STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Realizzato da Studio AG.I.COM. per :

Istituto Tecnico Industriale Statale
"ALESSANDRO VOLTA"
Viale Giovanni XXIII°, 9
26900 LODI

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL DLGS 196/2003, E DEL DISCIPLINARE TECNICO ALLEGATO AL MEDESIMO DECRETO SUB B)

VERSIONE AGGIORNATA E RIVEDUTA IN OSSERVANZA DEL DECRETO DEL MINISTRO DELLA PUBBLICA ISTRUZIONE N° 305 DEL 7 DICEMBRE 2006 RECANTE "IDENTIFICAZIONE DEI DATI SENSIBILI E GIUDIZIARI TRATTATI E DELLE RELATIVE OPERAZIONI EFFETTUATE… omissis…"

INCLUDE LA NOMINA DELL'AMMINISTRATORE DI SISTEMA (Provv. Garante 27/11/2008).

PER AUTOPRESTAZIONE

La certificazione della data avviene tramite l'apposizione del timbro postale sul bollo o della firma digitale sul file o trasmettendo il medesimo mediante Posta Elettronica Certificata

CERTIFICAZIONE DELLA DATA

Termine ultimo di validità :

31 Marzo
2012

agicom@pec.agicomstudio.it
POSTA ELETTRONICA CERTIFICATA

FIRAS-SPP
Federazione Italiana Responsabili e Addetti alla Sicurezza
Servizio di Prevenzione e Protezione

Studio AG.I.COM. S.r.l. unipersonale
Via Guglielmo Marconi, 4 - 20077 MELEGNANO (MI)
Tel. 02-90601324 Fax 02-700527180 E-mail info@agicomstudio.it
P.IVA, C.F. e Iscrizione C.C.I.A.A. 05078440962
Capitale sociale : 10.000,00 Euro interamente versati

INTRODUZIONE

Il Decreto Legislativo 196 del 30 giugno 2003 si pone come Testo Unico in materia di riservatezza e protezione dei dati personali. L'esigenza di mettere mano in maniera così penetrante ad una materia che era stata già regolamentata recentemente (nel 1996 era entrata in vigore la Legge 675 che già aveva rappresentato un notevole passo avanti nella definizione di un diritto soggettivo alla riservatezza) è figlia delle grandi trasformazioni mediatiche che sta vivendo il nostro tempo.

Internet, in pochi anni, è divenuto il più importante strumento di comunicazione e di transito dei dati di tutto il mondo civilizzato; le nuove tecnologie hanno velocizzato in maniera sensibile l'accesso alla rete in modo da rendere facilmente realizzabili trasferimenti di enormi quantità di dati in pochissimi secondi.
La diffusione incontrollata dei sistemi di videosorveglianza, la prossima introduzione dei primi esempi di domotica, l'uso indiscriminato di tecniche di intercettazione, la biometria e ancora tanto altro non potevano essere lasciate alla coscienza dei loro utilizzatori.

Il 2009 si è chiuso con la piena entrata in vigore del Provvedimento del Garante per la protezione dei dati personali del 27 Novembre 2008 con cui si impone a molti soggetti impegnati nel trattamento dei dati sensibili, tra cui gli Istituti di istruzione, la nomina di un "Amministratore di sistema" che garantisca la corretta applicazione delle regole tecniche previste dall'Allegato B del Codice della privacy.

Alle inevitabili polemiche che accompagnano l'entrata in vigore di questa come della gran parte delle nuove normative, ci sentiamo di dare una risposta a favore di questo Testo Unico.
L'introduzione, nella Vostra infrastruttura informatica, di questo nuovo *modus operandi* consentirà a molti di Voi di sperimentare sistemi enormemente più efficienti in termini di protezione dei dati da perdite accidentali, da attacchi virali o anche solo da errori umani, di quelli tradizionalmente applicati.
Chissà che un guasto evitato, un virus intercettato o un errore a cui si possa facilmente porre rimedio non Vi facciano ringraziare di aver applicato alla Vostra realtà i principi di questa nuova "Legge sulla Privacy".

Luca Corbellini
Specialista in informatica giuridica
Amministratore Unico - Studio AG.I.COM. S.r.l.

REFERENZE

Lo Studio AG.I.COM. è uno dei maggiori protagonisti in tutta la Lombardia in materia di sicurezza informatica, protezione digitale dei dati riservati e messa in sicurezza delle infrastrutture logistiche ed informatiche in cui avviene il trattamento dei dati personali.
Oltre ad aver curato l'adeguamento di centinaia di segreterie di istituti di istruzione pubblica e privata, vanta una presenza molto significativa nel mondo dell'impresa per aver assunto la supervisione diretta delle procedure di adeguamento di importanti aziende dei settori chimico ed industriale.
Luca Corbellini è consulente per la privacy dell'Associazione Medici Legali Ambrosiana (A.M.L.A.), dell'Associazione Europea di Chirurgia Estetica (ASS.E.C.E.) nonché di alcune importanti multinazionali chimiche (Istituto delle Vitamine S.p.A., UNIVAR S.p.A., Gruppo DSM., ALKOR Deco S.p.A., Venilia S.r.l.).

INDICE

I° SEZIONE DEL DOCUMENTO – FINALITA', NORMATIVA, DEFINIZIONI

I. Scopo del documento 6

II. Ambito di applicazione del documento 6

III. Fonti del diritto 7

IV. I Soggetti del trattamento dei dati 8

Il Titolare del trattamento 8
Il Responsabile del trattamento 9
Gli Incaricati del trattamento 10
Il Custode delle parole chiave 10

II° SEZIONE DEL DOCUMENTO – LUOGHI, PERSONE, TRATTAMENTI

V. Sedi in cui avviene il trattamento e strumenti utilizzati 12

VI. Individuazione dei trattamenti eseguiti 13

Tabella B – Censimento dei trattamenti effettuati 13
Tabella C – Censimento dei trattamenti effettuati all'esterno 14
Tabella B2 – Descrizione dei trattamenti eseguiti mediante uso di elaboratori 15
Tabella B3 – Descrizione dei trattamenti eseguiti senza l'uso di elaboratori 16

VII. Individuazione dei soggetti del trattamento 17

VIII. Individuazione dei trattamenti eseguiti per categoria 18

Elenco dei soggetti incaricati del trattamento ex Art. 30 D.Lgs. 196/2003 19
Profili di autorizzazione degli incaricati del trattamento 20
Richiami al D.M. 305 del 07 Dicembre 2006 (SCHEDE DEI TRATTAMENTI) 22

III° SEZIONE DEL DOCUMENTO – AMMINISTRAZIONE DEL SISTEMA INFORMATICO

IX. Introduzione alla amministrazione della rete informatica 27

X. Cosa si intende per Amministratore di sistema 27

XI. Nomina dell'Amministratore di sistema 28

IV° SEZIONE DEL DOCUMENTO – ANALISI DEI RISCHI E MISURE MINIME

XII. Le misure di sicurezza globali 31

Uso di internet da parte dei soggetti del trattamento 31
Uso della posta elettronica da parte dei soggetti del trattamento 31
Uso del fax da parte dei soggetti del trattamento 32
Distruzione di documenti da parte dei soggetti del trattamento 32
Gestione della posta cartacea da parte dei soggetti del trattamento 32

XIII. Misure minime di sicurezza contro il rischio di perdita dei dati 33

Procedura di esecuzione del Back-up 33

XIV. Criteri per la tenuta di supporti digitali removibili 34

Criteri e procedure per il salvataggio ed il ripristino della disponibilità dei dati 35
Cifratura dei dati e separazione dei dati identificativi 35

XV. Virus informatici 35

XVI. Altre misure di sicurezza 35

Assegnazione nomi utente 35
Assegnazione parole chiave 36
Sicurezza delle trasmissioni dati 36
Personale autorizzato al trattamento 36

XVII. Manutenzione delle apparecchiature 37

XVIII. Il piano dei rischi 37

XIX. Analisi dei rischi – Danni causati dagli operatori 38

XX. Analisi dei rischi – Danni causati da malfunzionamenti 39

XXI. Analisi dei rischi – Danni causati da eventi fisici o atmosferici 40

XXII. Analisi dei rischi – Rischi specifici delle risorse connesse ad internet 41

V° SEZIONE DEL DOCUMENTO – VALUTAZIONI PROGRAMMATICHE

XXIII. Altre misure minime di sicurezza da adottare 43

XXIV. Formazione degli incaricati 43

XXV. Notificazione al Garante 44

XXVI. Menzione a bilancio 44

XXVII. Revisioni 44

SCADENZIARIO E ASSUNZIONE DELLE RESPONSABILITA' 45

I° SEZIONE
DEL DOCUMENTO

(STATICA)

FINALITA'
NORMATIVA
DEFINIZIONI

I. SCOPO DEL DOCUMENTO

Scopo di questo documento è di delineare il quadro delle misure minime di sicurezza, organizzative, fisiche e logiche, da adottare per il trattamento dei dati personali effettuato all'interno della struttura, al fine di conoscere il proprio stato di sicurezza rispetto ai rischi di violazione della riservatezza e perdita di dati.
Esso viene redatto entro il 31 Marzo di ogni anno per una perfetta aderenza del contenuto dello stesso alle modificate esigenze di sicurezza nonché, al variare nel tempo, del profilo dei rischi incombenti sui dati.

Il modello grafico adottato è stato realizzato in proprio dallo Studio AG.I.COM. sulla base delle indicazioni acquisite tramite la "Guida alla redazione del DPS" pubblicata sul sito del Garante.

In particolare nel Documento Programmatico Sulla Sicurezza (DPS) vengono definiti i criteri per:

I. La protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
II. I criteri e le procedure per assicurare l'integrità dei dati;
III. I criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
IV. L'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

Il presente documento è redatto e firmato in calce dal Titolare del trattamento.

II. AMBITO DI APPLICAZIONE DEL DOCUMENTO

Il presente Documento Programmatico Sulla Sicurezza (DPS) è applicato ai trattamenti di dati che avvengono all'interno delle strutture di competenza del titolare, ovunque esse si trovino sul territorio italiano.

Nel presente documento si forniscono idonee informazioni riguardanti :

a) l'elenco dei trattamenti di dati personali (*punto 19.1 del disciplinare)* mediante :

- Individuazione tipologia di dati trattati
- Descrizione aree, locali e strumenti con cui si esegue il trattamento
- Elaborazione mappa dei trattamenti effettuati

b) la distribuzione dei compiti e delle responsabilità (*mansionario privacy di cui al punto 19.2 del disciplinare*) e la previsione di interventi formativi degli incaricati individuati dal presente *(punto 19.6 del disciplinare)*

c) l'analisi dei rischi che incombono sui dati *(punto 19.3 del disciplinare)*

d) le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati *(punto 19.4 del disciplinare)*

e) i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento *(punto 19.5 del disciplinare)*

f) i criteri da adottare per garantire l'adozione delle misure minime di sicurezza dei dati

g) le procedure per seguire il controllo dello stato di sicurezza

Il Documento Programmatico Sulla Sicurezza (DPS) si applica al trattamento di tutti i dati personali per mezzo di:

- Strumenti vari di elaborazione (ad es.: cartacei, visivi e audiovisivi, ecc.);
- Strumenti elettronici di elaborazione.

Il Documento Programmatico Sulla Sicurezza (DPS) deve essere conosciuto ed applicato da tutti gli uffici ed i reparti su cui è strutturato l'ente titolare del trattamento.

III. FONTI DEL DIRITTO

Il Documento Programmatico Sulla Sicurezza e le disposizioni che esso contiene sono conformi a quanto previsto dal D.P.R. n° 318 del 28 luglio 1999, dalla Legge n° 325 del 3 novembre 2000 e dal D.Lgs 196 del 30 giugno 2003.

Con particolare riferimento alla tipologia del soggetto obbligato alla redazione del presente documento, Istituto di Istruzione Statale, esso è stato rivisto nel Gennaio 2007 ed è conforme ai principi indicati nel Decreto del Ministro della Pubblica Istruzione N° 305 del 15 Gennaio 2007, denominato anche "Regolamento per i dati sensibili e giudiziari del Ministero della Pubblica Istruzione".

Per una maggiore comprensione del documento, riteniamo utile definire i concetti sotto elencati che, in seguito, si daranno per acquisiti :

Per **sistema informativo** s'intende l'insieme delle risorse umane, delle regole organizzative, delle risorse hardware e software (applicazioni e dati), dei locali e della documentazione che, nel loro complesso, consentono di acquisire, memorizzare, elaborare, scambiare e trasmettere informazioni inerenti alle attività dello studio legale.

I dati personali contenuti nel sistema informativo **devono essere protetti** adottando le misure minime di sicurezza previste dal D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali" (d'ora in poi codice) artt. 33-36, con le modalità descritte dal **disciplinare tecnico allegato B** al codice stesso.

Ai fini del **D. Lgs. 196/2003** si intende per:

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

b) "**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;

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

d) "**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;

e) "**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;

f) "**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;

g) "**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;

h) "**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

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

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

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

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

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

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

q) "**Garante**", l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

[…]

Ai fini del **D. Lgs. 196/2003** si intende, inoltre, per:

a) "**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;

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

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

d) "**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;

e) "**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;

f) "**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;

g) "**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.

IV. SOGGETTI DEL TRATTAMENTO DEI DATI

La normativa vigente ha definito talune figure fondamentali a cui attribuisce ruoli chiave nei vari passaggi su cui è strutturato il trattamento dei dati.

Queste figure sono :

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

La persona giuridica o l'Istituzione statale è, "*ope legis*", per mezzo del suo rappresentante legale, TITOLARE DEL TRATTAMENTO ai sensi dell'Art. 4 comma 1 lettera f) del D.Lgs 196/2003 e, quale Titolare del trattamento gli è consentito individuare, nominare e incaricare per iscritto un Responsabile del trattamento dei dati, che assicuri e garantisca che vengano adottate le misure di sicurezza minime previste dalla legge.
Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto.

Il titolare svolge le funzioni di "**titolare del trattamento dei dati personali**" e decide riguardo alle modalità di trattamento e agli strumenti utilizzati, ivi **compreso il profilo della sicurezza**. Il titolare può essere una **persona fisica**, una **persona giuridica** […], **associazione** od organismo (art. 4 lett. f) del codice). E' previsto, inoltre, che le decisioni possano essere prese **anche unitamente ad altro titolare** (art. 4 lett. f) del codice).

Il Titolare del trattamento dei dati:

- adotta (art. 31 "codice"), riguardo al trattamento di dati personali, le **misure minime di sicurezza** (art. 33 "codice") con le modalità previste dal Titolo V, Capo II del "codice" e dal disciplinare tecnico contenuto nell'allegato B) del "codice" stesso;
- adotta il **documento programmatico della sicurezza entro il 31 marzo di ogni anno**, ai sensi della regola 19 all. B del codice, vigilando sulla sua effettiva applicazione.
  nel caso in cui per obiettive ragioni tecniche, all'entrata in vigore del codice, non fosse stato possibile applicare immediatamente, in tutto o in parte, le misure minime di sicurezza (ivi compreso il piano di sicurezza), il titolare avrà provveduto alla **redazione di un documento a data certa descrivente tali ragioni, da conservare presso la propria struttura**. (art. 180 c.2 del codice).

In casi particolari il Titolare:

- adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, ricevendo dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del disciplinare tecnico allegato al "codice" (art. 25 all. B "codice");

- verifica l'adeguamento delle misure minime di sicurezza previste per la protezione dei dati personali all'aggiornamento periodico predisposto dal Ministro della Giustizia di concerto con il Ministro per le innovazioni e le tecnologie, in relazione all'evoluzione tecnica e all'esperienza maturata nel settore (art. 36 del "codice").

IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

In relazione all'attività del Titolare del trattamento, è prevista come facoltativa, la nomina del Responsabile del trattamento, con compiti specifici in relazione alle funzioni svolte. Il Titolare del trattamento se vuole, affida al Responsabile del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più Incaricati del trattamento.
Il Responsabile del trattamento dei dati ha il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco dei trattamenti effettuati;

- Attribuire ad ogni Utente (USER) o incaricato un Codice identificativo personale (USER ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;

- Autorizzare i singoli incaricati del trattamento e della manutenzione, qualora utilizzino elaboratori accessibili in rete e nel caso di trattamento di dati sensibili e giudiziari; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibile al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;

- Verificare, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali;

- Garantire che tutte le misure di sicurezza riguardanti i dati in possesso della società siano applicate all'interno ed eventualmente al di fuori della stessa, qualora cedute a soggetti terzi, quali Responsabili del trattamento, tutte o parte delle attività di trattamento;

- Informare il Titolare nell'eventualità che siano rilevati dei rischi.

Il Titolare del trattamento dei dati deve informare il Responsabile del trattamento dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal DLGS 196/2003.

Al Responsabile del trattamento il Titolare deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

INCARICATI DEL TRATTAMENTO DEI DATI

Al Responsabile del trattamento è affidato il compito di nominare, con comunicazione scritta, uno o più Incaricati del trattamento dei dati. La nomina di ciascun Incaricato del trattamento dei dati deve essere effettuata con lettera di incarico in cui sono specificati i compiti che gli sono affidati.
Gli Incaricati del trattamento 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 deve essere assegnata una parola chiave e un codice identificativo personale.
La nomina degli incaricati del trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli Incaricati del trattamento il Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli incaricati è a tempo indeterminato e decade per revoca, per dimissioni o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

CUSTODE DELLE PAROLE CHIAVE

È compito del Custode delle parole chiave gestire e custodire le *password* per l'accesso ai dati da parte degli incaricati.
Il Custode delle parole chiave deve predisporre, per ogni Incaricato del trattamento, una busta sulla quale è indicato lo USER ID utilizzato: all'interno della busta deve essere indicata la *password* usata per accedere alla banca di dati.
Le buste con le *password* debbono essere conservate in luogo sicuro e protetto.
Il Custode delle parole chiave deve revocare tutte le *password* non utilizzate per un periodo superiore a sei (6) mesi.
Il Titolare del trattamento nomina un Custode delle parole chiave a cui è conferito il compito di custodire le *password* per l'accesso ai dati archiviati nei sistemi di elaborazione dei dati.
La nomina del Custode delle parole chiave deve essere effettuata con lettera di incarico.
La nomina di Custode delle parole chiave deve essere controfirmata dall'interessato per presa visione e copia della nomina accettata deve essere conservata in luogo sicuro a cura del Responsabile del trattamento, se diverso dal Custode delle parole chiave.
Il Responsabile del trattamento deve informare il Custode delle parole chiave della responsabilità che gli è stata affidata in relazione a quanto disposto dalle normative in vigore ed in particolare di quanto stabilito dal DLGS 196/2003
Al Custode delle parole chiave, il Responsabile del trattamento deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina del Custode delle parole chiave è a tempo indeterminato e decade per revoca o per dimissioni dello stesso.
La nomina del Custode delle parole chiave può essere revocata in qualsiasi momento dal Titolare del trattamento senza preavviso ed essere affidata ad altro soggetto.

II° SEZIONE
DEL DOCUMENTO

(ANALITICO-DESCRITTIVA)

LUOGHI
PERSONE
TRATTAMENTI

V. SEDI IN CUI VENGONO TRATTATI I DATI E STRUMENTI UTILIZZATI

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

Indipendentemente dal luogo ove viene eseguito il trattamento, il Responsabile del trattamento vigila affinché esso avvenga entro locali sicuri ed opera di personale autorizzato.

Per l'ente in oggetto le sedi vengono riportate nella tabella seguente :

LUOGHI IN CUI AVVIENE IL TRATTAMENTO DEI DATI

Tabella A

SL	SEDE LEGALE	Viale Papa Giovanni XXIII, 9 26900 LODI (LO)

VI. INDIVIDUAZIONE DEI TRATTAMENTI DEI DATI EFFETTUATI

Al Responsabile del trattamento dei dati 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 cartaceo deve essere classificato in relazione alle informazioni in esso contenute indicando se si tratta di dati personali, sensibili, giudiziari o altro.

A fini classificatori abbiamo ritenuto utile suddividere i trattamenti di competenza del Titolare scrivente secondo questa logica :

Tabella B	Pagina 13	Trattamenti dati eseguiti all'interno di una delle sedi di cui alla Tabella A
Tabella B2	Pagina 15	Trattamenti interni eseguiti avvalendosi di strumenti informatici
Tabella B3	Pagina 16	Trattamenti interni eseguiti senza avvalersi di strumenti informatici
Tabella C	Pagina 14	Trattamenti dati affidati a soggetti esterni alla struttura del Titolare

Tabella B

CENSIMENTO DEI TRATTAMENTI E REPARTI IN CUI ESSO AVVIENE

ID	Descrizione sintetica del Trattamento	Categorie interessate dal trattamento	Natura dati (1)	Strutture entro le quali avviene il trattamento	Luogo (2)	Locale o Reparto in cui avviene il trattamento	Formato dei dati trattati (3)
T1	**Assistenza scolastica (amministrazione degli studenti)** ISCRIZIONE ALUNNI PRATICHE HANDICAP ALUNNI DENUNCE INFORTUNI ALUNNI ESAMI DI STATO TENUTA REGISTRO DIPLOMI CERTIFICAZIONI ALUNNI RICH. / TRASM. DOCUMENTI ALUNNI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI VERBALI ORGANI COLLEGIALI OSSERVATORIO OBBLIGO FORMATIVO SPORTELLO DIDATTICA	Alunni e Genitori	S/G	Uffici di segreteria	SL	Uffici di segreteria	D/C
T2	**Trattamento giuridico ed economico del personale dipendente** GESTIONE DELLE GRADUATORIE RACCOLTA INIZIALE DATI DIPENDENTI STIPULA CONTRATTI DI LAVORO RILEVAZIONE ASSENZE PERSONALE ELABORAZIONE RETRIBUZIONI RICOSTRUZIONE CARRIERA ISTRUZIONE PRATICHE DI PENSIONE DENUNCE INFORTUNI PERSONALE GESTIONE DOMANDE PRESTITI PERS. PRATICHE PROCEDIMENTI DISCIPLINARI CERTIFICAZIONI PERSONALE PRATICHE MOBILITA' PERSONALE PRATICHE INIDONEITA' PERSONALE PRATICHE EX LEGGE 104 770 / IRAP PERMESSI SINDACALI GESTIONE T.F.R. PERMESSI – CONGEDI – FERIE RICH./ TRASM. DOCUMENTI PERSONALE RISCATTO PENSIONE E LIQUIDAZIONE SCIOPERO – TRASMISSIONE DATI	Personale docente e non docente	S/G	Uffici di segreteria	SL	Uffici di segreteria	D/C
T3	**Gestione fornitori di beni e servizi**	Fornitori	P	Uffici di segreteria	SL	Uffici di segreteria	D/C
T4	**Gestione posta elettronica e cartacea**	Tutti	P	Uffici di segreteria	SL	Uffici di segreteria	D/C

(1) NATURA DEI DATI ..... P = meramente personali S = sensibili G = giudiziari

(2) LUOGO ..... Si faccia riferimento a quanto indicato alla TABELLA A

(3) FORMATO DEI DATI TRATTATI ..... D = digitali / informatici C = cartacei

Alcuni trattamenti di dati personali possono essere stati affidati all'esterno della struttura del titolare, per questi è mandatorio indicarne gli estremi, identificarne il soggetto esterno ed acquisire idonea autocertificazione degli impegni assunti da questo in ordine alla regolare tenuta dei dati a lui affidati :

CENSIMENTO DEI TRATTAMENTI AFFIDATI ALL'ESTERNO

Tabella C

ID	Descrizione sintetica dell'attività esternalizzata	Trattamenti interessati	Soggetto esterno	Descrizione criteri ed impegni assunti dal soggetto esterno per l'adozione delle misure minime
E1	**Adempimenti e formazione in materia di SICUREZZA DEI DATI PERSONALI (PRIVACY) (D.Lgs 196/2003)**	T1 e T2	Studio AG.I.COM. S.r.l. Via Guglielmo Marconi, 4 MELEGNANO (MI)	Il soggetto esterno assume l'incarico, ai sensi dell'Art. 29 D.Lgs 196/2003 di RESPONSABILE "ESTERNO" DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal "Codice della Privacy" per chi esercita un trattamento di dati personali in proprio o conto terzi.
E2	**Adempimenti e formazione in materia di SICUREZZA ed IGIENE DEL LAVORO (D.Lgs 81/2008)**	T1 e T2	Giancarlo Boldini Viale Papa Giovanni XXIII, 9 26900 LODI	Il soggetto esterno assume l'incarico, ai sensi dell'Art. 29 D.Lgs 196/2003 di RESPONSABILE "ESTERNO" DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal "Codice della Privacy" per chi esercita un trattamento di dati personali in proprio o conto terzi.
E3	**Servizio di SUPPORTO PSICOLOGICO a Studenti, Genitori e Docenti dell'Istituto**	T1	Dott.ssa Vincenzina Mandarini (presso I.I.S. Volta) Dott.ssa Giada Sposito (presso I.I.S. Volta)	Il soggetto esterno assume l'incarico, ai sensi dell'Art. 29 D.Lgs 196/2003 di RESPONSABILE "ESTERNO" DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal "Codice della Privacy" per chi esercita un trattamento di dati personali in proprio o conto terzi.
E4	**Attività di sorveglianza Sanitaria MEDICO COMPETENTE (D.Lgs 81/2008)**	T2	Dott. Mennoia Nunzio Valerio Via Ungaretti, 1 CARBONARA TICINO (PV)	Il soggetto esterno assume l'incarico, ai sensi dell'Art. 29 D.Lgs 196/2003 di RESPONSABILE "ESTERNO" DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal "Codice della Privacy" per chi esercita un trattamento di dati personali in proprio o conto terzi.
E5	**Attività di gestione informatica delle presenze degli studenti**	T1	MASTER TRAINING S.r.l. Via Timolini, 18 CORREGGIO (RE)	Il soggetto esterno assume l'incarico, ai sensi dell'Art. 29 D.Lgs 196/2003 di RESPONSABILE "ESTERNO" DEL TRATTAMENTO DEI DATI PERSONALI e si obbliga ai doveri di riservatezza e di organizzazione previsti dal "Codice della Privacy" per chi esercita un trattamento di dati personali in proprio o conto terzi.

In considerazione della difficoltà di eseguire controlli e verifiche presso strutture esterne alla propria, e vista la non eccezionale delicatezza dei dati affidati all'esterno, il Titolare del trattamento dei dati ritiene adeguato richiedere al soggetto esterno, a garanzia della corretta esecuzione del trattamento, un'autocertificazione dell'osservanza dei criteri individuati dal D.Lgs 196/2003 quali "minimi" per eseguire un trattamento di dati.

Resta comunque salvo l'obbligo per tutti gli incaricati del trattamento che intrattengano rapporti con il soggetti esterno, di richiamare l'osservanza delle misure minime nonché di segnalare, senza ritardo alcuno, al responsabile del trattamento, eventuali difformità rispetto a quanto autocertificato.

DESCRIZIONE ULTERIORE DEI TRATTAMENTI DI DATI PERSONALI INTERNI ALLA STRUTTURA DEL TITOLARE, CHE AVVENGONO MEDIANTE L'UTILIZZO DI STRUMENTI INFORMATICI

Tabella B2

ID	Denominazione banca dati	Luogo custodia dei dati in linea	Tipo e luogo custodia supporti di back-up	Tipologie dispositivi di accesso (4)	Tipologia di interconnessione (5)
T1	**Assistenza scolastica (amministrazione degli studenti)** ISCRIZIONE ALUNNI PRATICHE HANDICAP ALUNNI DENUNCE INFORTUNI ALUNNI ESAMI DI STATO TENUTA REGISTRO DIPLOMI CERTIFICAZIONI ALUNNI RICH. / TRASM. DOCUMENTI ALUNNI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI VERBALI ORGANI COLLEGIALI OSSERVATORIO OBBLIGO FORMATIVO SPORTELLO DIDATTICA	**SERVER**	I SUPPORTI DI BACKUP VENGONO CUSTODITI DALL'INCARICATO IN MANIERA SICURA DAI RISCHI CONNESSI ALLA DIFFUSIONE ED ALLA DISTRUZIONE DEGLI STESSI	PCOK	LAN
T2	**Trattamento giuridico ed economico del personale** GESTIONE DELLE GRADUATORIE RACCOLTA INIZIALE DATI DIPENDENTI STIPULA CONTRATTI DI LAVORO RILEVAZIONE ASSENZE PERSONALE ELABORAZIONE RETRIBUZIONI RICOSTRUZIONE CARRIERA ISTRUZIONE PRATICHE DI PENSIONE DENUNCE INFORTUNI PERSONALE GESTIONE DOMANDE PRESTITI PERS. PRATICHE PROCEDIMENTI DISCIPLINARI CERTIFICAZIONI PERSONALE PRATICHE MOBILITA' PERSONALE PRATICHE INIDONEITA' PERSONALE PRATICHE EX LEGGE 104 770 / IRAP PERMESSI SINDACALI GESTIONE T.F.R. PERMESSI – CONGEDI – FERIE RICH./ TRASM. DOCUMENTI PERSONALE RISCATTO PENSIONE E LIQUIDAZIONE SCIOPERO – TRASMISSIONE DATI	**SERVER**	I SUPPORTI DI BACKUP VENGONO CUSTODITI DALL'INCARICATO IN MANIERA SICURA DAI RISCHI CONNESSI ALLA DIFFUSIONE ED ALLA DISTRUZIONE DEGLI STESSI	PCOK	LAN
T3	**Gestione fornitori di beni e servizi**	**SERVER**	I SUPPORTI DI BACKUP VENGONO CUSTODITI DALL'INCARICATO IN MANIERA SICURA DAI RISCHI CONNESSI ALLA DIFFUSIONE ED ALLA DISTRUZIONE DEGLI STESSI	PCOK	LAN
T4	**Gestione posta elettronica e cartacea**	**SERVER**	I SUPPORTI DI BACKUP VENGONO CUSTODITI DALL'INCARICATO IN MANIERA SICURA DAI RISCHI CONNESSI ALLA DIFFUSIONE ED ALLA DISTRUZIONE DEGLI STESSI	PCOK	LAN

(4) TIPOLOGIA DISPOSITIVI DI ACCESSO .....

PCOK = Personal Computer equipaggiati con sistemi operativi adeguati
PCKO = Personal Computer equipaggiati con sistemi operativi obsoleti
PALM = Palmari
TEL = Telefoni cellulari

(5) TIPOLOGIA DI INTERCONNESSIONE .....

LAN = Rete fisica su cavo
WL = Rete wireless
BT = Rete Bluetooth
INET = Internet
GEO = Rete geografica

DESCRIZIONE ULTERIORE DEI TRATTAMENTI DI DATI PERSONALI INTERNI ALLA STRUTTURA DEL TITOLARE, CHE AVVENGONO MEDIANTE L'UTILIZZO DI STRUMENTI NON INFORMATICI

Tabella B3

ID	Denominazione banca dati	Luogo custodia dei dati cartacei	Sistema di protezione di accesso previsto (6)	Sistema di sicurezza anti-distruzione previsto (7)	Luogo di archiviazione storica	Sistema di protezione di accesso previsto per l'archivio (6)	Sistema di sicurezza anti-distruzione previsto per l'archivio (7)
T1	**Assistenza scolastica (amministrazione degli studenti)** ISCRIZIONE ALUNNI PRATICHE HANDICAP ALUNNI DENUNCE INFORTUNI ALUNNI ESAMI DI STATO TENUTA REGISTRO DIPLOMI CERTIFICAZIONI ALUNNI RICH. / TRASM. DOCUMENTI ALUNNI NULLAOSTA CORRISPONDENZA SCUOLA-GENITORI VERBALI ORGANI COLLEGIALI OSSERVATORIO OBBLIGO FORMATIVO SPORTELLO DIDATTICA	ARMADI CHIUSI DI SEGRETERIA	KEY	EST	LOCALE ARCHIVIO CHIUSO A CHIAVE	KEY	EST
T2	**Trattamento giuridico ed economico del personale** GESTIONE DELLE GRADUATORIE RACCOLTA INIZIALE DATI DIPENDENTI STIPULA CONTRATTI DI LAVORO RILEVAZIONE ASSENZE PERSONALE ELABORAZIONE RETRIBUZIONI RICOSTRUZIONE CARRIERA ISTRUZIONE PRATICHE DI PENSIONE DENUNCE INFORTUNI PERSONALE GESTIONE DOMANDE PRESTITI PERS. PRATICHE PROCEDIMENTI DISCIPLINARI CERTIFICAZIONI PERSONALE PRATICHE MOBILITA' PERSONALE PRATICHE INIDONEITA' PERSONALE PRATICHE EX LEGGE 104 770 / IRAP PERMESSI SINDACALI GESTIONE T.F.R. PERMESSI – CONGEDI – FERIE RICH./ TRASM. DOCUMENTI PERSONALE RISCATTO PENSIONE E LIQUIDAZIONE SCIOPERO – TRASMISSIONE DATI	ARMADI CHIUSI DI SEGRETERIA	KEY	EST	LOCALE ARCHIVIO CHIUSO A CHIAVE	KEY	EST
T3	**Gestione fornitori di beni e servizi**	ARMADI CHIUSI DI SEGRETERIA	KEY	EST	LOCALE ARCHIVIO CHIUSO A CHIAVE	KEY	EST
T4	**Gestione posta elettronica e cartacea**	ARMADI CHIUSI DI SEGRETERIA	KEY	EST	LOCALE ARCHIVIO CHIUSO A CHIAVE	KEY	EST

(6) PROTEZIONE DI ACCESSO ..... KEY = Chiave / Serratura / Combinazione
BLD = Cassaforte / Armadio blindato
BIO = Sistema di accesso biometrico

(7) SICUREZZA ANTI-DISTRUZIONE ..... EST = Estintore regolarmente revisionato
ANTI = Sistema antincendio

VII. INDIVIDUAZIONE DEI SOGGETTI DEL TRATTAMENTO

Il trattamento dei dati personali deve avvenire esclusivamente a cura di taluni soggetti ben individuati dalla legge (Titolare del trattamento), dal Titolare del trattamento (Responsabile del trattamento, Custode delle parole chiave) o dal Responsabile del trattamento (Incaricati del trattamento).
A nessuno, al di fuori di questa sfera di soggetti, è consentito di venire a contatto con i dati personali trattati.

In questa pagina del documento vengono individuati, nominativamente, alla data di redazione dello stesso, i soggetti su cui è imperniato il trattamento dei dati (Titolare, Responsabile e Custode delle parole chiave).

Di seguito invece, indicheremo le classi (gruppi) di incaricati presenti all'interno della struttura e definiremo i poteri loro assegnati. La definizione nominativa sempre aggiornata degli Incaricati del trattamento, attesa la frequente loro precarietà nell'incarico dovuta alla tipologia del rapporto di lavoro, è lasciata alle lettere di incarico.

ORGANIGRAMMA SOGGETTI INTERESSATI AL TRATTAMENTO DEI DATI – FUNZIONI CHIAVE

SOGGETTO	CRITERIO			
TITOLARE del TRATTAMENTO	Persona giuridica nella persona del suo legale rappresentante	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Luciana TONARELLI Dirigente Scolastico TUTTE LE SEDI	INDIVIDUATO "OPE LEGIS"
RESPONSABILE del TRATTAMENTO per la SEGRETERIA	Individuato personalmente dal Titolare del trattamento	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Maria SURACE Direttore SS.GG.AA. TUTTE LE SEDI	NOMINATO CON LETTERA DI INCARICO
RESPONSABILE del TRATTAMENTO per la DOCENZA	Individuato personalmente dal Titolare del trattamento	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Luciana TONARELLI Docente TUTTE LE SEDI	NOMINATO CON LETTERA DI INCARICO
CUSTODE delle PAROLE CHIAVE	Individuato personalmente dal Titolare del trattamento	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Maria SURACE Direttore SS.GG.AA. TUTTE LE SEDI	NOMINATO CON LETTERA DI INCARICO
INCARICATO del BACKUP	Individuato personalmente dal Responsabile del trattamento	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Studio AG.I.COM Srl (out sourcing) Esterno TUTTE LE SEDI	NOMINATO CON LETTERA DI INCARICO
AMMINISTRATORE di SISTEMA	Individuato personalmente dal Responsabile del trattamento	NOME E COGNOME RUOLO LUOGO DI RIFERIMENTO (*)	Luca CORBELLINI Consulente esterno INFRASTRUTTURA DI RETE DI SEGRETERIA	NOMINATO CON LETTERA DI INCARICO

(*) Per la lettura del luogo di riferimento si veda la **TABELLA A** di Pagina 12.

VIII. INDIVIDUAZIONE DEI TRATTAMENTI ESEGUITI PER CATEGORIA

All'interno del comparto scolastico è facile associare taluni trattamenti dati ad alcune categorie di lavoratori operanti all'interno della struttura del titolare. Ferme restando le peculiarità emergenti dalle lettere di incarico consegnate ai singoli incaricati del trattamento, rileviamo alcuni tratti comuni :

DESCRIZIONE DEI TRATTAMENTI ESEGUITI DA CIASCUNA CATEGORIA DI AMMESSA AL TRATTAMENTO

Tabella D

ID	Denominazione categoria	Banche dati a cui ha accesso	Struttura di riferimento	Strumenti CARTACEI	Strumenti INFORMATICI
DS	DIRIGENTE SCOLASTICO	1) FASCICOLI DI TUTTO IL PERSONALE 2) VERBALI ASSEMBLEE ORGANI COLLEGIALI 3) PROGRAMMAZIONE RELATIVA STATO DI DISAGIO DI TUTTE LE CLASSI 4) PROTOCOLLO RISERVATO 5) FASCICOLO DEL PERSONALE IN PROVA 6) REGISTRI DI CLASSE E PERSONALI DEL DOCENTE	Dirigenza	Armadio e cassettiera	Archivio software gestionale Gestione anagraf. Alunni Gestione Esiti finali Gestione anagraf. Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
DA	DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI	1) FASCICOLI DI TUTTO IL PERSONALE 2) ANAGRAFE DEI FORNITORI ED I CONTRATTI 3) DOCUMENTAZIONE CONTABILE E FINANZIARIA 4) DOCUMENTAZIONE DIDATTICA DA ARCHIVIARE 5) REGISTRO INFORTUNI 6) PROTOCOLLO	Ufficio D.S.G.A. Segreteria Archivio	Armadio e cassettiera	Archivio software gestionale Gestione anagraf. Alunni Gestione Esiti finali Gestione anagraf. Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
AA	ASSISTENTE AMMINISTRATIVO	1) FASCICOLI DI TUTTO IL PERSONALE 2) ANAGRAFE DEI FORNITORI ED I CONTRATTI 3) DOCUMENTAZIONE CONTABILE E FINANZIARIA 4) DOCUMENTAZIONE DIDATTICA DA ARCHIVIARE 5) REGISTRO INFORTUNI 6) PROTOCOLLO	Segreteria Archivio	Armadi e cassettiere	Archivio software gestionale Gestione anagraf. Alunni Gestione Esiti finali Gestione anagraf. Personale Gestione Trasferimenti Gestione Rapporti EE.LL. Gestione Rapporti ASL Gestione graduatorie Gestione Infortuni Gestione Posta elettronica Archivio Microsoft OFFICE
D	DOCENTE	1) REGISTRO DI CLASSE 2) REGISTRO DEI VERBALI CONSIGLIO DI CLASSE E INTERCLASSE 3) DOCUMENTI DI PROGRAMMAZIONE DIDATTICA 4) DOCUMENTI RELATIVI ALL'HANDICAP IN CLASSE 5) CERTIFICATI MEDICI ALLIEVI DELLA CLASSE 6) CORRISPONDENZA CON LE FAMIGLIE 7) REGISTRO PERSONALE 8) ELABORATI DEI PROPRI ALLIEVI	Aula docenti	Armadio e cassettiera	NESSUNO
CS	COLLABORATORE SCOLASTICO	1) FOTOCOPIA DI DOCUMENTI PERSONALI 2) ESECUZIONE PULIZIA LOCALI SEGRETERIA / ARCHIVI	Locale fotocopie Segreteria Archivio	Fotocopiatrice	NESSUNO

ELENCO DEI SOGGETTI INCARICATI DEL TRATTAMENTO NOMINATI EX ART. 30 D.LGS 196/2003

NOME e COGNOME	FUNZIONE	PROFILI DI AUTORIZZAZIONE (POLICIES)												
		DIDATTICA	PERSONALE	AMMINISTRATIVA	AFFARI GENERALI	PROTOCOLLO	FAX	POSTA ELETTRONICA	BACK-UP	COLLABORATORE DEL D.S.	COORDINATORE DI PLESSO	SICUREZZA (Dlgs 81/08)	FORMAZIONE CLASSI	COMITATO DI VALUTAZIONE
Maria Filomena VORTICE	ASSISTENTE AMM.VO		X	X										
Mara LA MOLA	ASSISTENTE AMM.VO		X	X										
Ernesta MASCOLO	ASSISTENTE AMM.VO		X											
Mara CARBONE	ASSISTENTE AMM.VO		X											
Scilla FALCIANI	ASSISTENTE AMM.VO	X						X						
Giorgio DI MINICA	ASSISTENTE AMM.VO	X				X								
Vittorina ZAMPERONI	ASSISTENTE AMM.VO	X				X								
Daniela CAMPANA	ASSISTENTE AMM.VO	X				X								
Ermelinda BANDINO	ASSISTENTE AMM.VO	X				X								
AnnaMaria CARINELLI	ASSISTENTE AMM.VO	X				X								
Daniela FERMI	ASSISTENTE AMM.VO	X				X								
Grazia ACUCELLA	ASSISTENTE AMM.VO			X	X									
LIZZI GIOVANNA	ASSISTENTE AMM.VO			X	X									
Mario ARFANI	DOCENTE									X				
Enrico PALLOTTA	DOCENTE									X				
Marco DE GIORGI	DOCENTE									X				
Alessandro IAVONE	DOCENTE									X				
Antonella BARBIERI (R.L.S)	DOCENTE											X		
Giancarlo BALDINI (A.S.P.P.)	DOCENTE											X		
Salvatore RAMUNDO (A.S.P.P.)	DOCENTE											X		
Ciro CONTE (A.S.P.P.)	DOCENTE											X		
Pasquale CONZA	DOCENTE												X	
Antonietta DE PALO	DOCENTE												X	
Antonella BONINI	DOCENTE													X
Maria Spasimina CERTO	DOCENTE													X
Giuseppe DE FILIPPIS	DOCENTE													X
Gaetano ZENI	DOCENTE (Resp. U.T.)				X									
Susanna DEL GAMBA	DOCENTE (Ref. Handicap)	X												
Luigi CASATUTO	COLL. SCOL. (Fotocopie)	X	X	X	X									
Pasqualina BERCELLINI	COLL. SCOL. (Fotocopie)	X	X	X	X									

X	TITOLARE

S	SUPPLENTE

I PROFILI DI AUTORIZZAZIONE DEGLI INCARICATI DEL TRATTAMENTO

Profili di autorizzazione (Policies)	Principali autorizzazioni assegnate al profilo	Aree di riferimento SW di segreteria	Schede di riferimento (Pagg. 21 ss.)
AREA DIDATTICA	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti cartacei ed ai documenti in formato elettronico (Word, Excel etc.) riferibili agli alunni, al loro andamento scolastico, ai loro dati anagrafici, ai loro trasferimenti da o per altri Istituti di istruzione, agli adempimenti inerenti alle uscite didattiche e altre attività a queste assimilate. Crea ed aggiorna il fascicolo personale dell'alunno. Si preoccupa che tutti gli alunni iscritti all'Istituto e tutti quelli non più frequentanti di cui però vengono trattati ancora i dati siano stati raggiunti da idonea informativa circa le modalità del trattamento. Si preoccupa inoltre di ottenere espressamente il consenso per i trattamenti di dati degli alunni non connaturati al ruolo di un Istituto di Istruzione o non strettamente necessari. Crea, concordemente con il Responsabile del trattamento, dei sistemi per la gestione degli interessati che non abbiano prestato il consenso.	ALUNNI BIBLIOTECA LIBRI DI TESTO	3 4 5 7
AREA PERSONALE	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti cartacei ed ai documenti in formato elettronico (Word, Excel etc.) riferibili al personale docente e non docente impiegato presso l'Istituto, ai loro dati anagrafici, ai loro trasferimenti da o per altri Istituti di istruzione, agli adempimenti inerenti alle pratiche di ricostruzione carriera, alle pratiche contrattuali e altre attività a queste assimilate. Crea ed aggiorna il fascicolo personale del dipendente. Si preoccupa che tutti i dipendenti dell'Istituto e tutti quelli non più in servizio di cui però vengono trattati ancora i dati siano stati raggiunti da idonea informativa circa le modalità del trattamento. Si preoccupa inoltre di ottenere espressamente il consenso per i trattamenti di dati dei dipendenti non connaturati al ruolo di un datore di lavoro o non strettamente necessari. Crea, concordemente con il Responsabile del trattamento, dei sistemi per la gestione degli interessati che non abbiano prestato il consenso.	PERSONALE RETRIBUZIONI	1 2 3 4
AREA AMMINISTRATIVA	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti cartacei ed ai documenti in formato elettronico (Word, Excel etc.) riferibili alla gestione amministrativa dell'Istituto e per questo motivo, normalmente, non riferibili a persone fisiche. Vigila sul fatto che soggetti non autorizzati non accedano a questi dati riservati.	NUOVO BILANCIO MINUTE SPESE	1
AREA AFFARI GENERALI	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti cartacei ed ai documenti in formato elettronico (Word, Excel etc.) riferibili alla gestione generale dell'Istituto e per questo motivo, normalmente, non riferibili a persone fisiche. Nel rapporto con i fornitori di cui vengono trattati i dati, l'incaricato si accerta che essi abbiano ricevuto idonea informativa circa le modalità del trattamento. Si preoccupa inoltre di ottenere espressamente il consenso per i trattamenti di dati dei fornitori non connaturati al ruolo di un cliente o non strettamente necessari. Crea, concordemente con il Responsabile del trattamento, dei sistemi per la gestione degli interessati che non abbiano prestato il consenso.	MAGAZZINO	NESSUNA
AREA PROTOCOLLO	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti cartacei in ingresso all'Istituto ad eccezione di quelli personalmente indirizzati al Titolare o al Responsabile del trattamento dei dati. E' tenuto a mantenere la riservatezza sui documenti aperti ed a garantire la consegna rapida e precisa al destinatario.	PROTOCOLLO (SE PRESENTE)	1 2 3 4 5 7

Profili di autorizzazione (Policies)	Principali autorizzazioni assegnate al profilo	Aree di riferimento SW DI SEGRETERIA	Schede di riferimento (Pagg. 21 ss.)
FAX	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è responsabile della riservatezza dei fax in arrivo. Li smista senza ritardo ai destinatari e verifica che nessun estraneo acceda ai documenti arrivati e non ancora smistati.	NESSUNA	NESSUNA
AREA POSTA ELETTRONICA	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area, ha accesso ai documenti elettronici in ingresso all'Istituto ad eccezione di quelli personalmente indirizzati al Titolare o al Responsabile del trattamento dei dati. E' tenuto a mantenere la riservatezza sui documenti aperti ed a garantire la consegna rapida e precisa al destinatario.	NESSUNA	NESSUNA
BACK-UP	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è personalmente responsabile delle condizioni necessarie per la buona riuscita della copia di back-up. Quando il sistema di back-up installato è automatico, egli si preoccupa di cambiare regolarmente il supporto e di riporre quello scritto in luogo sicuro ed in particolare nel luogo e con le precauzioni indicate dal responsabile del trattamento. Quando il sistema di back-up è manuale, egli si preoccupa della sua esecuzione. Quando il back-up non va a buon fine ne da immediatamente notizia al Responsabile del trattamento per gli adempimenti tecnici del caso.	NESSUNA	NESSUNA
I° E II° COLLABORATORE DEL DIRIGENTE SCOLASTICO	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è un docente al quale il Titolare del trattamento e la legge hanno attribuito funzioni vicarie. In mancanza delle condizioni che rendono effettiva la sostituzione del Dirigente Scolastico, l'Incaricato, sotto il profilo dell'accesso ai dati, gode degli stessi poteri concessi agli incaricati dell'AREA DIDATTICA.	NESSUNA	3 4 5 7
COORDINATORE DI PLESSO	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è un docente al quale il Titolare del trattamento ha attribuito funzioni di coordinamento. Sotto il profilo dell'accesso ai dati, gode degli stessi poteri concessi agli incaricati dell'AREA DIDATTICA, ma limitatamente al plesso scolastico in cui svolge la propria funzione.	NESSUNA	3 4 5 7
SICUREZZA (RSPP – ASPP – RLS)	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è un soggetto, interno od esterno all'istituzione scolastica, che, solo ai fini strettamente necessari per dare esecuzione al proprio ruolo di Responsabile del Servizio di Prevenzione e Protezione, Addetto a tale servizio o Rappresentante dei Lavoratori per la Sicurezza (D.Lgs 81/2008), ha diritto a trattare dati sanitari al fine di adeguare le procedure di sicurezza (evacuazione, segnali sonori e visivi di pericolo etc.) alle eventuali inabilità di lavoratori o studenti.	NESSUNA	NESSUNA
MEMBRO COMMISSIONE FORMAZIONE CLASSI	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è un docente al quale il Titolare del trattamento ha attribuito funzioni inerenti al procedimento di formazione delle classi. Sotto il profilo dell'accesso ai dati, gode degli stessi poteri concessi agli incaricati dell'AREA DIDATTICA.	NESSUNA	3 4 5 7
MEMBRO COMITATO DI VALUTAZIONE	L'Incaricato a cui vengono attribuite le autorizzazioni tipiche di quest'area è un docente al quale il Titolare del trattamento ha attribuito funzioni inerenti al procedimento di valutazione dei docenti all'atto del loro probabile inserimento in ruolo. Sotto il profilo dell'accesso ai dati, gode degli stessi poteri concessi agli incaricati dell'AREA PERSONALE.	NESSUNA	1 2 3 4

Il Ministero della Pubblica Istruzione, mediante il Regolamento dei dati sensibili e giudiziari (D.M. 305 del 07/12/2006), ha identificato in maniera precisa quali trattamenti dei dati sono consentiti all'interno di una istituzione scolastica.
Per fare questo ha utilizzato il sistema delle **SCHEDE,** indicando, in ciascuna di esse, le tipologie di dati sensibili e giudiziari e di operazioni su di essi indispensabili per la gestione del sistema della Pubblica Istruzione in un particolare comparto della stessa.

Preventivamente ha però individuato, all'Art. 2, dei limiti oggettivi entro i quali rimanere anche in caso di operazioni legittime su dati sensibili o giudiziari, infatti tutti i dati sensibili e giudiziari individuati dal regolamento in oggetto possono essere trattati previo verifica della loro :

PERTINENZA

Cioè i dati personali raccolti devono essere riferibili perfettamente all'interessato ed alla finalità del trattamento, sia nella loro forma individuale che nella forma più complessa dei documenti che li contengono.

COMPLETEZZA

Cioè i dati personali devono essere raccolti nella loro interezza onde evitare errori di valutazione che possano derivare dalla loro non completezza.

INDISPENSABILITA'

Cioè assolutamente indispensabili per raggiungere lo scopo prefissato.

Soprattutto in considerazione del fatto che tali dati non vengono quasi mai raccolti presso l'interessato, come di norma imporrebbe l'Art. 22 comma 4 del Codice della Privacy.

I PROFILI DI AUTORIZZAZIONE DEGLI INCARICATI DEL TRATTAMENTO - SCHEDE DEI TRATTAMENTI LECITI

SCHEDA N° 1 SELEZIONE, RECLUTAMENTO, INSTAURAZIONE, GESTIONE E CESSAZIONE DEL RAPPORTO DI LAVORO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
STATO DI SALUTE	Stato giuridico, idoneità al servizio, assunzione categoria protette, protezione maternità, igiene e sicurezza dei luoghi di lavoro, onoreficenze, assicurazioni, trattamenti assistenziali e previdenziali, denunce infortuni, malattie professionali, fruizione permessi, assenze giustificate.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 62 - Rilascio documenti di riconoscimento Art. 67 - Attività di controllo ed ispettive Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 70 - Obiezione di coscienza Art. 72 - Rapporti con Enti di culto Art. 73 - Supporto al collocamento e avviamento al lavoro
ADESIONE A SINDACATI	Versamento quote di iscrizione, esercizio diritti sindacali.	
CONVINZIONI RELIGIOSE	Concessione permessi e festività religiose, reclutamento docenti di religione.	
CONVINZIONI FILOSOFICHE	Svolgimento sevizio di leva come obiettore di coscienza.	
DATI GIUDIZIARI	Valutazione requisiti di ammissione, adozione di provvedimenti amministrativo-contabili.	
VITA SESSUALE	Rettificazione attribuzione di sesso	

COMUNICAZIONI DI DATI CONSENTITE
SERVIZI SANITARI COMPETENTI PER VISITE FISCALI ED ACCERTAMENTO IDONEITA' ALL'IMPIEGO; ORGANI PREPOSTI ALLA VIGILANZA IN MATERIA DI IGIENE E SICUREZZA LUOGHI DI LAVORO (D.Lgs. 626/1994); ENTI ASSISTENZIALI,PREVIDENZIALI ED ASSICURATIVI; AMMINISTRAZIONI PROVINCIALI PER GLI ASSUNTI EX L. 68/1999; ORGANIZZAZIONI SINDACALI PER GESTIONE PERMESSI E VERSAMENTO QUOTA DI ISCRIZIONE; PUBBLICHE AMMINISTRAZIONI VERSO LE QUALI SONO ASSEGNATI I DIPENDENTI IN MOBILITA'; ORDINARIO DIOCESANO PER IDONEITA' ALL'INSEGNAMENTO DELLA RELIGIONE CATTOLICA; ORGANI DI CONTROLLO (CORTE DEI CONTI e MEF); AGENZIA DELLE ENTRATE ; PRESIDENZA DEL CONSIGLIO DEI MINISTRI PER LA RILEVAZIONE ANNUALE DEI PERMESSI PER CARICHE SINDACALI ETC.

SCHEDA N° 2 GESTIONE DEL CONTENZIOSO E PROCEDIMENTI DISCIPLINARI

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla difesa in giudizio del Ministero della Pubblica Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro, amministrativo, penale e civile.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

COMUNICAZIONI DI DATI CONSENTITE
MINISTERO DEL LAVORO PER SVOLGIMENTO TENTATIVI OBBLIGATORI DI CONCILIAZIONE; ORGANI ARBITRALI PER SVOLGIMENTO PROCEDURE ARBITRALI INDICATE NEI CCNL; AVVOCATURA DELLO STATO PER DIFESA E CONSULENZA; MAGISTRATURA E ORGANI DI POLIZIA GIUDIZIARIA; LIBERI PROFESSIONISTI A FINI DI PATROCINIO E CONSULENZA, INCLUSI QUELLI DI CONTROPARTE.

SCHEDA N° 3 ORGANISMI COLLEGIALI E COMMISSIONI ISTITUZIONALI

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Attivazione degli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero dell'Istruzione e dell'ordinamento scolastico.	Art. 65 - pubblicità dell'attività di organi. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.

COMUNICAZIONI DI DATI CONSENTITE
NESSUNA, ATTIVITA' INTERNA ALL'ISTITUZIONE SCOLASTICA.

SCHEDA N° 4 ATTIVITA' PROPEDEUTICHE ALL'AVVIO DELL'ANNO SCOLASTICO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli alunni di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.	
STATO DI SALUTE	Per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti, o qualora l'Autorità Giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno o alunni che abbiano commesso reati.	

COMUNICAZIONI DI DATI CONSENTITE

ENTI LOCALI PER LA FORNITURA DI SERVIZI;
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALUNNI E DI SUPPORTO;
AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP.

SCHEDA N° 5 ATTIVITA' EDUCATIVA, DIDATTICA E FORMATIVA, DI VALUTAZIONE

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli alunni di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso.	
STATO DI SALUTE	Per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni diversamente abili, dell'insegnamento domiciliare ed ospedaliero, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate ed ai viaggi di istruzione.	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti.	
CONVINZIONI POLITICHE	Per la costituzione ed il funzionamento delle Consulte e delle Associazioni di studenti e dei genitori.	
DATI SENSIBILI IN GENERALE	In generale per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.	

COMUNICAZIONI DI DATI CONSENTITE

ALTRE ISTITUZIONI SCOLASTICHE STATALI E NON PER TRASMISSIONE DOCUMENTAZIONE ATTINENTE LA CARRIERA;
ENTI LOCALI PER FORNITURA SERVIZI;

COMUNICAZIONI DI DATI CONSENTITE (segue Scheda 5)
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALUNNI E DI SUPPORTO; ISTITUTI DI ASSICURAZIONE PER DENUNCIA INFORTUNI E CONNESSA R.C.; ALL'INAIL PER LA DENUNCIA INFORTUNI; AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP; AZIENDE, IMPRESE ED ALTRI SOGGETTI PUBBLICI O PRIVATI PER STAGES.

SCHEDA N° 6 SCUOLE NON STATALI

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
FASCICOLI PERSONALI DI DOCENTI E ALUNNI	Per rendere effettiva l'attività di vigilanza e controllo eseguita dall'Amministrazione centrale o periferica nei confronti delle scuole non statali parificate.	Art. 67 - Attività di controllo ed ispettive

SCHEDA N° 7 RAPPORTI SCUOLA-FAMIGLIA GESTIONE DEL CONTENZIOSO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla instaurazione del contenzioso (reclami, ricorsi, esposti, provvedimenti disciplinari, ispezioni, citazioni, denunce etc.) con gli alunni e le famiglie e tutte le attività di difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado.	Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

III° SEZIONE DEL DOCUMENTO

AMMINISTRAZIONE DEL SISTEMA INFORMATICO

IX. INTRODUZIONE ALLA AMMINISTRAZIONE DELLA RETE INFORMATICA

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 che non rientrino in uno dei casi per i quali è possibile attuare un regime semplificato (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). 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 da mantenere aggiornato e disponibile in caso di accertamenti anche da parte del Garante.
Con il presente provvedimento il Garante intende pertanto richiamare tutti i titolari di trattamenti effettuati, anche in parte, mediante strumenti elettronici alla necessità di prestare massima attenzione ai rischi e alle criticità implicite nell'affidamento degli incarichi di amministratore di sistema.
L'Autorità ravvisa inoltre l'esigenza di individuare in questa sede alcune prime misure di carattere organizzativo che favoriscano una più agevole conoscenza, nell'ambito di organizzazioni ed enti pubblici e privati, dell'esistenza di determinati ruoli tecnici, delle responsabilità connesse a tali mansioni e, in taluni casi, dell'identità dei soggetti che operano quali amministratori di sistema in relazione ai diversi servizi e banche di dati.

X. COSA SI INTENDE PER “AMMINISTRATORE DI SISTEMA”

La figura dell’Amministratore di sistema non è mai stata esplicitamente prevista dal "Codice in materia di protezione dei dati personali" (D.Lgs 196/2003) ma viceversa dal vecchio D.P.R. 318/1999 (abrogato dal Codice) che lo definiva come 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 precisa che con il termine "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.

Il titolare del trattamento, prima di procedere alla nomina, ha valutato l'esperienza, la capacità e l'affidabilità dei soggetti designati quali "amministratore di sistema" e ha ritenuto che fornissero idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.
Nella valutazione dei profili professionali il titolare ha ritenuto di grande rilevanza 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 poiché in questo ambito è chiaro come ciò assuma un valore particolarmente importante per il "rispetto della garanzia delle vigenti disposizioni".
Nella designazione dell’amministratore di sistema si è tenuto conto che questi conoscesse la normativa sulla privacy.

XI. NOMINA DELL'AMMINISTRATORE DI SISTEMA

Il testo che segue ha valore di lettera di designazione ad "AMMINISTRATORE DI SISTEMA".

Ai sensi del provvedimento del Garante per la protezione dei dati personali del 27 novembre 2008 recepito nella Gazzetta Ufficiale. n. 300 del 24 dicembre 2008

- *VALUTATO che all'interno dell'Istituto di Istruzione non è individuabile una figura che possieda i requisiti professionali e di esperienza adeguati per svolgere la funzione di Amministratore di sistema;*
- *VISTO il contratto di prestazione professionale appositamente perfezionato con la società Studio AG.I.COM. S.r.l. con sede a Melegnano, Via Guglielmo Marconi, 4;*
- *TENUTO CONTO che tale contratto prevede l'individuazione personale di Luca Corbellini, quale soggetto incaricato dalla società stessa di assumere le obbligazioni da questo derivanti;*
- *VALUTATO il profilo professionale di Luca Corbellini come adeguato rispetto all'incarico quale amministratore di sistema rispetto alle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza;*

Il Dirigente Scolastico dell'Istituto di Istruzione, in qualità di titolare del trattamento del medesimo, con la presente nomina **LUCA CORBELLINI** *Amministratore di sistema per i trattamenti svolti internamente.*

Specificatamente e limitatamente a tale contesto i compiti dell'Amministratore consistono in:

- *assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso all'interno dell'Istituto;*
- *predisporre e rendere funzionanti le copie di sicurezza (operazioni di backup e recovery) dei dati e delle applicazioni;*
- *predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte dell'amministratore di sistema; tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.*

In considerazione del fatto che il provvedimento del Garante, obbliga l'istituto alla "verifica" almeno annuale delle attività svolte dall'amministratore di sistema in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti, il Dirigente Scolastico si riserva la possibilità di convocare l'Amministratore per ottenere una relazione del lavoro svolto.

Sulla base di quanto previsto al punto 2.c del citato Provvedimento del Garante, gli estremi identificativi dell'Amministratore di Sistema saranno comunicati secondo quanto stabilito al comma 4.3

Il Dirigente Scolastico prende atto del fatto che, in considerazione della tipologia del contratto concluso, l'Amministratore di Sistema effettuerà controlli circa la rispondenza del sistema informatico ove avviene il trattamento dei dati alla normativa vigente solo con frequenza bimestrale, anche mediante accesso da remoto al server.
In considerazione del fatto che l'Amministratore non sarà quotidianamente presente presso l'Istituto il Dirigente si assume la responsabilità rispetto agli interventi tecnici commissionati ad altri soggetti senza dare avviso degli stessi all'Amministratore, nonché della comunicazione delle credenziali di accesso di rango amministrativo a terzi senza darne avviso all'Amministratore.

AMMINISTRATORE di SISTEMA

DIPENDENTE o ESTERNO	NOME o RAGIONE SOCIALE	ANNOTAZIONI
ESTERNO	**LUCA CORBELLINI** c/o Studio AG.I.COM. S.r.l. Via Marconi, 4 - 20077 MELEGNANO (MI)	Incaricato di sovraintendere alla gestione ed amministrazione del sistema informatico ove avviene il trattamento dei dati sensibili.

AMMINISTRATORI di RETE

DIPENDENTE o ESTERNO	NOME o RAGIONE SOCIALE	ANNOTAZIONI
ESTERNO	**MARCO GALLERINI** c/o AG.I.COM. Italia S.r.l. Via Marconi, 4 - 20077 MELEGNANO (MI)	Incaricato della gestione a livello amministrativo del Server Windows nonché degli apparati attivi di rete (firewall etc.) al fine di attuare le misure minime di sicurezza indicate all'Allegato B del D.Lgs 196/2003
ESTERNO	**MATTEO OLIVO** c/o AG.I.COM. Italia S.r.l. Via Marconi, 4 - 20077 MELEGNANO (MI)	Incaricato della gestione a livello amministrativo del Server Windows nonché degli apparati attivi di rete (firewall etc.) al fine di attuare le misure minime di sicurezza indicate all'Allegato B del D.Lgs 196/2003
ESTERNO	**LUIGI LACERENZA** c/o AG.I.COM. Italia S.r.l. Via Marconi, 4 - 20077 MELEGNANO (MI)	Incaricato della gestione a livello amministrativo del Server Windows nonché degli apparati attivi di rete (firewall etc.) al fine di attuare le misure minime di sicurezza indicate all'Allegato B del D.Lgs 196/2003

Talvolta si ricorre a personale interno per l'esecuzione di alcune procedure (p.es. aggiornamento software di segreteria) per le quali è necessario disporre di diritti di accesso alla rete di tipo amministrativo o addirittura della password dell'utente "Administrator" :

INCARICATI TECNICI INTERNI

NOME DIPENDENTE	TIPOLOGIA DI ACCESSO	MOTIVAZIONE
Maria SURACE (D.S.G.A.)	Administrator	Aggiornamento software di segreteria
Scilla FALCIANI (Assistente Amministrativo)	Administrator	Aggiornamento software di segreteria

SE NON SI RICORRE A PERSONALE INTERNO LASCIARE LA TABELLA IN BIANCO

IV° SEZIONE
DEL DOCUMENTO

(ANALISI DEI RISCHI)

INDIVIDUAZIONE RISCHI
MISURE MINIME DI SICUREZZA

XII. LE MISURE DI SICUREZZA GLOBALI

La Legge definisce con il termine "misure minime di sicurezza", una serie di prescrizioni tecniche indispensabili affinché il trattamento dei dati personali, eseguito mediante l'impiego di apparecchiature elettroniche, sia minimamente sicuro.
Mentre la stragrande maggioranza di dette misure è positivamente indicata nel c.d. "Disciplinare Tecnico – Allegato B", molte altre indicazioni sono più generali e appartengono ad un metodo di lavoro organizzato secondo ragionevolezza e buona fede :

USO DI INTERNET DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Il corretto utilizzo di internet rappresenta uno dei punti cardini per la sicurezza dell'infrastruttura informatica entro la quale si effettua il trattamento dei dati.
Il momento "critico" è quello del "download" (scaricamento) di software o dati al di fuori dai casi espressamente previsti e consentiti dal Titolare del trattamento.
L'incaricato del trattamento dei dati mediante utilizzo di apparecchiature informatiche, deve astenersi dal compiere "download" non autorizzati onde prevenire situazioni critiche riconducibili a due fattispecie da evitare :

<u>"DOWNLOAD" INVOLONTARIO DI SOFTWARE CHE POSSA ESPORRE LA RETE A RISCHIO DI INTRUSIONI O DI DANNO CAGIONATO DA SOFTWARE RICONDUCIBILE A QUANTO PREVISTO DALL'ART. 615 QUINQUIES DEL CODICE PENALE (VIRUS INFORMATICI)</u>

Il "download" incontrollato molto frequentemente mina le misure di sicurezza adottate a protezione della rete. Le conseguenze tipiche di tale comportamento sono : L'apertura di un varco sul dispositivo firewall che agevoli l'accesso indebito alla rete da parte di soggetti non autorizzati; Il danneggiamento dei dispositivi operato da virus informatici.

<u>"DOWNLOAD" DI DATI CHE POSSANO ESSERE CATALOGATI EX ART. 4 PUNTO B DEL CODICE DELLA PRIVACY COME "PERSONALI" O FINANCO "SENSIBILI" EX ART. 4 PUNTO D IN MANIERA INCONSAPEVOLE DA PARTE DEL TITOLARE DEL TRATTAMENTO</u>

Il "download" incontrollato può riguardare non solo "maleware" (cioè software che abbia mire dannose per la rete) bensì anche dati personali o addirittura sensibili che si troveranno a risiedere su elaboratori elettronici in maniera non consapevole e quindi verranno trattati, con ogni probabilità, in maniera inadeguata.

USO DELLA POSTA ELETTRONICA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Al "download" di software o dati da internet è assimilabile la consultazione non remota della posta elettronica. La rete pertanto sarà configurata in modo da impedire ai soggetti del trattamento la configurazione di software di posta (Outlook, Eudora etc.) che comportino lo scaricamento dei dati sui propri elaboratori. Se la consultazione della posta elettronica privata è consentita, essa avverrà mediante accesso remoto alla casella mail tramite browser (Internet Explorer, Netscape Navigator etc.).

USO DEL FAX DA PARTE DEI SOGGETTI DEL TRATTAMENTO

I documenti in ingresso, contenenti dati personali, che pervengano via FAX, devono essere trattati con particolare cura, affinché non restino a disposizione di soggetti non autorizzati. L'incaricato della gestione dei FAX deve vigilare sulla corretta esecuzione della procedura di smistamento.

DISTRUZIONE DI DOCUMENTI DA PARTE DEI SOGGETTI DEL TRATTAMENTO

I documenti cartacei contenenti dati personali che, a qualsiasi titolo (dismissione di archivi, errori di scrittura, copie ridondanti etc.) debbano essere eliminati, saranno resi illeggibili dal soggetto incaricato mediante l'uso di un distruggidocumenti o di altro metodo parimenti idoneo.

GESTIONE DELLA POSTA CARTACEA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

La posta cartacea viene raccolta dall'incaricato in servizio in quel momento presso la portineria / reception ed immediatamente smistata verso gli uffici.
All'atto dell'apertura tutti i documenti contenenti dati personali devono essere smistati senza ritardi a cura del personale del protocollo stesso.

Il Responsabile del trattamento determina gli incaricati espressamente autorizzati, quali responsabili della tenuta del protocollo e della visione dei contenuti delle missive.

La posta elettronica viene "scaricata" da ciascun incaricato e, se stampata, segue lo stesso procedimento previsto per la posta cartacea.

Le lettere arrivate per posta che presentino all'esterno l'indicazione "RISERVATO" o altre formule atte a qualificarle come contenenti documenti di tipo particolare, non possono essere aperte dagli incaricati della gestione del protocollo ma devono immediatamente essere consegnati all'attenzione del Responsabile del trattamento il quale provvederà alla loro custodia ed all'inoltro, o a quella del destinatario in persona.

Si rammenta a ciascuno che :

Art. 616 Codice Penale
Violazione, sottrazione e soppressione di corrispondenza

Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da € 31,00 a € 516,00

[omissis]

XIII. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita, il Responsabile del trattamento dei dati stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati. Tale periodicità tuttavia non può essere superiore alla settimana.
I criteri debbono essere stabiliti dal Responsabile del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Procedura di esecuzione del Back-up

Il Responsabile del trattamento dei dati nomina il "Responsabile della procedura di Back-Up" con espressa lettera di incarico.
Il Responsabile della procedura di Back-Up deve essere formato affinché sia totalmente indipendente nell'eseguire i passi tecnici necessari per l'attuazione del salvataggio delle copie degli archivi informatici contenenti dati personali.
La procedura di Back-Up deve avvenire in maniera completamente automatizzata senza bisogno dell'intervento da parte dell'operatore al fine di escludere tutte le ipotesi di dimenticanza e imperizia dell'attuazione del procedimento.
Le mansioni cui è soggetto il Responsabile della procedura di Back-Up sono indicate in via generale nella lettera di incarico.

Il Responsabile del trattamento è responsabile della custodia e della conservazione di supporti utilizzati per il *back up* dei dati.
Essi devono essere custoditi in modo da scongiurare il più possibile le aggressioni da :

- Agenti chimici;
- Fonti di calore;
- Campi magnetici;
- Intrusione ed atti vandalici;
- Incendio;
- Allagamento;
- Furto.

L'accesso ai supporti utilizzati per il *back up* dei dati è limitato per ogni banca dati al Responsabile del trattamento della sicurezza dei dati ed all'Incaricato del trattamento di competenza.

Se il Responsabile del trattamento decide che i supporti per le copie di *back up* delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto, annullando e rendendo illeggibili le informazioni in esso contenute.
È compito del Responsabile del trattamento assicurarsi che in nessun caso vengano lasciate copie di *back up* delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.

I dati memorizzati sui supporti di back-up, nonché sui dispositivi mobili di archiviazione, devono risiedere sugli stessi in forma non-intelleggibile; perché questo avvenga è necessario prevedere l'installazione di software di criptaggio dei dati che impediscano, in caso di furto o smarrimento accidentale di questi supporti, la lettura da parte di chicchessia non autorizzato.

Con periodicità almeno semestrale viene verificato il corretto funzionamento della procedura di back-up simulando un ripristino totale dei dati.

XIV. CRITERI PER LA TENUTA DI SUPPORTI DIGITALI REMOVIBILI

I supporti di back-up (nastri, CD, DVD, FDD etc.), nonché tutti i supporti digitali removibili (PEN DRIVE, SD etc.) contenenti dati personali, devono essere limitati al minimo nel loro numero, devono essere tenuti esclusivamente da soggetti espressamente autorizzati e, se i dati sono di natura sensibile, devono risiedere sui supporti di archiviazione in formato non intelleggibile in quanto, in considerazione della loro forma, del loro peso e della loro facile portabilità, il rischio di smarrimento e di furto è da considerarsi elevatissimo.

Di seguito sono indicati i criteri di esecuzione del back-up, di ripristino dei dati salvati e di cifratura dei dati memorizzati :

CRITERI E PROCEDURE PER IL SALVATAGGIO ED IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI

Salvataggio

Banca dati	Tipo dati	Criteri e procedure di salvataggio	Periodicità	Luogo di custodia delle copie	Metodo di cifratura
MS OFFICE	P & S	PROCEDURA AUTOMATIZZATA	Almeno SETTIMANALE	I SUPPORTI DI BACKUP VENGONO CUSTODITI DALL'INCARICATO IN MANIERA SICURA DAI RISCHI CONNESSI ALLA DIFFUSIONE ED ALLA DISTRUZIONE DEGLI STESSI	NON PREVISTO
GESTIONALE DI SEGRETERIA	P & S		Almeno SETTIMANALE		NON PREVISTO
ALTRI SOFTWARE	P & S		Almeno SETTIMANALE		NON PREVISTO

Ripristino

Banca dati	Criteri e procedure	Pianificazione delle prove di ripristino
MS OFFICE	Ripristino dell'archivio su un'area del disco fisso non allocata	SEMESTRALE
GESTIONALE DI SEGRETERIA	Ripristino dell'archivio su un'area del disco fisso non allocata	SEMESTRALE
ALTRI SOFTWARE	Ripristino dell'archivio su un'area del disco fisso non allocata	SEMESTRALE

CIFRATURA DEI DATI O SEPARAZIONE DEI DATI IDENTIFICATIVI

Trattamento dei dati interessato (6)	Metodo CIFRATURA/SEPARAZIONE	Descrizione della tecnica adottata	Altre informazioni utili
NESSUNO			

XV. VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce quali protezioni *software* adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Responsabile del trattamento dei dati stabilisce inoltre la periodicità, non superiore a sei mesi, con cui debbono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattate.

I criteri debbono essere definiti dal Responsabile del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato;
- La periodicità degli aggiornamenti.

Nel caso in cui su uno o più sistemi si dovesse verificare la perdita di informazioni o danni a causa di infezione o contagio da virus informatici il Responsabile del trattamento deve provvedere ad attivare tutti i sistemi di risanamento idonei al recupero dell'elaboratore infetto, all'impedimento della propagazione del virus ed alla protezione della rete da attacchi futuri analoghi.

XVI. ALTRE MISURE DI SICUREZZA

Il DPR 318/1999 vieta a chiunque di :

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

Il Responsabile del trattamento dei dati deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
In linea di massima sono autorizzate all'accesso ai locali esclusivamente quelle persone incaricate del trattamento alle quali, il responsabile, concede l'accesso ai luoghi fisici mediante la consegna di un badge o di una chiave, nonché l'accesso agli ambiti informatici mediante la consegna di idonei criteri di accesso.

Il Responsabile del trattamento dei dati deve informare con una comunicazione scritta l'Incaricato dell'ufficio dei compiti che gli sono stati affidati (lettera di incarico) e deve provvedere a formarlo affinché le mansioni indicate nella lettera gli siano familiari.

ASSEGNAZIONE NOMI UTENTE
Il Responsabile del trattamento dei dati deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato del trattamento di accedere ai sistemi di trattamento delle banche di dati.
Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei pochi identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un Incaricato del trattamento deve essere annullato se l'Incaricato del trattamento ha dato le dimissioni.

ASSEGNAZIONE DELLE *PASSWORD*

Il Responsabile del trattamento dei dati deve definire le modalità di assegnazione delle *password* e decidere che ogni utente Incaricato del trattamento possa modificare autonomamente la propria *password* di accesso.
In questo caso la modifica richiede che venga data comunicazione al Custode della *password* e al Responsabile del trattamento (se diverso dal Custode delle *password*).
Le password saranno composte da almeno 8 caratteri e non dovranno contenere elementi immediatamente riconducibili ai proprietari delle stesse.

SICUREZZA DELLE TRASMISSIONI DATI

Al fine di garantire la sicurezza delle trasmissioni dei dati su rete pubblica, il Responsabile del trattamento dei dati stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dal Responsabile del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Il Documento programmatico sulla sicurezza è costantemente aggiornato ad opera del Responsabile del trattamento dei dati circa ogni variazione dell'elenco degli Incaricati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni Incaricato del trattamento deve essere indicato lo USER ID assegnato.
In caso di dimissioni di un Incaricato del trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Responsabile del trattamento dei dati deve darne immediata comunicazione al Custode delle *password* (se diverso dal Responsabile) che provvederà a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Al Responsabile del Trattamento è affidato il compito di verificare ogni anno, entro il 31 ottobre, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

Al Responsabile del Trattamento è affidato il compito di redigere e di aggiornare ad ogni variazione la Tabella dei permessi di accesso che indica per ogni banca di dati i tipi di permesso di accesso per ogni Incaricato del trattamento autorizzato.
In particolare, per ogni Incaricato del trattamento e per ogni banca dati debbono essere indicati i privilegi assegnati tra seguenti:

I. Inserimento dei dati;
II. Lettura e stampa dei dati;
III. Modifica di dati;
IV. Cancellazione di dati.

XVII. MANUTENZIONE DELLE APPARECCHIATURE

Al Responsabile del trattamento è affidato il compito di verificare ogni anno la situazione delle apparecchiature installate con cui vengono trattati i dati, delle apparecchiature periferiche e, in particolare, dei dispositivi di collegamento con le reti pubbliche.
La verifica ha lo scopo di controllare l'affidabilità del sistema 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 anche dell'evoluzione tecnologica.

Al Responsabile del trattamento è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi 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 Sistemi operativi utilizzati;
- Segnalazioni di *Patch*, *Fix* o *System-Pack* per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurarne il corretto trattamento dei dati in conformità alle norme in vigore.
Al Responsabile del trattamento è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del *software* applicativo, 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 della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
Nel caso in cui esistano rischi evidenti il Responsabile del trattamento dei dati deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

XVIII. IL PIANO DEI RISCHI

Momento fondamentale e qualificante del presente documento è quello della valutazione specifica dei rischi, tipici dell'infrastruttura oggetto di analisi, incombenti sui dati.
Per una trattazione più analitica della materia, suddividiamo l'analisi dei rischi in funzione delle 3 tipologie classiche di rischiosità incombente sui dati :

Paragrafo XV	Pagina 34	Rischi riconducibili al cattivo comportamento degli operatori
Paragrafo XVI	Pagina 35	Rischi riconducibili al malfunzionamento delle apparecchiature
Paragrafo XVII	Pagina 36	Rischi riconducibili ad eventi fisici ed atmosferici
Paragrafo XVIII	Pagina 37	Rischi specifici cui sono sottoposte le risorse connesse in rete internet

XIX. EVENTI DANNOSI IN SEGUITO A CATTIVO COMPORTAMENTO DEGLI OPERATORI O DI SOGGETTI TERZI

ANALISI DEI RISCHI

Descrizione del rischio	Probabilità dell'evento	Trattamento interessato (6)	Misura di sicurezza adottata	Tipologia della misura	Responsabile dell'attuazione della misura
Danneggiamento volontario	BASSA	TUTTI	Vigilanza sugli operatori	PREVENTIVA / DI CONTENIMENTO DEGLI EFFETTI DANNOSI	RESPONSABILE DEL TRATTAMENTO
Furto	BASSA	TUTTI	Vigilanza sugli operatori Installazione di un sistema antifurto o di sistemi anti-intrusione nei locali ove sono tenuti i dati. Adozione di tecniche di cifratura dei dati (Vedi tabella precedente)	PREVENTIVA / DI CONTRASTO	RESPONSABILE DEL TRATTAMENTO
Uso non autorizzato di supporti di memoria	ALTA	TRATTAMENTI INFORMATICI	Vigilanza sugli operatori e configurazione di utenze non amministrative. Adozione di tecniche di cifratura dei dati (Vedi tabella precedente)	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Errore del personale operativo	MEDIA	TUTTI	Vigilanza sugli operatori ed organizzazione corsi di formazione	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO
Errore di manutenzione	MEDIA	TRATTAMENTI INFORMATICI	Impiego di personale specializzato	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Uso illegale di software	ALTA	TRATTAMENTI INFORMATICI	Vigilanza sugli operatori e configurazione di utenze non amministrative	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Accesso non autorizzato alla rete	MEDIA	TRATTAMENTI INFORMATICI	Configurazione di utenze protette da password	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Indirizzamento non corretto della posta elettronica	MEDIA	TRATTAMENTI INFORMATICI	Vigilanza sul personale e formazione dello stesso	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO
Sottrazione di credenziali di autenticazione	MEDIA	TRATTAMENTI INFORMATICI	Configurazione di un sistema di cambio periodico della password e di disattivazione in caso di prolungato non impiego dell'utenza	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Visione da parte di soggetti non autorizzati di dati cartacei dopo la loro eliminazione	ALTA	TRATTAMENTI CARTACEI	Impiego di un distruggidocumenti o di altro metodo per rendere illeggibili tutti i fogli contenenti dati personali	DI CONTRASTO	RESPONSABILE DEL TRATTAMENTO
Lettura da parte di soggetti non autorizzati di dati digitali su supporti magnetici dopo la loro dismissione	MEDIA	TRATTAMENTI INFORMATICI	Impiego di un distruggi-CD o di altro metodo di annullamento dei supporti	DI CONTRASTO	RESPONSABILE DEL TRATTAMENTO

(6) TRATTAMENTO INTERESSATO ..... Si faccia riferimento alle TABELLE B e C

XX. EVENTI DANNOSI IN SEGUITO A MALFUNZIONAMENTO DELLE APPARECCHIATURE

ANALISI DEI RISCHI

Descrizione rischio	Probabilità dell'evento	Trattamento interessato (6)	Misura di sicurezza adottata	Tipologia della misura	Responsabile dell'attuazione della misura
Guasto hardware	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Linea elettrica instabile	MEDIA	TRATTAMENTI INFORMATICI	Installazione di unità di continuità elettrica stabilizzate	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Guasto tecnico al provider di rete	MEDIA	TRATTAMENTI INFORMATICI	Conclusione di contratti di somministrazione del servizio con provider certificati	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO
Danni sulle linee di rete	BASSA	TRATTAMENTI INFORMATICI	Certificazione realizzazione impianto secondo le regole dell'arte	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Guasto software	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione delle apparecchiature	PREVENTIVA / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Azione di virus informatici o di altro maleware	ALTA	TRATTAMENTI INFORMATICI	Installazione di un software antivirus di rete adeguato	PREVENTIVA / DI CONTRASTO /DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Spamming e tecniche di sabotaggio informatico	ALTA	TRATTAMENTI INFORMATICI	Installazione di un sistema di firewalling dimensionato sulla struttura	PREVENTIVA / DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Degrado delle apparecchiature	MEDIA	TRATTAMENTI INFORMATICI	Continua manutenzione e redazione di un piano di sostituzioni	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Intercettazioni di informazioni di rete	MEDIA	TRATTAMENTI INFORMATICI	Installazione di un sistema di firewalling dimensionato sulla struttura e adozione di policy di rete corrette	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE

(6) TRATTAMENTO INTERESSATO ..... Si faccia riferimento alle TABELLE B e C

XXI. EVENTI DANNOSI IN SEGUITO AD EVENTI FISICI ED ATMOSFERICI

ANALISI DEI RISCHI

Descrizione rischio	Probabilità dell'evento	Trattamento interessato (6)	Misura di sicurezza adottata	Tipologia della misura	Responsabile dell'attuazione della misura
Inondazione	BASSA	TUTTI I TRATTAMENTI	I SERVER ed in generale i dispositivi contenenti dati sono posti su supporti rialzati	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO
Fulmine	BASSA	TRATTAMENTI INFORMATICI	Installazione di unità di continuità elettrica stabilizzate	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Fuoco	BASSA	TUTTI I TRATTAMENTI	I SERVER ed in generale i dispositivi contenenti dati sono installati in locali dotati di estintore o di sistema anti-incendio	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO
Temperatura ed umidità eccessive	MEDIA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Polvere	ALTA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
Radiazioni elettromagnetiche	MEDIA	TRATTAMENTI INFORMATICI	I SERVER ed in generale i dispositivi contenenti dati sono posti all'interno di locali chiusi	DI CONTRASTO / DI CONTENIMENTO DELL'EVENTO DANNOSO	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE

(6) TRATTAMENTO INTERESSATO ..... Si faccia riferimento alle TABELLE B e C

XXII. RISCHI SPECIFICI CUI SONO SOTTOPOSTE LE RISORSE CONNESSE AD INTERNET

ANALISI DEI RISCHI

Descrizione del rischio	Probabilità dell'evento	Trattamento interessato (6)	Misura di sicurezza adottata	Tipologia della misura	Responsabile dell'attuazione della misura
IP SPOOFING Ovvero rischio che l'autore dell'attacco sostituisca la propria identità a quella dell'utente legittimo del sistema. Viene fatto non per generare intrusioni in senso stretto ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici come l'indirizzo IP o il mittente di E-mail	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
PACKET SNIFFING Apprendimento di informazioni e dati presenti in un sistema tramite l'uso di appositi programmi. L'aggressore mediante questi programmi è in grado di "intercettare" password, messaggi etc.	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
PORT SCANNING Serie programmata di tentativi di accesso ad un sistema diretti ad evidenziare, in funzione delle risposte ottenute, le caratteristiche tecniche del medesimo e, conseguentemente, le eventuali vulnerabilità	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
HIGHJACKING Intrusione in una connessione di rete in corso, simulando di essere una macchina parte della "conversazione" di rete	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE
PASSWORD CRACKING Programmi in grado di acquisire le password nel momento in cui queste sono digitate a tastiera	MEDIA	TRATTAMENTI INFORMATICI	Azione di protezione ottenuta dall'azione combinata di FIREWALL e SOFTWARE ANTIVIRUS	PREVENTIVA	RESPONSABILE DEL TRATTAMENTO / INCARICATO DELLA MANUTENZIONE

(6) TRATTAMENTO INTERESSATO ..... Si faccia riferimento alle TABELLE B e C

V° SEZIONE
DEL DOCUMENTO

(VALUTAZIONI PROGRAMMATICHE)

MISURE PROGRAMMATICHE
FORMAZIONE OBBLIGATORIA
NOTIFICA AL GARANTE

XXIII. ALTRE MISURE MINIME DI SICUREZZA DA ADOTTARE

Vista la permanenza di taluni rischi incombenti sui dati anche dopo l'individuazione e l'applicazione di tutte le misure minime di sicurezza indicate alle pagine precedenti, si formalizza la manifestazione della volontà del titolare del trattamento di incrementare il livello di sicurezza dei dati raggiunto implementando, nel breve/medio periodo, le seguenti, ulteriori, misure minime :

ALTRE MISURE MINIME DI SICUREZZA DA ADOTTARE

Misura di sicurezza da adottare	Descrizione del rischio da scongiurare	Trattamento interessato (6)	Probabilità dell'evento	Tipologia della misura
NESSUNA				

(6) TRATTAMENTO INTERESSATO ..... Si faccia riferimento alle TABELLE B e C

XXIV. FORMAZIONE DEGLI INCARICATI

Al Responsabile del trattamento dei dati è affidato il compito di verificare entro il 31 ottobre di ogni anno le necessità di formazione del personale incaricato di eseguire i compiti indicati nella lettera di incarico. Per ogni incaricato del trattamento il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata e ne fa immediatamente richiesta al Titolare.

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessate
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO Oggetto : - Informazione sul contenuto e disposizioni del D.Lgs 196/2003 - Uso delle CREDENZIALI DI ACCESSO ALLA RETE - Concetti di "IGIENE INFORMATICA" - Rilevanza legale del BACK-UP - Il Documento Programmatico sulla Sicurezza (DPS) - Natura giuridica della "LETTERA DI INCARICO" - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione	TITOLARE DEL TRATTAMENTO RESPONSABILE DEL TRATTAMENTO INCARICATI DEL TRATTAMENTO COLLABORATORI DEL DIRIGENTE COORDINATORI DI PLESSO
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO Oggetto : - Informazione sul contenuto e disposizioni del D.Lgs 196/2003 - Cenni di diritto in materia di POTESTA' GENITORIALE - Il Documento Programmatico sulla Sicurezza (DPS) - Natura giuridica della "LETTERA DI INCARICO" - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione	DOCENTI ADDETTI ALLA SICUREZZA (D.Lgs 81/08) COMMISSIONE FORMAZIONE CLASSI MEMBRI COMITATO DI VALUTAZIONE COLLABORATORI SCOLASTICI

XXV. NOTIFICAZIONE AL GARANTE

L'Art. 37 D.Lgs 196/2003 impone al Titolare del trattamento la notifica all'Autorità Garante per il trattamento dei dati personali per il trattamento di dati delle seguenti tipologie :

a) dati genetici, biometrici o dati che indichino la posizione geografica delle persone .. omissis…
b) dati idonei a rivelare lo stato di salute e la vita sessuale … omissis…
c) dati idonei a rivelare la vita sessuale e la sfera psichica … omissis…
d) dati trattati elettronicamente volti a tracciare il profilo o la personalità dell'interessato … omissis…
e) dati sensibili registrati in banche dati a fini di selezione del personale per conto terzi … omissis…
f) dati registrati in apposite banche dati, gestite con strumenti elettronici, e relative al rischio di solvibilità economica … omissis…

con riferimento ai trattamenti elencati alle tabelle B, B2 e B3 è chiara la rispondenza di alcuni di essi alla categoria suindicata sub b) e la sussistenza del conseguente **obbligo di notifica**.

Tuttavia, visto il contenuto dell'Art. 40 del medesimo Decreto e conseguentemente, viste le seguenti autorizzazioni generali del Garante (valide a tutto il 30/06/2011) :

- **Autorizzazione N° 1/2009 al trattamento dei dati sensibili nei rapporti di lavoro**

Il Titolare del trattamento si avvale della facoltà prevista ex Art. 1 Autor. N°1/2009 e pertanto **non procede alla notifica al Garante**.

XXVI. MENZIONE A BILANCIO

In conformità a quanto indicato al Punto 26 del Disciplinare Tecnico (Allegato B D.Lgs 196/2003) il Titolare del trattamento riferisce nella relazione accompagnatoria del programma annuale, della avvenuta redazione o aggiornamento del presente Documento Programmatico sulla Sicurezza.

XXVII. REVISIONI

Il presente Documento Programmatico Sulla Sicurezza (DPSS), fatte salve le scadenze operative diverse indicate in esso, dovrà essere revisionato entro il 31 marzo di ogni anno successivo al primo.

SCADENZIARIO

Pro-Memoria delle scadenze fissate dal D.Lgs 196/2003 e dal presente DPS :

Ogni Settimana	Aggiornamento delle definizioni dei virus del sistema antivirus adottato
31 Ottobre 2011	Verifica livello di formazione degli Incaricati del trattamento con particolare riferimento ai compiti loro demandati mediante lettera di incarico Verifica e riordino delle autorizzazioni dei singoli incaricati del trattamento in funzione delle esigenze che potrebbero essere mutate nel tempo Certificazione del mantenimento nel tempo delle misure minime di sicurezza
31 Marzo 2012	Rinnovo del Documento Programmatico sulla Sicurezza

CONCLUSIONI ED ASSUNZIONE DELLE RESPONSABILITA'

Il presente Documento Programmatico sulla Sicurezza è stato redatto dallo Studio Tecnico-Legale CORBELLINI, marchio della società a responsabilità limitata a socio unico "Studio AG.I.COM.", con sede in Via Guglielmo Marconi, 4 a Melegnano (MI), sulla base delle informazioni acquisite in uno o più colloqui intercorsi tra i nostri professionisti ed il personale incaricato dal titolare del trattamento dei dati, a descrivere l'attività svolta negli uffici.
Lo Studio non è responsabile per l'esattezza delle informazioni fornite non altrimenti verificabili.

Il Documento Programmatico sulla Sicurezza viene letto e confermato in ogni suo punto.

Data _____

Il Titolare del trattamento

_____