Documento Programmatico Sulla Sicurezza

Redatto in base alle disposizioni di cui al punto 19 del
DISCIPLINARE TECNICO IN MATERIA DI MISURE
MINIME DI SICUREZZA
del
CODICE IN MATERIA DI DATI PERSONALI
(Dls. n. 196 del 30 giugno 2003)
(D.M. 305 del 07/12/2006)

Ragione Sociale	ISTITUTO COMPRENSIVO 1 BASSANO DEL GRAPPA
Indirizzo	Piazzale Trento N. 21 – 36061 Bassano del Grappa (VI)
Tel.	+39 0424 524932
Fax	+39 0424 232542
Sito	www.jvittorelli.it
EMail	viic88800e@istruzione.it
Cod.	Mecc.: VIIC88800E – Fisc.: 82002830246

Indice

1 Documento programmatico sulla sicurezza

Redatto in base alle disposizione di cui al punto 19 del

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA

del

CODICE IN MATERIA DI DATI PERSONALI

(Dls. n.196 del 30 giugno 2003)

(D.M. 305 del 07/12/2006)

1.1 Revisione

Indice delle revisioni

Rev	Data	Descrizione	Redatto	Verificato	Approvato
1.00	04/02/2013 P. 708/A2d	VERSIONE D.P.s.S. 2013	DSGA	DSGA	D.S.

1.2 Scopo

Il presente MANUALE sul trattamento dei dati personali è stato elaborato 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 Dirigente Scolastico 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 documento che segue deve essere aggiornato ogni anno e sottoposto a revisione entro e non oltre ogni 31 marzo 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 anche da nuovi rischi.
Al fine della migliore applicazione della legge sulla Privacy, il Dirigente Scolastico 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 istituzionali presenti nella specifica realtà scolastica.
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'Istituto scolastico nonché per creare e sostenere la cultura della privacy tra il corpo docente, il personale non insegnante e tutti coloro che trattano dati personali per ragioni connesse al raggiungimento delle finalità sottese all'insegnamento.
Tali finalità sono evidenziate nel 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'istituto scolastico.

1.3 Campo di applicazione, Gruppo Privacy ed aggiornamento

Il Documento Programmatico Sulla Sicurezza definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico Sulla Sicurezza riguarda il trattamento di tutti i dati personali:
- Sensibili
- Giudiziari
- Identificativi

Il Documento Programmatico Sulla Sicurezza si applica al trattamento di tutti i dati personali per mezzo di:
- Strumenti elettronici di elaborazione
- Altri strumenti di elaborazione (ed esempio: Cartacei, Audio, Visivi e Audiovisivi, ecc..)

Il presente Documento è strutturato in sezioni. Ogni sezione presenta degli allegati, che sono contrassegnati, generalmente, con la sigla **D_TEC** e sono contrassegnate, progressivamente, da lettere dalla "A" alla "Z".

Al punto 1.1 è riportata una tabella che evidenzia lo stato delle verifiche, fatte dall'eventuale ***Gruppo Privacy*** e l'approvazione delle eventuali modifiche da adottarsi dal:

a) **Dirigente Scolastico,** nella sua qualità di Titolare pro - tempore del trattamento dei dati personali, per l'adozione o la modifica del presente manuale;
b) **Direttore dei Servizi Generali ed Amministrativi**, nella sua qualità di 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 Documento programmatico sulla sicurezza 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 a sinistra, nella griglia di revisione, contraddistinto da un numero progressivo e dalla data di approvazione.

Il Documento programmatico sulla sicurezza deve essere conosciuto ed applicato da tutte le funzioni che fanno parte dell'organizzazione ed 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.

Per la sua consultabilità presso la segreteria scolastica è inoltre ritenuto fondamentale per far maturare, crescere e sensibilizzare la cultura della privacy.

1.4 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)		
Regolamento sul trattamento dei dati sensibili e giudiziari e schede allegate (D.M. n.305/2006)		

I suddetti riferimenti normativi sono allegati integralmente al presente documento.

1.5 Elenco dei modelli

Codice	Tipo di documento	Descrizione
ADS	Lettera di incarico	Incaricato gestione e manutenzione strumenti elettronici
BKP	Lettera di incarico	Incaricato delle copie di sicurezza delle banche dati
CDP	Lettera di incarico	Custode delle copie delle credenziali
DTEC_W	Lettera di incarico	Responsabile del trattamento dei dati in Out-Sourcing
DTEC_W2	Lettera di incarico	Indicazione di Titolare autonomo
IDT2	Lettera di incarico	Incaricato del trattamento dei dati personali
RAL	Lettera di incarico	Responsabili dell'accesso ai locali
RDT	Lettera di incarico	Responsabile della sicurezza dei dati personali
RDT6	Lettera di incarico	Responsabile di specifici trattamenti di dati personali
DTEC_A	Modello	Elenco degli archivi dei dati oggetto del trattamento
DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati
DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati
DTEC_E	Modello	Enti terzi a cui è affidato il trattamento dei dati in out-sourcing
DTEC_F	Modello	Personale autorizzato al trattamento dei dati
DTEC_G	Modello	Permessi di accesso ai dati
DTEC_H	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità
DTEC_M	Modello	Criteri e procedure per garantire l'integrità dei dati
DTEC_N	Modello	Piano di formazione degli incaricati del back-up
DTEC_Q, DTEC_Q2, DTEC_R	Modello	Report dei virus informatici rilevati, Report dei virus informatici rilevati da eliminare, Report dei contagi da Virus Informatici
DTEC_R2	Modello	Report dei contagi da Virus Informatici Ripuliti
DTEC_S	Modello	Criteri di assegnazione delle credenziali d i accesso
DTEC_T	Modello	Report annuale dei rischi hardware
DTEC_U	Modello	Report annuale dei rischi sui software installati
DTEC_Z	Modello	Report annuale altri rischi

1.6 Definizioni

1.6.1 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 identificativicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati.

1.6.2 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.

1.6.3 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.

1.6.4 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.

1.6.5 Titolare
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.

1.6.6 Responsabile
La persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

1.6.7 Incaricati
Le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile.

1.6.8 Interessato
La persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

1.6.9 Identificativicazione
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.

1.6.10 Diffusione
Il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

1.6.11 Dato anonimo
Il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile.

1.6.12 Blocco
La conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

1.6.13 Banca dati
Qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti.

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

1.6.15 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'articolo 31.

1.6.16 Strumenti elettronici
Gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento.

1.6.17 Autenticazione informatica
L'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità.

1.6.18 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.

1.6.19 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.

1.6.20 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.

1.6.21 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.

2 Ruoli, compiti e nomina delle figure previste per la sicurezza dei dati personali

2.1 Titolare del trattamento dei dati personali

2.1.1 Compiti del titolare del trattamento dei dati personali

Il **Titolare del trattamento è** 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.
Il **Titolare del trattamento** si impegna ad assicurare e garantire direttamente che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA tese a ridurre al minimo il rischio di distruzione dei dati, accesso non autorizzato o trattamento non consentito, previe idonee istruzioni fornite per iscritto.
- Il **Titolare del trattament**o, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili della sicurezza dei dati** che assicurino e garantiscano che vengano adottate le misure di sicurezza ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA. Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dat**i, ne assumerà tutte le responsabilità e funzioni.

2.1.2 Nomina, facoltativa, del Gruppo Privacy interno all'Istituzione Scolastica

Scopo del Gruppo Privacy è quello di delineare compiti e responsabilità dell'eventuale Gruppo Privacy.

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, l'Istituto Scolastico, in persona del suo Dirigente Scolastico pro - tempore, ha ritenuto opportuno delineare i tratti ed i requisiti al fine della sua eventuale costituzione.

Qualora nominato, spetterà al Dirigente Scolastico**,** in qualità di rappresentante legale dell'istituto, 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.

In caso di nomina, la costituzione del Gruppo Privacy sarà effettuata dal Dirigente Scolastico 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 almeno dal **Dirigente Scolastico**, dal **Direttore dei Servizi Generali ed Amministrativi** e da eventuali altre figure tecniche specializzate e/o consulenti esterni.

Al Gruppo potranno appartenere anche altri soggetti aventi diverse professionalità:

1) **personale A.T.A.**: 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 all'Istituto e verso

l'esterno. Può essere utile quindi cogliere il valore aggiunto della legge sulla privacy in termini di riorganizzazione e di miglioramento del piano dell'offerta formativa (POF) all'utenza; in questa ottica, fanno parte del Gruppo privacy, in via necessaria i Responsabili incaricati delle posizioni organizzative nell'ambito delle proprie competenze e, specificamente, **l'Assistente Amministrativo** o altra figura diversamente denominata svolgente funzioni analoghe a quelle del soggetto sopra individuato;

3) **personale tecnico-informatico**: sono 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; appartiene al Gruppo Privacy **l'Assistente Tecnico** o altra figura diversamente denominata svolgente funzioni analoghe a quelle del soggetto sopra individuato;
4) **rappresentante del personale insegnante** per la coordinazione delle attività di sostegno per gli alunni portatori di handicap, per lo svolgimento di iniziative assistenziali e per l'insegnamento della religione per la quale l'insegnante deve prestare attenzione ai sensi dell'art. 309 e 310 del T.U..

Al Gruppo Privacy eventualmente nominato vengono assegnati i seguenti compiti:

1) predisposizione delle schede da utilizzare per il monitoraggio delle attività di trattamento;
2) elaborazione dei dati raccolti presso le unità dell'Istituto Scolastico con le schede;
3) segnalazione agli organi competenti delle azioni necessarie;
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;
6) programmazione di attività di formazione diretta e di informazione del personale;
7) preposto allo svolgimento delle operazioni di Trattamento;
8) cura e aggiornamento del presente documento;
9) predisposizione delle condizioni per la consultazione e per l'eventuale distribuzione del documento e degli aggiornamenti, utilizzando anche strumenti telematici;
10) segnalazione delle innovazioni di carattere normativo e delle necessarie modificazioni da apportare al presente documento e alla modulistica allegata;
11) vigilanza sull'attività svolta dai soggetti incaricati del Trattamento e sul rispetto delle istruzioni loro impartite;
12) effettuazione di attività di audit e di controllo sulla rispondenza delle attività svolte rispetto a quanto previsto dalla legge e dalla documentazione dell'istituto scolastico;
13) attività di report sulle non conformità riscontrate;
14) revisione periodica della modulistica;
15) raccolta di quesiti di interesse sulla materia della privacy;
16) controllo sulle richieste di accesso ai documenti amministrativi dell'istituzione scolastica ai sensi della Legge n. 241/1990 da parte degli interessati e sul soddisfacimento dei diritti previsti dall'art. 7 del D.Lgs. n. 196/2003;
17) 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;
18) Comunicazione al Dirigente Scolastico in qualità di rappresentante dell'Istituto Titolare del Trattamento, del numero degli incaricati secondo quanto previsto al paragrafo 3.4.

Per quanto sopra l'eventuale nomina del Gruppo Privacy permetterebbe all'Istituto scolastico la migliore gestione degli adempimenti per l'osservanza della legge sulla Privacy e ciò in quanto punto di incontro tra le specifiche e peculiari competenze del Dirigente Scolastico e del Direttore dei Servizi Generali ed Amministrativi.

Si ritiene che tale nomina costituirebbe il migliore e più opportuno strumento per favorire il confronto, lo scambio di opinioni e di esperienze in materia di Privacy nonché per condividere in sinergia tutti gli aspetti della Sicurezza del trattamento dei dati personali.

2.1.2.1 Modulistica

GRP 01.01 - Nomina Gruppo Privacy

2.2 Responsabile della sicurezza dei dati personali

2.2.1 Compiti del responsabile della sicurezza dei dati personali

Il **Responsabile della sicurezza dei dati personali** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo a cui sono affidate le seguenti responsabilità e compiti:

- Garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Redigere ed aggiornare ad ogni variazione l'elenco delle sedi in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco degli uffici in cui vengono trattati i dati.
- Redigere ed aggiornare ad ogni variazione l'elenco delle banche dati oggetto di trattamento.
- Se il trattamento è effettuato con mezzi informatici, redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione.
- Redigere e di aggiornare ad ogni variazione l'elenco delle sedi e degli uffici in cui viene effettuato il trattamento dei dati.
- Nominare per ciascun ufficio in cui viene effettuato il trattamento dei dati, un **incaricato** con il compito di controllare i sistemi, le apparecchiature, e se previsti, i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.
- Definire e verificare periodicamente le modalità di acceso ai locali e le misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità.
- Decidere se affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.
- Qualora il trattamento dei dati sia stato affidato in tutto o in parte all'esterno della struttura del titolare controllare e garantire che tutte le misure di sicurezza riguardanti i dati personali siano applicate.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Responsabili della gestione e della manutenzione degli strumenti elettronic**i.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati della custodia delle copie delle credenziali** qualora vi sia più di un incaricato del trattamento.
- Se il trattamento è effettuato con mezzi informatici, individuare, nominare e incaricare per iscritto, uno o più **Incaricati delle copie di sicurezza delle banche dat**i.
- Custodire e conservare i supporti utilizzati per le copie dei dati.

Il **Responsabile della sicurezza dei dati personal**i, in relazione all'attività svolta, può individuare, nominare e incaricare per iscritto, se lo ritiene opportuno uno o più **Responsabili di uno specifico trattamento** con il compito di individuare, nominare e incaricare per iscritto, gli **Incaricati del trattamento dei dati personal**i.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Responsabile di uno specifico trattament**o, ne assumerà tutte le responsabilità e funzioni.

Qualora il **Titolare del trattamento** ritenga di non nominare alcun **Responsabile della sicurezza dei dati personal**i, ne assumerà tutte le responsabilità e funzioni.

2.2.2 Nomina del responsabile della sicurezza dei dati personali

La nomina di ciascun **Responsabile della sicurezza dei dati personali** deve essere effettuata dal **Titolare del trattamento** con una lettera di incarico (LI_RDT) in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del **Titolare del trattamento** in luogo sicuro.

Il **Titolare del trattamento** deve informare ciascun **Responsabile della sicurezza dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in

particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il **Titolare del trattamento** deve consegnare a ciascun **Responsabile della sicurezza dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del **Responsabile della sicurezza dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del **Responsabile della sicurezza dei dati personali** può essere revocata in qualsiasi momento dal **Titolare del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.3 Incaricati della gestione e della manutenzione degli strumenti elettronici

2.3.1 Compiti degli incaricati della gestione e della manutenzione degli strumenti elettronici

L'**incaricato della gestione e della manutenzione degli strumenti elettronici** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che sovrintende alle risorse del sistema operativo di un elaboratore o di un sistema di Banche di dati.

E' onere del **Responsabile della sicurezza dei dati personal**i, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **incaricati della gestione e della manutenzione degli strumenti elettronic**i.

E' compito degli **Incaricati della gestione e della manutenzione degli strumenti elettronic**i:

- Attivare le credenziali di autenticazione agli **Incaricati del trattamento,** su indicazione del **Responsabile del trattamento,** per tutti i trattamenti effettuati con strumenti informatici.
- Definire quali politiche adottare per la protezione dei sistemi contro i virus informatici e verificarne l'efficacia con cadenza almeno semestrale.
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers").
- Informare il **Responsabile della sicurezza dei dati personali** nella eventualità che si siano rilevati dei rischi relativamente alle misure di sicurezza riguardanti i dati personali.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della gestione e della manutenzione degli strumenti elettronic**i, ne assumerà tutte le responsabilità e funzioni.

2.3.2 Nomina degli incaricati della gestione e della manutenzione degli strumenti elettronici

Il **Responsabile della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati della gestione e della manutenzione degli strumenti elettronici** a cui è conferito il compito di sovrintendere al buon funzionamento delle risorse del sistema informativo e delle **Banche di dat**i.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronic**i, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più **Incaricati della gestione e della manutenzione degli strumenti elettronici** deve essere effettuata con una lettera di incarico (LI_ADS) e deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della gestione e della manutenzione degli strumenti elettronici** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina dell'**Incaricato della gestione e della manutenzione degli strumenti elettronici** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina degli **Incaricati della gestione e della manutenzione degli strumenti elettronici** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed eventualmente affidata ad altro soggetto.

2.4 Incaricato della custodia delle copie delle credenziali

2.4.1 Compiti degli incaricati della custodia delle copie delle credenziali

E' onere del **Responsabile della sicurezza dei dati personal**i, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati della custodia delle copie delle credenzial**i.

E' compito degli **Incaricati della custodia delle copie delle credenzial**i:

- Gestire e custodire le credenziali per l'accesso ai dati degli **Incaricati del trattament**o.
- Predisporre, per ogni incaricato del trattamento, una busta sulla quale è indicato il nome dell'incaricato e all'interno della busta deve essere indicata la credenziale usata. Le buste con le credenziali debbono essere conservate in luogo chiuso e protetto.
- Istruire gli incaricati del trattamento sull'uso delle parole chiave, e sulle caratteristiche che debbono avere, e sulle modalità per la loro modifica in autonomia.
- Revocare tutte le credenziali non utilizzate in caso di perdita della qualità che consentiva all'incaricato l'accesso ai dati personali.
- Revocare le credenziali per l'accesso ai dati degli **Incaricati del trattamento** nel caso di mancato utilizzo per oltre 6 (sei) mesi.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato della custodia delle copie delle credenzial**i, ne assumerà tutte le responsabilità e funzioni.

2.4.2 Nomina degli incaricati della custodia delle copie delle credenziali

Il **Responsabile della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati della custodia delle copie delle credenziali** a cui è conferito il compito di custodire le Parole chiave per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** deve essere effettuata con una lettera di incarico (LI_CDP), deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare gli **Incaricati della custodia delle copie delle credenziali** della responsabilità che è stata loro affidata in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato della custodia delle copie delle credenzial**i, una copia di tutte le norme che riguardano la Sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina di uno o più **Incaricati della custodia delle copie delle credenziali** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** senza preavviso, ed essere affidata ad altro soggetto.

2.5 Incaricato delle copie di sicurezza delle banche dati

2.5.1 Compiti degli incaricati delle copie di sicurezza delle banche dati

L'**Incaricato delle copie di sicurezza delle banche dati** è la persona fisica o la persona giuridica che ha il compito di sovraintendere alla esecuzione periodica delle copie di sicurezza delle Banche di dati personali gestite.

E' onere del **Responsabile della sicurezza dei dati personal**i, in relazione all'attività svolta, individuare, nominare e incaricare per iscritto, se lo ritiene opportuno, uno o più **Incaricati delle copie di sicurezza delle banche dat**i.

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce, con il supporto tecnico del **Responsabile della gestione e della manutenzione degli strumenti elettronici** la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di Dati trattate.

I criteri debbono essere concordati con il **Responsabile della gestione e della manutenzione degli strumenti elettronici** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni **Banca di dati** debbono essere definite le seguenti specifiche:

- Il "Tipo di supporto" da utilizzare per le "Copie di Back-Up".
- Il numero di "Copie di Back-Up" effettuate ogni volta.
- Se i supporti utilizzati per le "Copie di Back-Up" sono riutilizzati e in questo caso con quale periodicità.
- Se per effettuare le "Copie di Back-Up" si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle "Copie di Back-Up".
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- L'Incaricato del trattamento a cui è stato assegnato il compito di effettuare le "Copie di Back-Up".
- Le istruzioni e i comandi necessari per effettuare le "Copie di Back-Up".

E' compito degli **Incaricati delle copie di sicurezza delle banche dat**i:

- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti dal **Responsabile della sicurezza dei dati personal**i.
- Assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro.
- Assicurarsi della conservazione delle copie di sicurezza in luogo adatto e sicuro e ad accesso controllato.
- Di provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato.
- Di segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Incaricato delle copie di sicurezza delle banche dat**i, ne assumerà tutte le responsabilità e funzioni.

2.5.2 Nomina degli incaricati delle copie di sicurezza delle banche dati

Il **Responsabile della sicurezza dei dati personali** nomina uno o più soggetti **Incaricati delle copie di sicurezza delle banche dati** a cui è conferito il compito di compito di effettuare periodicamente le copie di sicurezza delle Banche di dati gestite.

Anche se non espressamente previsto dalla norma, è opportuno che il **Responsabile della sicurezza dei dati personali** nomini uno o più **Incaricati delle copie di sicurezza delle banche dat**i, specificando gli elaboratori o le banche dati che è chiamato a sovrintendere.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Incaricato delle copie di sicurezza delle banche dati** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

La nomina di uno o più **Incaricati delle copie di sicurezza delle banche dati** deve essere effettuata con una lettera di incarico (LI_BKP) e deve essere controfirmata per accettazione.

Copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Incaricato delle copie di sicurezza delle banche dati** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

2.6 Responsabile di specifico trattamento dei dati personali

2.6.1 Compiti del responsabile di uno specifico trattamento di dati personali

Il **Responsabile di uno specifico trattamento di dati personali** è la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo che ha il compito di individuare, nominare e incaricare per iscritto, gli **Incaricati del trattamento dei dati personali** del trattamento specifico di cui è responsabile.

Il **Responsabile di uno specifico trattamento di dati personali** ha il compito di:

- Nominare gli incaricati del trattamento per le Banche di dati che gli sono state affidate.
- Di sorvegliare che il trattamento sia effettuato nei termini e nei modi stabiliti dal Codice in materia di dati personali.
- Di dare le istruzioni adeguate agli **Incaricati del trattamento** effettuato con strumenti elettronici e non.
- Periodicamente, e comunque almeno annualmente, deve verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione degli **Incaricati del trattamento dei dati personal**i.

Qualora il **Responsabile della sicurezza dei dati personali** ritenga di non nominare alcun **Responsabile di uno specifico trattamento di dati personal**i, ne assumerà tutte le responsabilità e funzioni.

2.6.2 Nomina dei responsabili di uno specifico trattamento di dati personali

La nomina di ciascun **Responsabile di uno specifico trattamento di dati personali** deve essere effettuata dal **Responsabile della sicurezza dei dati personali** con una lettera di incarico in cui sono specificate le responsabilità che gli sono affidate e deve essere controfirmata dall'interessato per accettazione.

Nella lettera di nomina debbono essere indicate le **Banche dati** di cui è responsabile per quanto attiene alla sicurezza e a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.
Copia della lettera di nomina (LI_RTD) accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare ciascun **Responsabile di uno specifico trattamento di dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il **Responsabile della sicurezza dei dati personali** deve consegnare a ciascun **Responsabile di uno specifico trattamento di dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del **Responsabile di uno specifico trattamento di dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina del **Responsabile di uno specifico trattamento di dati personali** può essere revocata in qualsiasi momento dal **Responsabile della sicurezza dei dati personali** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.7 Incaricato del trattamento dei dati personali

2.7.1 Compiti degli incaricati del trattamento dei dati personali

Gli **Incaricati del trattamento** sono le persone fisiche autorizzate a compiere operazioni di trattamento sui dati personali da un **Responsabile del trattament**o.

In particolare gli incaricati del trattamento dei dati personali debbono osservare le seguenti disposizioni:

- Gli incaricati che hanno ricevuto credenziali di autenticazione per il trattamento dei dati personali, debbono conservare con la massima segretezza le parole chiave e i dispositivi di autenticazione in loro possesso e uso esclusivo.
- La parola chiave, quando è prevista dal sistema di autenticazione, deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito.
- La parola chiave non deve contenere riferimenti agevolmente riconducibili all'incaricato.
- L'incaricato del trattamento deve modificarla al primo utilizzo e, successivamente, almeno ogni sei mesi.
- In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave deve essere modificata almeno ogni tre mesi.
- Gli incaricati del trattamento non debbono in nessun caso lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento dei dati personali.
- Gli incaricati del trattamento debbono controllare e custodire, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, gli atti e i documenti contenenti dati personali.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

2.7.2 Nomina degli incaricati del trattamento dei dati personali

La nomina di ciascun **Incaricato del trattamento dei dati personali** deve essere effettuata dal **Responsabile del trattamento** con una **lettera di incarico** in cui sono specificati i compiti che gli sono stati affidati che deve essere controfirmata dall'interessato per presa visione.

Copia della lettera di nomina (LI_IDT) firmata deve essere conservata a cura del **Responsabile del trattamento** in luogo sicuro.

Il **Responsabile del trattamento** deve informare ciascun **Incaricato del trattamento dei dati personali** delle responsabilità che gli sono affidate in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Il **Responsabile del trattamento** deve consegnare a ciascun **Incaricato del trattamento dei dati personali** una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

Gli **Incaricati del trattamento dei dati personali** devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

Agli **Incaricati del trattamento dei dati personali** deve essere assegnata una **parola chiave** e un **codice di autenticazione informatic**a.

Agli **Incaricati del trattamento dei dati personali** è prescritto di adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e la diligente custodia dei dispositivi in possesso e ad uso esclusivo dell'incaricato.

La nomina dell'**Incaricato del trattamento dei dati personali** è a tempo indeterminato, e decade per revoca o dimissioni dello stesso.

La nomina dell'**Incaricato del trattamento dei dati personali** può essere revocata in qualsiasi momento dal **Responsabile del trattamento** dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

2.8 Amministratori di Sistema

In data 27 novembre 2008 il Garante per la protezione dei dati personali ha provveduto ad emanare un Provvedimento, recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008, relativo a "misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema". E' poi ritornato in argomento con i provvedimenti del 12 febbraio 2009 (G.U. n. 45 del 24 febbraio 2009) con cui si è disposto di unificare e contestualmente prorogare i termini per l'adempimento delle prescrizioni di cui al citato Provvedimento procrastinandone la scadenza al 30 giugno 2009; del 21 aprile 2009, con cui si è deciso di attivare una consultazione pubblica volta ad acquisire osservazioni e commenti da parte dei titolari del trattamento ai quali il provvedimento si rivolge con esclusivo riferimento a quanto prescritto al punto 2 del Provvedimento, dando tempo fino al 31 maggio 2009 per far pervenire osservazioni e commenti, pubblicato sulla G.U. n. 105 dell'8 maggio 2009; ed infine del 26 giugno 2009 con cui apportava modifiche al provvedimento del 27 novembre 2008 e proroga dei termini per il loro adempimento - 25 giugno 2009 (G.U. n. 149 del 30 giugno 2009)

Quanto previsto dal Provvedimento del Garante, datato 27 novembre 2008 e sue successive modificazioni ed integrazioni, non si esaurisce nella mera predisposizione di una nuova lettera di incarico o nella modifica di quella già esistente ma richiede al titolare una serie di "misure e accorgimenti" e, non ultimi, di "adempimenti in ordine all'esercizio dei doveri di controllo da parte del titolare (***due diligence***)" sulle attività dell'amministratore.

2.8.1 Il nuovo adempimento in sintesi

Con il **provvedimento a carattere generale del 27 novembre 2008** dal titolo "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema", pubblicato sulla G.U. n. 300 del 24 dicembre 2008, il Garante per la protezione dei dati personali impone ai titolari di trattamenti di dati personali (anche solo in parte gestiti mediante strumenti elettronici) di predisporre un "elenco degli amministratori di sistema e loro caratteristiche".

Gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel Documento Programmatico sulla Sicurezza, oppure, nei casi in cui il titolare non sia tenuto a redigere il DPS, annotati comunque in un documento interno da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.

Nella pratica occorre:

- **individuare coloro che ricadono nella categoria di "amministratore di sistema"**
- **valutare l'esperienza, la capacità e l'affidabilità** dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza
- **designare tali "amministratore di sistema" in modo individuale** con l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato
- **verificare l'operato degli amministratori di sistema, con cadenza almeno annuale**, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti
- **registrare gli accessi ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema**, mediante l'adozione di sistemi idonei alla registrazione degli accessi logici (autenticazione informatica).

Sono esclusi dall'ambito applicativo del presente provvedimento i titolari di alcuni trattamenti effettuati in ambito pubblico e privato a fini amministrativo-contabili, i quali pongono minori rischi per gli interessati e sono stati pertanto oggetto di recenti misure di semplificazione (art. 29 D.l. 25 giugno 2008, n. 112, convertito, con modifiche, con Legge 6 agosto 2008, n. 133; art. 34 del Codice; Provv. Garante 6 novembre 2008).

2.8.2 Cosa si intende per amministratore di sistema?

Il primo punto di riflessione riguarda l'individuazione di coloro che ricadono nella categoria di "amministratore di sistema".

Tale figura, anche se non esplicitamente indicata nel "Codice in materia di protezione dei dati personali" era prevista, viceversa, dal DPR 318/1999 (abrogato dal Codice) che definisce l'amministratore di sistema il "soggetto al quale è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di banca dati e di consentirne l'utilizzazione" (art. 1, comma 1, lett. c).

Nel provvedimento del 27 novembre 2008 il Garante dice che con "amministratore di sistema" si individuano figure professionali finalizzate alla gestione e alla manutenzione di un impianto di elaborazione o di sue componenti e che sono considerate tali anche altre figure equiparabili dal punto di vista dei rischi relativi alla protezione dei dati, quali gli **amministratori di basi di dati**, gli **amministratori di reti** e di **apparati di sicurezza** e gli **amministratori di sistemi software complessi** e ciò anche quando l'amministratore non consulti "in chiaro" le informazioni relative ai trattamenti di dati personali.

2.8.3 Come si valutano le capacità dell'amministratore di sistema?

Il titolare, prima di procedere alla nomina, deve valutare l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" che devono fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

In che modo ciò può essere svolto (ed eventualmente dimostrato al Garante in caso di ispezione)?

È ovvio che si parte dal presupposto che chi di fatto svolge già oggi la funzione di amministratore di sistema sia in grado si svolgere la propria funzione; è opportuno allora predisporre una sorta di **curriculum vitae** di ciascun amministratore che indichi chiaramente titoli di studio, certificazioni professionali, esperienze professionali, corsi di formazione già svolti. Il CV deve essere datato e firmato sia dall'amministratore che dal titolare. L'indicazione dei percorsi formativi svolti specie per gli ambiti non prettamente tecnologici ma relativi invece alle problematiche della privacy e della protezione dei dati personali assume un valore particolarmente importante per il "rispetto della garanzia delle vigenti disposizioni". L'amministratore di sistema non può essere solo un bravo tecnico ma deve conoscere la normativa sulla privacy.

2.8.4 Designazione dell'amministratore di sistema

Occorre predisporre una lettera di "incarico" specifica che contenga:

- attestazione che l'incaricato ha le caratteristiche richieste dalla legge;
- elencazione analitica degli ambiti di operatività richiesti e consentiti in base al profilo di autorizzazione assegnato;
- indicazione delle "verifiche" almeno annuali che il titolare svolgerà sulle attività svolte dall'amministratore di sistema;
- indicazione che la nomina ed il relativo nominativo sarà comunicato al personale ed eventualmente a terzi nei modi richiesti dalla legge.

2.8.5 Cos'è una "due diligence"?

Il Garante nel provvedimento del 27 novembre 2008 sull'amministratore di sistema usa per la prima volta l'espressione "*due diligence*" per indicare "gli accorgimenti e misure, tecniche e organizzative, volti ad agevolare l'esercizio dei doveri di controllo da parte del titolare" in relazione alle mansioni svolte dagli amministratori di sistema.

Come è noto, nell'ambito dell'internal audit e dell'information security con "*due diligence*" si intende un'attività di analisi e verifica volta al raggiungimento di un parere di conformità (*compliance*) in relazione a

particolari attività anche in relazione ai possibili rischi ed ai relativi impatti. Caratteristica della "due diligence" è inoltre, a fronte dei risultati ottenuti, la predisposizione di un piano di (eventuali) azioni correttive.

In sintesi l'output della due diligence del titolare sull'amministratore di sistema deve consistere almeno nei seguenti elementi:

1. giudizio di conformità sugli adempimenti richiesti;
2. valutazione dei possibili rischi (e relativi impatti);
3. indicazioni dei possibili interventi (se necessari o opportuni).

Giudizio di conformità sugli adempimenti richiesti

Il giudizio di conformità viene realizzato dal titolare o da una terza parte indipendente rispetto ai sistemi informativi (ad esempio l'Internal Audit) mediante la verifica del rispetto degli adempimenti richiesti.

2.8.6 Riepilogo degli adempimenti richiesti:

1) **nominare gli amministratori di sistema, siano essi interni o esterni**. E' meglio accompagnare la nomina con un documento in cui si inquadrino responsabilità e ambiti di azione (Modelli MAS04.17, MAS04.21 e MAS04.23):

   1.a) **Valutazione delle caratteristiche soggettive**: in sostanza, si devono nominare amministratori di sistema persone con adeguata esperienza, capacità e affidabilità.
   1.b) **Designazioni individuali**: la nomina deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato. Questo è un concetto molto importante, perché oltre alla nomina dei responsabili e degli incaricati adesso occorrerà nominare anche gli amministratori, tramite una lettera di incarico in cui si dovranno indicare anche le rispettive mansioni e gli ambiti di intervento.
   1.c) **Servizi in outsourcing**: nel caso di servizi di amministrazione di sistema affidati in outsourcing il titolare deve conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte quali amministratori di sistema. Anche in questo frangente l'adempimento è più rilevante che in passato, visto che per nel caso di responsabili di trattamenti in outsourcing il titolare era tenuto alla semplice nomina del responsabile esterno, senza ricevere informazioni sugli incaricati da esso designati. In pratica, non si trattavano nominativi di appartenenti a società esterne, mentre ora devono essere ben registrati. Se si erogano servizi informatici, hardware e/o software, di qualunque tipo e/o livello l'Azienda deve comunicare, almeno annualmente, i nominativi dei tecnici preposti ai propri Clienti.

2) **riportare l'elenco degli amministratori di sistema nel DPS**.

   2.a) **Elenco degli amministratori di sistema**: gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite, devono essere riportati nel documento programmatico sulla sicurezza. Questo è una novità rispetto alle nomine precedenti di incaricati e responsabili, che non dovevano essere inserite nel DPS. A questo proposito, si consiglia di riportate questo elenco in uno degli allegati al DPS, per motivi di protezione dei dati personali degli amministratori stessi. Inoltre, i titolari pubblici e privati sono tenuti a rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito delle proprie organizzazioni, secondo le caratteristiche dell'azienda o del servizio, in relazione ai diversi servizi informatici cui questi sono preposti (Modello MAS04.22 e MAS04.25).

3) Se si erogano servizi informatici, hardware e/o software, di qualunque tipo e/o livello l'Azienda deve **notificare l'elenco nominativo degli amministratori di sistema interni e le ragioni sociali degli amministratori di sistema esterni**, almeno annualmente, intesi come nominativi dei tecnici preposti ai propri Clienti.

4) **notificare l'elenco degli amministratori di sistema ai dipendenti tramite informativa** (si può fare in diversi modi, dalla notifica al momento della nomina come incaricati del trattamento ad una schermata informativa in fase di login al sistema, oppure con una circolare in bacheca o una mail rivolta a tutti. Modello MAS04.26);

5) **verificare periodicamente l'operato degli amministratori di sistema e i nominativi previsti** (questo si può anche fare annualmente, in fase di revisione del DPS. Modello MAS04.20)

5.a) **Verifica delle attività:** l'operato degli amministratori di sistema deve essere oggetto, con cadenza almeno annuale, di un'attività di verifica da parte dei titolari del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti.

6) **attuare la registrazione temporale degli accessi al sistema da parte degli amministratori**. Questo è comunque un argomento che va studiato caso per caso.

6.a) **Registrazione degli accessi:** devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo per cui sono richieste. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi. Questo è un adempimento piuttosto complesso da rispettare, poichè è richiesto il tracciamento degli accessi degli amministratori al sistema informatico in termini di riferimenti temporali. Ma se la cosa è fattibile per quanto riguarda i sistemi operativi (es accesso ai sistemi windows), non è detto che gli applicativi specifici (es ragioneria, paghe, ecc) siano in grado di tracciare tali log. Inoltre, la cosa diventa ulteriormente complessa nei casi in cui gli archivi vengano gestiti con strumenti di office automation: se ad esempio un archivio è gestito con un foglio excel, registrare tutti gli accessi diventa nel complesso di difficile gestione.

2.8.7 Allegati

ADS.01.01 - Verbale annuale di nomina o verifica ADS.rtf
ADS.01.02 - Elenco Amministratori di Sistema Interni e Responsabili Esterni nel Trattamento Informatico dei dati
ADS.01.03 - Comunicazione al personale nominativi Amministratori di Sistema
ADS.01.04 - Nomina dell'amministratore di sistema interno
ADS.01.05 - Nomina Amministratori di Sistema Aule Informatiche
ADS.01.06 - Nomina a Responsabile Esterno nel Trattamento Informatico dei Dati
ADS.01.07 - Richiesta nominativi amministratori di sistema
ADS.01.08 - Verbale di verifica delle attività di Amministratore di Sistema

3 Trattamenti con l'ausilio di strumenti elettronici

3.1 Sistema di autenticazione informatica

3.1.1 Procedura di identificazione

Nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, il **Responsabile della sicurezza dei dati personali** deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di **credenziali di autenticazione** che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

3.1.2 Identificazione dell'incaricato

Il **Responsabile della sicurezza dei dati personali** deve assicurare che il trattamento di dati personali, effettuato con strumenti elettronici, sia consentito solamente agli incaricati dotati di una o più **credenziali di autenticazione** tra le seguenti:

- Un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo
- Un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave
- Una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

Il **Responsabile della sicurezza dei dati personali** deve assicurarsi che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

Il **Responsabile della sicurezza dei dati personali** deve assicurarsi che le **credenziali di autenticazione** non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

Il **Responsabile della sicurezza dei dati personali** deve assicurarsi che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni **Incaricato del trattamento** possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

3.1.3 Caratteristiche della parola chiave

La componente riservata delle credenziali di autenticazione (parola chiave) deve rispettare i seguenti criteri:

- Non deve contenere nomi identificativi
- Non deve contenere nomi di persona
- Deve contenere sia lettere che numeri
- Deve comprendere almeno 3 caratteri alfabetici
- Deve comprendere almeno 2 caratteri numerici
- Deve essere diversa dallo User-Id
- Deve essere lunga 8 caratteri o massimo consentito dal sistema di autenticazione
- Non deve essere riconducibile all'incaricato.

Ogni incaricato deve essere informato e reso edotto che:

- Le credenziali di accesso sono personali
- Le credenziali di accesso devono essere memorizzate
- Le credenziali di accesso non devono essere identificativicate a nessuno
- Le credenziali di accesso non devono essere trascritte

Il **Responsabile di uno specifico trattamento** deve consegnare ad ogni incaricato del trattamento il modulo DTEC_s, con le istruzioni per l'utilizzo della componente riservata delle credenziali di autenticazione (parola chiave) che deve essere controfirmato da quest'ultimo e deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.1.4 Cautele per assicurare la segretezza della componente riservata della credenziale

Gli incaricati debbono adottare le necessarie cautele per assicurare la segretezza della **parola chiave** e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..).
In particolare è fatto divieto identificativicare a chiunque altro incaricato le proprie credenziali di accesso al sistema informatico.

3.1.5 Istruzioni per non lasciare incustodito e accessibile lo strumento elettronico

Gli **incaricati del trattamento** hanno l'obbligo di:

- Non lasciare incustodito il proprio posto di lavoro.
- Di chiudere tutte le applicazioni aperte o meglio ancora di spegnere il sistema informatico in caso di assenza prolungata.

3.1.6 Accesso straordinario

Gli **Incaricati della custodia delle copie delle credenziali**, hanno il compito di assicurare la disponibilità dei dati e degli strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

La custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza.

Gli **Incaricati della custodia delle copie delle credenziali** devono informare tempestivamente l'**Incaricato del trattamento** ogni qualvolta sia stato effettuato un tale tipo di intervento.

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

3.2 Sistema di autorizzazione

I **Responsabili del trattamento** hanno il compito di individuare gli **Incaricati del trattamento** per ogni tipologia di banca di dati personali trattata.
Il tipo di trattamento effettuato da ogni singolo **Incaricato del trattamento** può essere differenziato.

In particolare ad ogni **Incaricato del trattamento** può essere data dal **Responsabile del trattamento** la possibilità di:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella banca di dati personali
- Cancellare le informazioni esistenti nella banca di dati personali

Il **Responsabile del trattamento** deve aggiornare l'Elenco dei **Permessi di accesso** ai dati utilizzando il modulo DTEC_g, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.3 Altre misure di sicurezza

In considerazione di quanto disposto dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal **Responsabile della sicurezza dei dati personali** di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personal**i, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.4 Periodicità di revisione del documento programmatico sulla sicurezza

Entro il 31 marzo di ogni anno, il **Titolare del trattamento** di dati sensibili o di dati giudiziari deve verificare ed eventualmente predisporre una nuova versione del **Documento programmatico sulla sicurezza** contenente idonee informazioni riguardo ai punti 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA del CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003).

3.5 Elenco dei trattamenti di dati personali

3.5.1 Elenco delle sedi e degli uffici in cui vengono trattati i dati

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle sedi in cui viene effettuato il trattamento dei dati.

In conformità a quanto disposto dal **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) per redigere l' Elenco delle sedi in cui vengono trattati i dati deve essere utilizzato il modulo DTEC_b, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere aggiornato e conservato in luogo sicuro a cura del **Responsabile della sicurezza dei dati personal**i.

3.5.2 Elenco degli archivi dei dati oggetto del trattamento

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco delle tipologie di trattamenti effettuati.

Ogni **banca di dati** o archivio deve essere classificato in relazione alle informazioni contenute indicando se si tratta di:

- Dati personali Identificativi
- Dati personali Sensibili
- Dati personali Giudiziari

In conformità a quanto disposto dal **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) per l'individuazione degli archivi dei dati oggetto del trattamento deve essere utilizzato il modulo DTEC_a, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.5.3 Elenco dei sistemi di elaborazione per il trattamento

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione con cui viene effettuato il trattamento dei dati.

Per ogni sistema deve essere specificato:

- Il **Responsabile della gestione e della manutenzione**
- Il nome dell'incaricato o degli incaricati che lo utilizzano
- Il nome di uno o più **Incaricati della custodia delle copie delle credenziali**

In conformità a quanto disposto dal **punto 19.1 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) per ogni sistema deve essere utilizzato il modulo DTEC_d, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro e deve essere trasmesso in copia controllata al **Responsabile della gestione e della manutenzione degli strumenti elettronici** di competenza.

3.6 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

3.6.1 Elenco dei soggetti autorizzati al trattamento dei dati

Il **Responsabile della sicurezza dei dati personali** ha il compito di assegnare le **credenziali di autenticazione** e di aggiornare l'**elenco del personale autorizzato al trattamento dei dati** utilizzando il modulo DTEC_f., che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personal**i, in luogo sicuro e deve essere trasmesso in copia controllata all'**Incaricato della custodia delle copie delle credenziali** di competenza.

3.6.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

Il **Responsabile della sicurezza dei dati personali** ha il compito di verificare ogni anno, entro il 31 dicembre, le **credenziali di autenticazione** e di aggiornare l'**elenco dei soggetti autorizzati al trattamento dei dati** utilizzando il modulo DTEC_f, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personal**i, in luogo sicuro e deve essere trasmesso in copia controllata agli **Incaricati della custodia delle copie delle credenziali** di competenza.

3.6.3 Distribuzione dei compiti e delle responsabilità

In conformità a quanto disposto dal **punto 19.2 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003), il **Titolare del trattamento** una volta stabilita la struttura di riferimento, i compiti e le relative responsabilità, in relazione ai trattamenti effettuati, deve predisporre il modulo DTEC_J, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.7 Analisi dei rischi

3.7.1 Analisi dei rischi hardware

Il **Responsabile della gestione e della manutenzione degli strumenti elettronic**i, anche avvalendosi di consulenti interni o esterni, deve di verificare ogni anno:

- La situazione delle apparecchiature hardware installate con cui vengono trattati i dati
- La situazione delle apparecchiature periferiche
- La situazione dei dispositivi di collegamento con le reti pubbliche

La verifica ha lo scopo di controllare l'affidabilità del sistema tenendo conto anche dell'evoluzione tecnologica, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** deve aggiornare il **Report annuale dei rischi hardware** conformemente al modulo DTEC_t.

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_t, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

I **Responsabili della gestione e della manutenzione degli strumenti elettronici** nel caso in cui esistano rischi evidenti debbono informare il **Responsabile della sicurezza dei dati personali** perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.2 Analisi dei rischi sui sistemi operativi e sui software installati

Al **Responsabile della gestione e della manutenzione degli strumenti elettronici** è affidato il compito di verificare ogni anno, la situazione dei Sistemi Operativi e delle applicazioni software installate sulle apparecchiature con cui vengono trattati i dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei software utilizzati.
- Segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti.
- Segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** deve aggiornare il **Report annuale dei rischi sui software installati** conformemente al modulo DTEC_u.

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_u, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

I **Responsabili della gestione e della manutenzione degli strumenti elettronic**i, nel caso in cui esistano rischi evidenti, debbono informare il **Responsabile della sicurezza dei dati personali** affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.7.3 Analisi degli altri rischi nel trattamento dei dati

Al **Responsabile della gestione e della manutenzione degli strumenti elettronici** è affidato il compito di analizzare eventuali altri rischi connessi al trattamento dei dati.

La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi e delle applicazioni software, per quanto riguarda:

- La sicurezza dei dati trattati.
- Il rischio di distruzione o di perdita.
- Il rischio di accesso non autorizzato o non consentito.

Tenendo conto in particolare di:

- Rischi connessi al comportamento degli operatori
- Rischi connessi al contesto fisico ed ambientale

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** deve aggiornare il **Report annuale degli altri rischi** conformemente al modulo DTEC_z.

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_z, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

I **Responsabili della gestione e della manutenzione degli strumenti elettronic**i, nel caso in cui esistano rischi evidenti, debbono informare il **Responsabile della sicurezza dei dati personali** affinché siano presi gli opportuni provvedimenti per assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

3.8 Misure da adottare per garantire l'integrità e la disponibilità dei dati

Il **Responsabile della gestione e della manutenzione degli strumenti elettronici** al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banca di dati trattati.
I criteri debbono essere definiti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Il **Responsabile della gestione e della manutenzione degli strumenti elettronic**i, per ogni banca di dati deve predisporre le istruzioni di copia, verifica e ripristino dei dati, utilizzando il modulo DTEC_m.

In conformità a quanto disposto dal **punto 19.5 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_m, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

Il "Documento con le istruzioni di copia" deve essere conservato a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro e deve essere trasmesso in copia controllata a ciascun incaricato delle copie di sicurezza delle banche dati.

In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

- Il Tipo di supporto da utilizzare per le Copie di sicurezza dei dati.
- Il numero di Copie di sicurezza dei dati effettuate ogni volta
- Se i supporti utilizzati per le Copie di sicurezza dei dati sono riutilizzati e in questo caso con quale periodicità .
- Se per effettuare le Copie di sicurezza dei dati si utilizzano procedure automatizzate e programmate.
- Le modalità di controllo delle Copie di sicurezza dei dati.
- La durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati.
- Il nome dell'incaricato a cui è stato assegnato il compito di effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare le Copie di sicurezza dei dati.
- Le istruzioni e i comandi necessari per effettuare il ripristino delle Copie di sicurezza dei dati.

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di verificare ogni anno, entro il 31 dicembre, le necessità di formazione del personale incaricato di effettuare periodicamente le Copie di sicurezza delle banca di dati trattate, in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, utilizzando il modulo DTEC_n.

In conformità a quanto disposto dal **punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_n, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.9 Misure da adottare per la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

3.9.1 Misure generali

In considerazione di quanto disposto dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal **Responsabile della sicurezza dei dati personali** di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personal**i, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

3.9.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, e di nominare per ciascun ufficio un **incaricato** con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali allo scopo di impedire intrusioni o danneggiamenti.

Il **Responsabile della sicurezza dei dati personali** deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.

Il **Responsabile della sicurezza dei dati personali** deve incaricare per iscritto con una lettera di nomina ogni incaricato del controllo di accesso ai locali dei compiti che gli sono stati affidati utilizzando il modello L_RAL.

In conformità a quanto disposto dal **punto 19.4 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) copia di moduli L_RAL, debbono essere allegati al presente Documento Programmatico sulla Sicurezza.

3.10 Formazione degli incaricati del trattamento

3.10.1 Piano di formazione

Il **Responsabile del trattamento dei dati personali** valuta, per ogni incaricato a cui ha affidato il trattamento, sulla base dell'esperienza, delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessario pianificare interventi di formazione.

La formazione è programmata già al momento dell'ingresso in servizio di nuovi incaricati del trattamento, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

Al **Responsabile della sicurezza dei dati personali** è affidato il compito di redigere ogni anno, **entro il 31 dicembr**e, il **Piano di Formazione del personale** utilizzando il modulo DTEC_h, specificando le necessità di ulteriore formazione del personale.

Il Piano di formazione del personale deve essere predisposto per:

- Rendere edotti gli incaricati del trattamento sui rischi che incombono sui dati
- Rendere edotti gli incaricati del trattamento sulle misure disponibili per prevenire eventi dannosi
- Rendere edotti gli incaricati del trattamento sui profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività
- Rendere edotti gli incaricati del trattamento sulle responsabilità che ne derivano
- Rendere edotti gli incaricati del trattamento sulle modalità per aggiornarsi sulle misure minime adottate dal titolare

In conformità a quanto disposto dal **punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_h, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.11 Criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare

3.11.1 Trattamenti di dati personali affidati all'esterno della struttura del titolare

Il **Responsabile della sicurezza dei dati personal**i, può decidere di affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare.

Il **Responsabile della sicurezza dei dati personal**i, deve redigere e aggiornare ad ogni variazione l'elenco dei soggetti che effettuano il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, ed indicare per ognuno di essi il tipo di trattamento effettuato specificando:

- I soggetti interessati
- I luoghi dove fisicamente avviene il trattamento dei dati stessi
- I responsabili del trattamento di dati personali

Per l'inventario dei soggetti a cui affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare, deve essere utilizzato il modulo DTEC_e, che deve essere allegato al presente Documento Programmatico sulla Sicurezza, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personal**i, in luogo sicuro.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, sia possibile nominare responsabili del trattamento soggetti controllabili dal **Titolare del trattamento** stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso), è possibile indicare gli stessi **Responsabili del trattamento in Out-sourcin**g, mediante il modello DTEC_w, che deve essere allegato al presente Documento Programmatico sulla Sicurezza.

Nel caso in cui, per i trattamenti dei dati affidati in tutto o in parte all'esterno della struttura del titolare, non sia possibile nominare i responsabili del trattamento, in quanto soggetti autonomi non controllabili dal titolare del trattamento stesso (relativamente alle modalità e alle misure minime di sicurezza da adottare nel trattamento stesso) , è possibile indicare i **Titolari autonomi del trattamento in Out-sourcin**g, mediante il modello DTEC_w2, per il quale trattamento, ai sensi dell'art. 28 del CODICE IN MATERIA DI DATI PERSONALI, devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

In conformità a quanto disposto dal **punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_w2, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.11.2 Criteri per la scelta degli enti terzi per il trattamento di dati personali affidati all'esterno della struttura del titolare

Il **Responsabile della sicurezza dei dati personal**i, può affidare il trattamento dei dati in tutto o in parte all'esterno della struttura del titolare a quei soggetti terzi che abbiano i requisiti individuati all'art. 29 del CODICE IN MATERIA DI DATI PERSONALI (esperienza, capacità ed affidabilità).

Il Titolare a cui è stato affidato il trattamento dei dati all'esterno deve rilasciare una dichiarazione scritta da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento ai sensi del CODICE IN MATERIA DI DATI PERSONALI e del DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

3.11.3 Nomina del responsabile del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il **Responsabile della sicurezza dei dati personali** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il **Responsabile del trattamento in Out-sourcing** deve accettare la nomina, secondo il modello DTEC_w.

La nomina del **Responsabile del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare il **Responsabile del trattamento in Out-sourcin**g, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Al momento dell'affidamento dell'incarico il **Responsabile del trattamento in Out-sourcin**g, deve dichiarare per iscritto:

· Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali · Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali · Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
· Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
· Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

In conformità a quanto disposto dal **punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_w, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.11.4 Nomina del titolare autonomo del trattamento in Out-sourcing

Per ogni trattamento affidato ad un soggetto esterno alla struttura del titolare, il **Responsabile della sicurezza dei dati personali** deve assicurarsi che siano rispettate le norme di sicurezza di un livello non inferiore a quanto stabilito per il trattamento interno.

Il **Titolare autonomo del trattamento in Out-sourcing** deve accettare la nomina, secondo il modello DTEC_w2.

La nomina del **Titolare autonomo del trattamento in Out-sourcing** deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro.

Il **Responsabile della sicurezza dei dati personali** deve informare il **Titolare autonomo del trattamento in Out-sourcin**g, dei compiti che gli sono assegnati in conformità a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA.

Al momento dell'affidamento dell'incarico il **Titolare autonomo del trattamento in Out-sourcing**, deve dichiarare per iscritto:

· Di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali

· Di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali
· Di adottare le istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o di integrarle nelle procedure già in essere.
· Di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
· Di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

In conformità a quanto disposto dal **punto 19.7 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_w2, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.12 Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

3.12.1 Protezione contro l'accesso abusivo

Al fine di garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso abusivo, il **Responsabile della sicurezza dei dati personal**i, stabilisce, con il supporto tecnico dei **Responsabili della gestione e della manutenzione degli strumenti elettronic**i, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione da parte di hackers su ogni sistema.

I criteri debbono essere definiti dal **Responsabile della sicurezza dei dati personali** in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure applicate per evitare intrusioni.
- Le misure applicate per evitare contagi da "Virus Informatici".

Per ogni sistema deve essere utilizzato il modulo DTEC_d, e deve essere conservato a cura del **Responsabile della sicurezza dei dati personali** in luogo sicuro e deve essere trasmesso in copia controllata al **Responsabile della gestione e della manutenzione degli strumenti elettronici** di competenza.

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) il modulo DTEC_d, deve essere allegato al presente Documento Programmatico sulla Sicurezza.

3.12.2 Istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili

Il **Responsabile della sicurezza dei dati personali** è responsabile della custodia e della conservazione dei supporti utilizzati per le copie dei dati.

Per ogni banca di dati deve essere individuato il luogo di conservazione copie dei dati in modo che sia convenientemente protetto dai potenziali rischi di:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni e atti vandalici
- Incendio
- Allagamento
- Furto

Nel modulo DTEC_m deve essere specificato il luogo di conservazione supporti utilizzati per le copie dei dati.

L'accesso ai supporti utilizzati per le copie dei dati è limitato per ogni banca di dati a:

- **Incaricati delle copie di sicurezza delle banche dati**
- **Responsabile della sicurezza dei dati personali**

In conformità a quanto disposto dal **punto 19.3 del Disciplinare tecnico in materia di misure minime di sicurezza** (allegato B del Dlgs. 196 del 30 giugno 2003) i moduli DTEC_m, debbono essere allegati al presente Documento Programmatico sulla Sicurezza.

3.12.3 Riutilizzo dei supporti rimovibili

Se il **Responsabile della sicurezza dei dati personali** decide che i supporti magnetici contenenti dati sensibili o giudiziari non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto annullando e rendendo intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso contenute.

E' compito del **Responsabile della sicurezza dei dati personali** assicurarsi che in nessun caso vengano lasciate copie di **Banche di dati** contenenti dati sensibili o giudiziari, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese intelligibili e tecnicamente in alcun modo ricostruibili le informazioni in esso registrate.

3.12.4 Ripristino dell'accesso ai dati in caso di danneggiamento

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del **Responsabile della sicurezza dei dati personal**i.

La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

Una volta valutata la assoluta necessità di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento il **Responsabile della sicurezza dei dati personali** deve provvedere tramite l'**Incaricato delle copie di sicurezza delle banche dati** e tramite **il Responsabile della gestione e della manutenzione degli strumenti elettronici** all'operazione di ripristino dei dati.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti, è compito esclusivo del **Responsabile della sicurezza dei dati personali** che si può avvalere del parere del **Responsabile della gestione e della manutenzione degli strumenti elettronic**i.

La decisione di ripristinare la funzionalità degli elaboratori elettronici guasti deve essere presa rapidamente e in ogni caso la funzionalità deve essere ripristinata al massimo entro sette giorni.

3.13 Misure di tutela e garanzia

3.13.1 Descrizione degli interventi effettuati da soggetti esterni

Nel caso in cui ci si avvale di soggetti esterni alla propria struttura, per provvedere al controllo del buon funzionamento hardware e/o software degli strumenti elettronici e alla eventuale riparazione, aggiornamento o sostituzione, il **Responsabile della sicurezza dei dati personal**i, deve farsi consegnare puntualmente dal personale che ha effettuato l'intervento tecnico, una dichiarazione scritta con la descrizione dettagliata delle operazioni eseguite che attesti la conformità a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003).

4 Trattamenti senza l'ausilio di strumenti elettronici

4.1 Nomina e istruzioni agli incaricati

Per ogni archivio i **Responsabili della sicurezza dei dati personali** debbono definire l'elenco degli incaricati autorizzati ad accedervi e impartire istruzioni tese a garantire un controllo costante nell'accesso negli archivi.

Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano dati sensibili o giudiziari ai sensi dell'art. 4 del CODICE IN MATERIA DI DATI PERSONALI, gli incaricati del trattamento sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

4.2 Copie degli atti e dei documenti

In base a quanto stabilito dal CODICE IN MATERIA DI DATI PERSONALI (Dls. n.196 del 30 giugno 2003) e dal DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA, è fatto divieto a chiunque di:

- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal **Responsabile della sicurezza dei dati personali,** di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal **Responsabile della sicurezza dei dati personal**i, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

5 Informative e Consensi Informati

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.

5.1 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

5.2 Responsabilità

Il Responsabile del trattamento ed i singoli incaricati sono tenuti a fornire le informative approvate dal Dirigente Scolastico, in qualità di rappresentante dell'Istituto Scolastico, 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).

5.3. 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).
In tal senso 'informativa ha un duplice scopo:

a) 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;
b) in secondo luogo, nei casi in cui sia necessario, le informazioni servono a rendere edotto 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'Istituto Scolastico 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 che codesto Istituto Scolastico effettuerà in applicazione delle norme in tema di informativa, conservazione dei dati ed adozione delle misure minime di sicurezza strumentali, come detto, a consentire l'esercizio delle facoltà riconosciute all'interessato e degli obblighi del Dirigente Scolastico.

5.3.1. 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'Istituto Scolastico, 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 da codesto Istituto Scolastico non è 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, l'Istituto Scolastico ha ritenuto, 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:

1. le finalità e le modalità del Trattamento;
2. la natura obbligatoria o facoltativa del conferimento dei dati;
3. le conseguenze di un eventuale rifiuto di rispondere;
4. i soggetti o le categorie di soggetti ai quali i dati possono essere comunicati e l'ambito di diffusione dei dati medesimi;
5. i diritti di cui all'articolo 7 del D.Lgs. n.196/2003;
6. 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:

1. elementi necessari, che non possono mai mancare in una informativa: l'identità del Titolare, la finalità del Trattamento (ad esempio: finalità connesse all'insegnamento, gestione dei permessi sindacali, ecc.), il riferimento ai diritti dell'interessato, di cui all'art. 7;
2. 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);
3. 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 indicazione dei Responsabili nominati: come peraltro già detto precedentemente. Questa opzione consente di gestire le informative in senso dinamico, senza dover procedere alla modificazione del contenuto delle stesse, qualora venga sostituita la persona fisica alla quale è stata conferita la Responsabilità della struttura. Inoltre, al fine di consentire all'interessato un buon rapporto con l'Istituto Scolastico 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.

Dalla compiuta analisi del Trattamento dei dati effettuata da codesto Istituto Scolastico ne discende, in definitiva, che residuerà a carico del medesimo un obbligo di informazione a tutti quei soggetti i cui dati non rientrano nel "normale" Trattamento di cui alla superiore lettera c).

5.3.2 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:

1. 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;
2. 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);
3. 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.
   In riferimento ai dati sensibili e, specificatamente ai dati idonei a rivelare le convinzioni religiose degli alunni deve rilevarsi che il trattamento di questa categoria di dati personali non necessità di alcun consenso poichè l'insegnamento religioso è disciplinato dalla L.5.6.1930 n.824, dal D.P.R. 12.2.1985 n.104, dai D.P.R. 21.7.1987 n.339 e n. 350 e dal T.U. 16.4.1994 n.297 artt. 309 e 310

Deve prestarsi invece attenzione al consenso nei casi in cui il trattamento di questi dati venga effettuato eventualmente per finalità non istituzionali e qualora si riferisca a confessioni religiose i cui rapporti non sono regolati con lo Stato sulla base di accordi o intese ai sensi degli art. 7 e 8 della Costituzione.

5.4 Modulistica

INF 02.01 - Modello per le informative agli interessati (generica)
INF 02.02 - Modello per l'informativa ai docenti
INF 02.03 - Modello per l'informativa ai fornitori

6 Diritti dell'interessato

6.1 Diritto di accesso ai dati personali

1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro identificativicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

a) dell'origine dei dati personali;
b) delle finalità e modalità del trattamento;
c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere identificativicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
c) l'attestazione che le operazioni di cui alle lettere a) e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati identificativicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di identificativicazione commerciale.

6.2 Esercizio dei diritti

1. I diritti di cui all'articolo 7 sono esercitati con richiesta rivolta senza formalità al titolare o al responsabile, anche per il tramite di un incaricato, alla quale è fornito idoneo riscontro senza ritardo.

2. I diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145, se i trattamenti di dati personali sono effettuati:

a) in base alle disposizioni del decreto-legge 3 maggio 1991, n. 143, convertito, con modificazioni, dalla legge 5 luglio 1991, n. 197, e successive modificazioni, in materia di riciclaggio;
b) in base alle disposizioni del decreto-legge 31 dicembre 1991, n. 419, convertito, con modificazioni, dalla legge 18 febbraio 1992, n. 172, e successive modificazioni, in materia di sostegno alle vittime di richieste estorsive;
c) da Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione;
d) da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità;
e) ai sensi dell'articolo 24, comma 1, lettera f), limitatamente al periodo durante il quale potrebbe derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive o per l'esercizio del diritto in sede giudiziaria;
f) da fornitori di servizi di identificativicazione elettronica accessibili al pubblico relativamente a identificativicazioni telefoniche in entrata, salvo che possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397;
g) per ragioni di giustizia, presso uffici giudiziari di ogni ordine e grado o il Consiglio superiore della magistratura o altri organi di autogoverno o il Ministero della giustizia;
h) ai sensi dell'articolo 53, fermo restando quanto previsto dalla legge 1° aprile 1981, n. 121.

3. Il Garante, anche su segnalazione dell'interessato, nei casi di cui al comma 2, lettere a), b), d), e) ed f), provvede nei modi di cui agli articoli 157, 158 e 159 e, nei casi di cui alle lettere c), g) ed h) del medesimo comma, provvede nei modi di cui all'articolo 160.

4. L'esercizio dei diritti di cui all'articolo 7, quando non riguarda dati di carattere oggettivo, può avere luogo salvo che concerna la rettificazione o l'integrazione di dati personali di tipo valutativo, relativi a giudizi, opinioni o ad altri apprezzamenti di tipo soggettivo, nonché l'indicazione di condotte da tenersi o di decisioni in via di assunzione da parte del titolare del trattamento.

6.3 Modalità di esercizio

1. La richiesta rivolta al titolare o al responsabile può essere trasmessa anche mediante lettera raccomandata, telefax o posta elettronica. Il Garante può individuare altro idoneo sistema in riferimento a nuove soluzioni tecnologiche. Quando riguarda l'esercizio dei diritti di cui all'articolo 7, commi 1 e 2, la richiesta può essere formulata anche oralmente e in tal caso è annotata sinteticamente a cura dell'incaricato o del responsabile.

2. Nell'esercizio dei diritti di cui all'articolo 7 l'interessato può conferire, per iscritto, delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può, altresì, farsi assistere da una persona di fiducia.

3. I diritti di cui all'articolo 7 riferiti a dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.

4. L'identità dell'interessato è verificata sulla base di idonei elementi di valutazione, anche mediante atti o documenti disponibili o esibizione o allegazione di copia di un documento di riconoscimento. La persona che agisce per conto dell'interessato esibisce o allega copia della procura, ovvero della delega sottoscritta in presenza di un incaricato o sottoscritta e presentata unitamente a copia fotostatica non autenticata di un documento di riconoscimento dell'interessato. Se l'interessato è una persona giuridica, un ente o un'associazione, la richiesta è avanzata dalla persona fisica legittimata in base ai rispettivi statuti od ordinamenti.

5. La richiesta di cui all'articolo 7, commi 1 e 2, è formulata liberamente e senza costrizioni e può essere rinnovata, salva l'esistenza di giustificati motivi, con intervallo non minore di novanta giorni.

6.3.1 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'Istituto Scolastico deve adottare una apposita procedura (INT 01.01) e disciplinare le modalità per rispondere tempestivamente alle richieste avanzate dagli interessati.
Inoltre predisporre un modulo (INT 01.02), che gli interessati possono richiedere all'Ufficio di segreteria, per l'esercizio delle diverse facoltà all'uopo previste.

6.4 Riscontro all'interessato

1. Per garantire l'effettivo esercizio dei diritti di cui all'articolo 7 il titolare del trattamento è tenuto ad adottare idonee misure volte, in particolare:

a) ad agevolare l'accesso ai dati personali da parte dell'interessato, anche attraverso l'impiego di appositi programmi per elaboratore finalizzati ad un'accurata selezione dei dati che riguardano singoli interessati identificati o identificabili;
b) a semplificare le modalità e a ridurre i tempi per il riscontro al richiedente, anche nell'ambito di uffici o servizi preposti alle relazioni con il pubblico.

2. I dati sono estratti a cura del responsabile o degli incaricati e possono essere identificativicati al richiedente anche oralmente, ovvero offerti in visione mediante strumenti elettronici, sempre che in tali casi la comprensione dei dati sia agevole, considerata anche la qualità e la quantità delle informazioni. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica.

3. Salvo che la richiesta sia riferita ad un particolare trattamento o a specifici dati personali o categorie di dati personali, il riscontro all'interessato comprende tutti i dati personali che riguardano l'interessato comunque trattati dal titolare. Se la richiesta è rivolta ad un esercente una professione sanitaria o ad un organismo sanitario si osserva la disposizione di cui all'articolo 84, comma 1.

4. Quando l'estrazione dei dati risulta particolarmente difficoltosa il riscontro alla richiesta dell'interessato può avvenire anche attraverso l'esibizione o la consegna in copia di atti e documenti contenenti i dati personali richiesti.

5. Il diritto di ottenere la identificativicazione in forma intelligibile dei dati non riguarda dati personali relativi a terzi, salvo che la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato.

6. La identificativicazione dei dati è effettuata in forma intelligibile anche attraverso l'utilizzo di una grafia comprensibile. In caso di identificativicazione di codici o sigle sono forniti, anche mediante gli incaricati, i parametri per la comprensione del relativo significato.

7. Quando, a seguito della richiesta di cui all'articolo 7, commi 1 e 2, lettere a), b) e c) non risulta confermata l'esistenza di dati che riguardano l'interessato, può essere chiesto un contributo spese non eccedente i costi effettivamente sopportati per la ricerca effettuata nel caso specifico.

8. Il contributo di cui al comma 7 non può comunque superare l'importo determinato dal Garante con provvedimento di carattere generale, che può individuarlo forfettariamente in relazione al caso in cui i dati sono trattati con strumenti elettronici e la risposta è fornita oralmente. Con il medesimo provvedimento il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato.

9. Il contributo di cui ai commi 7 e 8 è corrisposto anche mediante versamento postale o bancario, ovvero mediante carta di pagamento o di credito, ove possibile all'atto della ricezione del riscontro e comunque non oltre quindici giorni da tale riscontro.

7. Regolamentazione Dell'utilizzo Degli Strumenti Informatici

Lo scopo della presente sezione è descrivere le misure adottate dal Titolare del Trattamento in merito a:

- utilizzo di Internet da parte degli operatori dell'Istituto scolastico;
- tipo di informazioni conservate e tempi di conservazione relative alla navigazione web;
- utilizzo della posta elettronica da parte degli operatori dell'Istituto scolastico.

7.1 Riferimenti Normativi

Norma	Descrizione
Del. n.13 del 1 Marzo 2007	Linee guida del Garante per posta elettronica e internet

7.2 Responsabilità

È competenza del Titolare del Trattamento assicurare la funzionalità e il corretto impiego della posta elettronica e di internet da parte dei lavoratori, definendone le modalità di uso nell'ambito dell'attività lavorativa, per prevenire utilizzi indebiti e tutelare i lavoratori dalla possibilità di acquisizione e/o conoscenza da parte di altro personale dell'organizzazione e/o del Titolare del Trattamento di informazioni di carattere personale e privato.

7.3 Descrizione

Nei casi in cui l'utilizzo di internet e della posta elettronica, da parte dei lavoratori, costituisca oggetto di analisi da parte del Titolare del Trattamento o da parte di altro personale dell'organizzazione, si può configurare l'ipotesi di trattamento illecito di dati personali e sensibili, espressamente contenuti nei messaggi di posta elettronica o desumibili dalle pagine web visualizzate dal lavoratore. Si rende pertanto opportuno indicare chiaramente e in modo particolareggiato:

1. quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette;
2. in che misura e con quali modalità vengono effettuati controlli;
3. le soluzioni prefigurate per garantire,con la cooperazione del lavoratore, la continuità dell'attività lavorativa in caso di assenza del lavoratore stesso.

A tal fine l'Istituto scolastico ha adottato un disciplinare interno contenente la descrizione delle misure adottate in tema di utilizzo dei suddetti strumenti elettronici, pubblicizzato mediante affissione all'albo dell'Istituto scolastico e sottoposto ad aggiornamento periodico.

7.4 Modulistica

MOD 01.01 - Disciplinare interno sull'utilizzo degli strumenti elettronici
MOD 01.02 - Lettera di delega al fiduciario per il controllo della posta elettronica
MOD 01.03 - Verbale di comunicazione dei messaggi di posta elettronica al TdT

8 Allegati

8.1 Elenco dei modelli allegati

Allegato	Codice	Tipo di documento	Descrizione
X	ADS	Lettera di incarico	Incaricato gestione e manutenzione strumenti elettronici
X	BKP	Lettera di incarico	Incaricato delle copie di sicurezza delle banche dati
X	CDP	Lettera di incarico	Custode delle copie delle credenziali
X	DTEC_W	Lettera di incarico	Responsabile del trattamento dei dati in Out-Sourcing
X	DTEC_W2	Lettera di incarico	Indicazione di Titolare autonomo
X	IDT2	Lettera di incarico	Incaricato del trattamento dei dati personali
X	RAL	Lettera di incarico	Responsabili dell'accesso ai locali
X	RDT	Lettera di incarico	Responsabile della sicurezza dei dati personali
X	RDT6	Lettera di incarico	Responsabile di specifici trattamenti di dati personali
X	DTEC_A	Modello	Elenco degli archivi dei dati oggetto del trattamento
X	DTEC_B	Modello	Elenco delle sedi/uffici in cui vengono trattati i dati
X	DTEC_D	Modello	Sistemi di elaborazione per il trattamento dei dati
X	DTEC_E	Modello	Enti terzi a cui è affidato il trattamento dei dati in out-sourcing
X	DTEC_F	Modello	Personale autorizzato al trattamento dei dati
X	DTEC_G	Modello	Permessi di accesso ai dati
X	DTEC_H	Modello	Piano di formazione del personale autorizzato al trattamento dei dati
X	DTEC_J	Modello	Distribuzione dei compiti e delle responsabilità
X	DTEC_M	Modello	Criteri e procedure per garantire l'integrità dei dati
X	DTEC_N	Modello	Piano di formazione degli incaricati del back-up
	DTEC_Q	Modello	Report dei virus informatici rilevati
	DTEC_Q2	Modello	Report dei virus informatici rilevati da eliminare
	DTEC_R	Modello	Report dei contagi da Virus Informatici
	DTEC_R2	Modello	Report dei contagi da Virus Informatici Ripuliti
X	DTEC_S	Modello	Criteri di assegnazione delle credenziali d i accesso
	DTEC_T	Modello	Report annuale dei rischi hardware
	DTEC_U	Modello	Report annuale dei rischi sui software installati
X	DTEC_Z	Modello	Report annuale altri rischi
X		Inventario	Elenco dei Software installati

8.2 Altri allegati

Allegato	Codice	Tipo di documento	Descrizione
X	ADS 01.01	Verbale	Verbale annuale di nomina o verifica ADS
X	ADS 01.02	Elenco	Elenco Amministratori di Sistema Interni e Responsabili Esterni nel Trattamento Informatico dei dati
X	ADS 01.03	Lettera	Comunicazione al personale nominativi Amministratori di Sistema
X	ADS 01.04	Lettera	Nomina dell'amministratore di sistema interno
X	ADS 01.05	Lettera	Nomina Amministratori di Sistema Aule Informatiche
X	ADS 01.06	Lettera	Nomina a Responsabile Esterno nel Trattamento Informatico dei Dati
X	ADS 01.07	Lettera	Richiesta nominativi amministratori di sistema
X	ADS 01.07	Verbale	Verbale di verifica delle attività di Amministratore di Sistema
X	INT 01.01	Procedura	Procedura d'accesso ai dati
X	INT 01.02	Modulo	Modulo di richiesta d'accesso ai dati da parte degli interessati (ex art. 7)
X	INT 01.03	Registro	Registro Carico Scarico documentazione sensibile
X	INF 01.01	Informativa	Informativa Famiglie
X	INF 01.02	Informativa	Informativa Docenti
X	INF 01.03	Informativa	Informativa Fornitori
X	MOD 01.01	Regolamento	Disciplinare interno sull'utilizzo degli strumenti elettronici
X	MOD 01.02	Lettera	Lettera di delega al fiduciario per il controllo della posta elettronica
X	MOD 01.03	Verbale	Verbale di comunicazione dei messaggi di posta elettronica al TdT

8.3 Allegati normativi

Allegato	Descrizione
X	**CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI** (Decreto Legislativo del 30 giugno 2003 n. 169) completo di Allegti: A.1 Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica. A.2 Codice di deontologia e di buona condotta per il trattamento di dati personali per scopi storici. A.3 Codice di deontologia e di buona condotta per i trattamenti di dati personali a scopi statistici e di ricerca scientifica effettuati nell'ambito del sistema statistico nazionale. B – Disciplinare tecnico in materia di misure minime di sicurezza
X	**AUTORIZZAZIONI DIVERSE**
X	**DELIBERA GARANTE PRIVACY Nr 1 del 31.3.2004**
X	**TAVOLA DI CORRISPONDENZA L. 675/96 – D.LGS. 196/03**
X	**ALLEGATI DIVERSI e NORMATIVA RELATIVA ALLA VIDEOSORVEGLIANZA**

8.4 Registri

X	ReAL	Registro	ReAL Registro Accesso Locali
X	ReB	Registro	Registro Backup
X	SKRHW	Scheda	Scheda Rischio Hardware
X	SKRSW	Scheda	Scheda Rischio Software
X	SKRV	Scheda	Scheda Rilevazione contagio Virus

8.5 Gestione Passowrd e Credenziali

X	ReGP	Registro	Registro Gestione Password
X	SAI	Istruzioni	Sistema Autenticazione - istruzioni custodia password
X	SAIN	Istruzioni	Sistema Autenticazione - istruzioni custodia password - notebook
X	SAMP1	Modulo	Sistema Autenticazione - modulo prima consegna password
X	SAMP	Modulo	Sistema Autenticazione - modulo custodia password
X	SAN	Istruzioni	Sistema Autenticazione - note incaricato custodia pw