assegnare ad ogni fattore di rischio un indice numerico relativo alla frequenza e all'incidenza del rischio stesso: questa valutazione può essere fatta sia in termini quantitativi, sia qualitativi. Le modalità seguite sono illustrate nel documento programmatico sulla sicurezza, in allegato al manuale (MAS 04.01);
3. **trattamento:** dopo aver ottenuto il fattore rischio, che è dato dal prodotto dell'indice della probabilità del verificarsi dell'evento per quello della gravità del danno, si deve procedere all'adozione delle misure specifiche di sicurezza per ogni fattore. È ovvio che occorre adottare le misure previste dal disciplinare tecnico del D.Lgs. n.196/2003, che sono stratificate a seconda della tipologia di strumenti utilizzati e della natura dei dati trattati.

Per far questo si è proceduto a verificare i dati raccolti, in sede di monitoraggio, con le schede tecniche (MAS 02.02). Inoltre, come detto, non basta l'adozione di misure minime, ma occorre adottare anche protezioni idonee.

Al Trattamento di tali dati si procede con particolari modalità e cautele che, per quanto riguarda la conservazione dei dati stessi secondo un profilo statico del Trattamento impone che i dati relativi alla salute siano tenuti separati dai restanti. L'Autorità ha, inoltre, sottolineato che la normativa vigente, pur non arrivando a stabilire un obbligo di assoluta e integrale segretazione dei dati ha introdotto una serie di obblighi e cautele da rispettare nel trattamento dei dati personali.

Per quanto sopra riportato si sottolinea che il Responsabile del Trattamento di dati personali ha l'obbligo di verificare che, qualora gli incaricati debbano comunicare dati di natura sensibile a terzi vengano osservate le cautele previste dal Testo Unico.

4.4.2. Controllo del processo di Trattamento.

In particolare l'art. 11 del D.Lgs. 30 giugno 2003 n.196 prevede che i dati personali oggetto di Trattamento devono essere:

1. trattati in modo lecito e secondo correttezza: ossia in modo conforme rispetto alle norme giuridiche e alle regole informatiche.
1. raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in operazioni di Trattamento.
2. La finalità non può essere determinata per relationem, o con una tale genericità, che permetta un uso plurimo e

imprevedibile dei dati: occorre sempre informare l'interessato degli scopi del Trattamento.

3. conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

4.4.3. Il controllo della qualità e della quantità dei dati trattati

Un altro obbligo, costituente un'assoluta novità per chi tratta dati personali è dato dalla necessità di controllare sia la qualità, sia la quantità dei dati, con riferimento soprattutto alla finalità dei trattamenti.

I dati raccolti e successivamente trattati devono essere:

1. **esatti:** il dato deve riprodurre con esattezza la fonte, che, nel caso di dati sensibili e qualora non sia stata specificamente indicata, si intende rilevata
2. **direttamente presso l'interessato:** a riguardo le istruzioni impartite agli incaricati e, specificatamente atteso gli stessi devono essere armonizzati, eliminando discrasie e divergenze.
3. **aggiornati:** l'aggiornamento riguarda, in particolare, l'esattezza ed è richiesto solo se necessario.
4. **pertinenti:** è la caratteristica fondamentale del dato e costituisce un elemento fondamentale per la gestione soprattutto degli output.
5. **non eccedenti** le finalità per le quali gli stessi vengono raccolti.
6. **completi:** attiene sia alla finalità della banca dati, sia ai dati stessi memorizzati.

4.4.4. L'adozione di procedure per favorire l'esercizio dei diritti da parte dell'interessato

Per facilitare l'esercizio dei diritti dell'interessato ai sensi dell'articolo 7 del D.Lgs. n. 196/2003 l'Ente ha adottato una apposita procedura (MAS 04.09), disciplinante le modalità per rispondere tempestivamente alle richieste avanzate dagli interessati.

Inoltre è stato predisposto un modulo (MAS 04.10), che gli interessati possono richiedere per l'esercizio delle diverse facoltà all'uopo previste.

4.5. ALLEGATI

MAS 04.01 - Documento programmatico sulla sicurezza

MAS 04.06 - Registro di carico e scarico documentazione

MAS 04.09 - Procedura per la gestione delle richieste degli interessati

MAS 04.10 - Modulo per l'esercizio dei diritti da parte degli interessati

MAS 04.11 - Modulo nomina incaricato accesso ai locali ove avviene il trattamento

ADEMPIMENTI A RILEVANZA ESTERNA

5.1. **SCOPO**

5.2. **RIFERIMENTI NORMATIVI**

5.3. **RESPONSABILITÀ**

5.4. **DESCRIZIONE**

5.4.1. **INFORMATIVE ALL'INTERESSATO**(art. 13 D.Lgs. n. 196/2003)

5.4.2. **IL CONSENSO PER IL TRATTAMENTO DEI DATI SANITARI**

5.5. **ALLEGATI**

VERIFICA						
Data	Funz.	Modifica	Firma	Data	Funz.	Firma
	GP				TDT	

GP = Gruppo Privacy

TDT = Titolare del Trattamento

5.1. SCOPO

Lo scopo della presente sezione è descrivere:

- le modalità utilizzate per la predisposizione delle informative agli interessati;
- l'ambito di operatività e le modalità per la predisposizione dei moduli per il consenso dell'interessato al Trattamento dei dati sensibili;
- i casi in cui occorre un regolamento per il Trattamento dei dati sensibili.

5.2. RIFERIMENTI NORMATIVI

Articolo	Norma	Descrizione
Art. 1	D.Lgs. n.196/2003	Diritto alla protezione dei dati personali
Art. 2	D.Lgs. n.196/2003	Finalità
Art. 13	D.Lgs. n.196/2003	Informativa

5.3. RESPONSABILITÀ

Il Responsabile del trattamento ed i singoli incaricati sono tenuti a fornire le informative approvate dal Titolare del Trattamento. È in facoltà di ogni Responsabile del Trattamento adattare la modulistica generale a seconda delle proprie esigenze, riferendone nella relazione periodica che viene consegnata al Gruppo Privacy e dallo stesso discussa in sede di conferenza.

Le informative possono essere fornite agli interessati anche dagli incaricati del Trattamento, con libertà di forme decise dai Responsabili. Particolare attenzione deve essere prestata ai moduli per ottenere il consenso degli interessati per il Trattamento dei dati sensibili e per effettuare le comunicazioni di cui all'art. 96 del D.Lgs. n.196/2003 che, comunque, per esigenze di semplificazione e nel pieno rispetto dei diritti degli interessati, sono stati accorpati in un unico documento approvato dal Titolare del Trattamento.

Possono ricevere il consenso al Trattamento anche gli incaricati che provvedono alla elaborazione della documentazione ed alla conservazione della relativa modulistica secondo quanto previsto nelle istruzioni impartite loro (sezione 03 del presente manuale).

5.4. DESCRIZIONE

La legge prevede anche una serie di obblighi di trasparenza, che si sostanziano nella necessità di fornire una pluralità di informazioni all'interessato (art. 13 del D.Lgs. n.196/2003).

L'informativa ha un duplice scopo:

- consentire all'interessato di conoscere l'identità di chi sta trattando dati personali che lo riguardano, per quali finalità e modalità e ciò al fine di controllare ed esercitare i diritti riconosciuti dalla legge in ordine all'utilizzo dei propri dati personali;
- le informazioni servono a rendere edotto, nei casi in cui sia necessario, il soggetto chiamato ad esprimere il proprio consenso al Trattamento liberamente e in forma specifica.

Oltre agli adempimenti relativi alla cd. discovery, tra gli obblighi a rilevanza esterna rientrano anche quelli connessi alla legittimazione al Trattamento che l'Ente pone in essere per finalità istituzionali ad esso proprie. Come si può notare l'insieme dei presupposti del Trattamento non è inspirato ad un criterio proprietario dell'informazione, ma alla circolazione e al controllo dei dati stessi,

assecondando la tesi per cui il rafforzamento della tutela apprestata al soggetto fa sì che le attività diventino più trasparenti. In questa ottica devono essere letti gli adempimenti effettuati in applicazione delle norme in tema di informativa, conservazione dei dati ed adozione delle misure minime di sicurezza strumentali, come detto, per consentire l'esercizio delle facoltà riconosciute all'interessato e degli obblighi del RdT.

5.4.1. Informative all'interessato (art. 13 D.Lgs. n.196/2003)

L'art. 13 del Testo Unico in materia di trattamento dei dati personali indica una serie di elementi che devono essere necessariamente presenti nell'informativa che l'Ente, nella qualità di Titolare del Trattamento dei dati personali deve obbligatoriamente rendere all'interessato o alla persona presso la quale sono raccolti i dati. Quest'obbligo risponde ad una precisa *ratio* dell'adempimento, che come tale, è finalizzato a rendere edotto l'interessato sull'identità dei soggetti istituzionalmente previsti ed appositamente preposti al Trattamento dei dati che lo riguardano e su tutte le circostanze del processo stesso. Premesso che il Trattamento di dati personali effettuato può essere condizionato dal previo consenso dell'interessato in quanto rientrante integralmente nella previsione dei CASI DI ESCLUSIONE DEL CONSENSO e considerata inoltre la possibilità di fornire una informativa anche orale, si ritiene, comunque, necessario

fornire sempre un'informativa scritta all'interessato al fine di permettere il più agevole raggiungimento ed il maggiore soddisfacimento degli scopi previsti nell'art.13 del D.Lgs. n.196/2003 e garantire agli interessati un reale, efficace e trasparente controllo del Trattamento dei dati personali che li riguardano. Per completezza dell'argomento si ricorda comunque che il legislatore ha anche previsto la possibilità di poter omettere le informazioni che siano già note alla persona che fornisce i dati o all'interessato.

Le informazioni da fornire riguardano:

- le finalità e le modalità del Trattamento;
- la natura obbligatoria o facoltativa del conferimento dei dati;
- le conseguenze di un eventuale rifiuto di rispondere;
- i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
- i diritti di cui all'articolo 7 del D.Lgs. n.196/2003;
- il nome, la denominazione o la ragione sociale e il domicilio, la residenza o la sede del Titolare e, se designato, del Responsabile.

Le informative sono redatte in base ai seguenti criteri:

- elementi necessari, che non possono mai mancare in una informativa: l'identità del Titolare, la finalità del Trattamento (ad esempio: finalità connesse all'espletamento del servizio ecc.), il riferimento ai diritti dell'interessato, di cui all'art. 7;
- le informazioni opportune: natura obbligatoria o facoltativa del conferimento e conseguenze di un eventuale rifiuto (si pensi alla necessità, in sede di richiesta di sussidi attuativi dell'attività assistenziale di cui al D.P.R. 24.7.1977 n.616);
- elementi eventuali: categorie di soggetti destinatari di comunicazione anche ai sensi dell'art.96 del D.Lgs. n.196/2003 ed ambito di diffusione dei dati (non necessariamente vengono trasferiti all'esterno in forma nominativa). Inoltre, al fine di consentire all'interessato un buon rapporto con l'Ente, nell'informativa viene indicata il luogo in cui è consultabile un elenco completo e sempre aggiornato dei Responsabili e del presente manuale sul trattamento dei dati personali.

5.4.2. Il consenso per il Trattamento dei dati sensibili

Di norma, come si è avuto modo di evidenziare in precedenza, i soggetti pubblici possono procedere al Trattamento dei dati personali senza dover richiedere il consenso degli interessati.

La legge infatti prevede in generale il principio di finalità istituzionale, con regole particolari a seconda della natura dei dati trattati:

- qualora oggetto del Trattamento siano i dati comuni si evidenzia che il Trattamento è consentito soltanto per lo svolgimento delle funzioni istituzionali, nei limiti stabiliti dalla legge o dai regolamenti: questa regola è strettamente connessa al principio di legalità dell'azione amministrativa;

- per quanto riguarda i dati sensibili e quelli giudiziari, si evidenzia che gli artt. 21 e 22 del testo Unico sulla Privacy prevedono ed autorizzano il trattamento qualora previsto da una espressa disposizione di legge (ancora con riferimento al principio di legalità);

- infine, con riguardo al Trattamento dei dati sensibili il citato Testo Unico prevede che è consentito se autorizzato da espressa disposizione di legge, nella quale siano specificati i tipi di dati che possono essere trattati, le operazioni eseguibili e le rilevanti finalità di interesse pubblico perseguite.

5.5. ALLEGATI

MAS 05.01- Modelli per le informative agli interessati

MAS 05.02- Modelli per la richiesta del consenso al Trattamento dei dati sensibili

NOI PER L'EUROPA – **Gruppo Europeo di Interesse Economico**

ANAFI Associazione MINERVA SAPIENS srl Unipersonale ASCO Associazione FORIF Due sro Rep. Cec