



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

PREFAZIONE

Il Dirigente dell'Istituto Comprensivo di Faedis

Visto il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 34 ss., nonché l'allegato B del suddetto d.lgs., contenente il Disciplinaire tecnico in materia di misure minime di sicurezza.

Considerato che l'Istituto Comprensivo di Faedis, con sede in piazza mons. Pellizzo n. 11 - 33040 Faedis (UD), in quanto dotato di un autonomo potere decisionale, ai sensi dell'art. 28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

Atteso che la suddetta Istituzione scolastica e tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del d.lgs. n.196 del 2003, adotta il presente.

SCOPO E AMBITO DI APPLICAZIONE DEL DPSS

L'Istituzione scolastica, per l'espletamento della funzione didattica e formativa, raccoglie e tratta dati personali dei soggetti coinvolti nell'offerta formativa ovvero dei destinatari della stessa, anche con l'ausilio di soggetti esterni, ai sensi del punto 19 dell'Allegato "B", talché si precisano i seguenti elementi:

- a. Elenco dei trattamenti di dati personali;
- b. Elenco dei dati personali di natura comune, sensibile o giudiziaria
- c. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- d. Ambito dei trattamenti.
- e. Analisi dei rischi incombenti sui dati;
- f. Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- g. Criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- h. Programma degli interventi formativi degli incaricati del trattamento;
- i. Criteri previsti per garantire il rispetto delle misure minime per i trattamenti di dati personali affidati all'esterno della struttura;
- j. Trattamenti di dati personali sensibili o giudiziari con strumenti elettronici affidati all'esterno.

Il Documento Programmatico Sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati nominati con apposite lettere di incarico allegate al presente documento. Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici, interni (P.C.) ovvero collegati in rete fra loro, e/o mediante collegamenti alla rete intranet, e/o alla rete internet. Con riferimento alla gestione dei dati mediante rete ministeriale, l'Istituzione scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

Le sedi e i locali nei quali avviene il trattamento dei dati sono dettagliati nell'allegato EUF.

Le tipologie di dati e le modalità di trattamento sono dettagliate nel modello ECR intestato ad ogni soggetto che riceve l'incarico di accesso alle banche dati.

Le modalità di trattamento dei dati con l'ausilio di strumenti elettronici avvengono secondo i dettami della normativa con le modalità di accesso previste negli allegati ECR e con le ulteriori specifiche descritte nell'allegato LTS.

Le modalità di trattamento dati senza l'ausilio di strumenti elettronici verranno dettagliate nell'allegato LTC redatto dal Responsabile del trattamento o, in mancanza, dal Titolare.

Il presente documento è valido per un anno. Trascorso tale termine, e non oltre il 31 marzo di ogni anno, sarà oggetto di opportune revisioni per adeguarlo ad eventuali modifiche normative, al mutato livello di rischio a cui sono soggetti i dati trattati, ad eventuali assegnazioni o revoche di incarichi, all'utilizzo di nuovi strumenti informatici o in generale a un mutato assetto organizzativo.

ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Finalità:

Al fine di perseguire le finalità istituzionali, l'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori. I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi; somministrazione dei servizi formativi; gestione e formazione del personale, nelle sue varie componenti (docente e non



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

docente, in ruolo presso altri apparati pubblici); adempimenti assicurativi; tenuta della contabilità; gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n. 150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni"; attività strumentali alle precedenti.

L'istituzione scolastica con propria delibera ha adottato il "Regolamento" recante l'identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate come da D.M. n. 305 del 7 dicembre 2006.

Fonte dei dati:

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'istituzione scolastica, in ragione della produzione: di atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art.316 c.c., dei servizi formativi; documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori; documentazione bancaria, finanziaria e/o assicurativa; documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

ELENCO DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE

Sulla scorta delle precisazioni sopra elencate, l'istituzione scolastica, sulla base di una prima ricognizione, con salvezza della possibilità di procedere a successive integrazioni e/o correzioni entro il 30.6.2006, dichiara, con riferimento ai destinatari o famigliari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

- a) Dati identificativi, ai sensi dell'art.4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva.
- b) Dati identificativi, ai sensi dell'art.4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
- c) Dati sensibili, ai sensi dell'art.4, comma 1, lett.d) del d.lgs. n.196 del 2003;
- d) Dati giudiziari, ai sensi dell'art.4, comma 1, lett.e) del d.lgs. n.196 del 2003;
- e) Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- f) Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
- g) Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art.4 comma 1, lett.e) del d.lgs. n.196 del 2003;
- h) Dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei famigliari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
- i) Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- k) Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;
- l) Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
- m) Dati contabili e fiscali;
- n) Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
- o) Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

ELENCO CARICHE

Titolare del trattamento

Al Titolare del trattamento spetta l'onere di individuare e incaricare uno o più Responsabili del Trattamento, qualora lo ritenesse opportuno. La nomina deve avvenire per iscritto e sempre per iscritto il Titolare elencherà in dettaglio le mansioni assegnate. Il Titolare, a tal proposito, redigerà apposita lettera di incarico che dovrà essere sottoscritta per accettazione dal Responsabile. Sarà cura del Titolare conservare in luogo sicuro una copia della lettera di incarico e istruire adeguatamente i Responsabili in merito agli incarichi assegnati.

Tra i compiti non delegabili assegnati al Titolare e prevista la vigilanza sul rispetto da parte dei Responsabili degli incarichi loro assegnati, nonché sulla diligente osservanza delle vigenti disposizioni in materia di trattamento, con particolare riguardo alle misure di sicurezza da adottare.

Nel caso in cui non venisse nominato alcun Responsabile del Trattamento, il Titolare ne assume il ruolo e tutte le responsabilità.



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

Il Titolare del trattamento provvederà ad agevolare l'accesso ai dati personali da parte dell'interessato, a fornirgli le informazioni richieste e a ridurre i tempi per il riscontro del richiedente.

Responsabili del trattamento

In ottemperanza all'articolo 29 del D. lgs 196/2003, il Titolare del Trattamento può nominare uno o più Responsabili del trattamento con apposita lettera di incarico (Modello IRE). La nomina avviene per iscritto. I Responsabili devono essere individuati fra soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, con particolare riguardo alla sicurezza dei dati. I Responsabili, pertanto, dovranno adottare tutte le misure idonee ad assicurare l'integrità dei dati oggetto del trattamento, a ridurre i rischi di diffusione o trattamento di dati non consentiti e mantenere in piena efficienza tutti gli strumenti e la struttura organizzativa al fine di perseguire gli scopi dettati dal presente DPSS.

Per esigenze organizzative il Titolare può suddividere i compiti fra i diversi Responsabili del trattamento nominati.

I Responsabili del trattamento hanno il dovere di informare tempestivamente il Titolare di eventuali incidenti o della sopravvenuta mancanza dei requisiti minimi di sicurezza richiesti.

Ai Responsabili è conferita possibilità di nominare uno o più Incaricati al trattamento e istruirli adeguatamente per renderli idonei a svolgere le mansioni assegnate.

Se non diversamente previsto nella lettera di incarico, la nomina dei Responsabili si intende a tempo indeterminato e decade o per dimissioni o per revoca comunicata per iscritto o con idonei mezzi informatici dal Titolare del trattamento.

Incaricati del trattamento

Qualora la gestione delle banche dati richieda l'intervento operativo di altri soggetti, il Titolare o il Responsabile possono nominare uno o più Incaricati del trattamento con apposita comunicazione scritta (Modello ITR). Sempre per iscritto devono essere specificati i compiti loro assegnati. La lettera di incarico deve essere sottoscritta dal soggetto interessato e sarà cura del Responsabile della conservazione o del Titolare (a seconda di chi ha conferito l'incarico) custodire copia della lettera in luogo sicuro.

Loro compito è quello di svolgere gli incarichi assegnati, dettagliatamente specificati nella lettera di incarico, sempre nel pieno rispetto del presente Documento Programmatico Sulla Sicurezza. In caso di incidenti o di conoscenza di circostanze che possano far venir meno i requisiti minimi di sicurezza, gli Incaricati dovranno comunicare tempestivamente tale circostanza al Responsabile del trattamento o, in mancanza, al Titolare.

Se non diversamente previsto nella lettera di incarico, gli Incaricati del trattamento vengono nominati a tempo indeterminato e decadono per dimissioni o per revoca.

Nomina degli Amministratori di sistema

Il Responsabile del trattamento o il Titolare conferiscono a uno o più incaricati le mansioni di gestione delle soluzioni informatiche sia hardware che software adottate per la gestione e la tenuta in sicurezza delle banche dati. La nomina avviene per iscritto e nella lettera di incarico (Modello IAS) verranno dettagliati i compiti assegnati, compreso quello di approntare i mezzi necessari per effettuare le copie di sicurezza dei dati e il loro ripristino in caso di accidentale distruzione. L'Amministratore di sistema ha anche l'onere di valutare periodicamente lo stato di efficienza delle soluzioni informatiche adottate e provvedere alla loro modifica o integrazione in base all'esperienza acquisita e al progresso tecnologico.

Qualora non fosse già stato incaricato un altro soggetto, l'Amministratore di sistema può essere nominato come custode delle credenziali di autenticazione (codici identificativi, User ID, Password, ecc.) assegnate ad ogni soggetto incaricato.

L'amministratore, nello svolgere questo incarico, si atterra a quanto previsto nel presente DPSS per il Custode delle credenziali di autenticazione.

Nel caso in cui non venisse nominato alcun Amministratore di sistema, le relative mansioni saranno svolte dal Responsabile del trattamento o, in mancanza, dal Titolare.

Nomina del custode delle credenziali di autenticazione

Il Responsabile, di concerto con il Titolare, può nominare uno o più custodi delle credenziali di autenticazione per l'accesso ai sistemi di elaborazione dati. L'incarico viene assegnato per iscritto e la lettera deve essere conservata in un luogo sicuro da parte del soggetto che conferisce l'incarico.

Il Custode delle credenziali sottoscrive il modello ECR col quale prende visione di tutte le credenziali di accesso da custodire. Le credenziali non dovranno essere divulgate e dovranno essere custodite in luogo sicuro. Spetta al custode definire le modalità di utilizzo delle credenziali di autenticazione in caso di impedimenti o prolungata assenza dell'incaricato alle quali sono state assegnate.

In mancanza di un custode delle credenziali di autenticazione, le mansioni sopra riportate saranno svolte dall'Amministratore del sistema o, in mancanza, dal soggetto che ha conferito l'incarico (Responsabile o Titolare del trattamento).



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

L'analisi dei rischi ai quali sono soggetti i dati trattati vengono dettagliati negli allegati EAR/OP - EAR/SO - EAR/HD. In tale documento verrà compilata un'apposita lista dei rischi incombenti sui dati da parte del sistema di elaborazione, dal Sistema operativo, dagli Applicativi. Nello stesso documento sono proposte le azioni correttive o preventive.

L'analisi dei rischi è redatta in relazione al progresso tecnologico, alla sostituzione, integrazione e sostituzione di hardware, agli aggiornamenti o alla sostituzione di sistemi operativi e/o programmi applicativi.

MISURE DI SICUREZZA E CONTROLLO ACCESSO AI LOCALI

In ottemperanza agli artt. 31, 32, 33, 34, 35 e 36 del D. Lgs 30/06/2003 n. 196, il presente DPSS prevede l'organizzazione di idonee misure di sicurezza da adottare volte a garantire la sicurezza dei dati. La sicurezza dei dati si esplica nella loro diligente custodia al fine di prevenirne alterazioni, distruzione, diffusioni non autorizzate o trattamenti non conformi alle finalità della raccolta.

Il Responsabile del trattamento o, in mancanza, il Titolare appronteranno tutti i mezzi necessari per il perseguimento dei fini legati alla sicurezza dei dati, sfruttando anche le conoscenze acquisite in base al progresso tecnico.

Sono previste specifiche misure di sicurezza sia per quanto riguarda la custodia di archivi elettronici e non, che l'accesso ai locali ove i dati oggetto del trattamento fisicamente sono conservati.

La procedura di preservazione dal rischio di perdita dei dati trattati con mezzi informatici o dalla divulgazione non autorizzata si esplica nella previsione di un piano basato su:

Copie periodiche di Backup.

Tale procedura, che il Responsabile del trattamento o il Titolare stileranno di concerto con l'amministratore di sistema, dovrà fornire le istruzioni e le modalità in merito al tipo di supporto utilizzato, all'impiego di specifici software per salvataggi automatizzati, alla nomina degli Incaricati del trattamento che eseguiranno le copie di Backup, alla custodia dei supporti nei quali sono stati memorizzati i dati, alla distruzione dei supporti dopo un certo lasso di tempo o comunque alla cancellazione dei dati dai supporti di Backup in maniera tale da impedire ogni possibile consultazione. La procedura di salvataggio prevede anche il monitoraggio di tutte le operazioni affinché il Responsabile o il Titolare possano individuare periodicamente circostanze che impongano l'adozione di un diverso piano di Backup o il suo aggiornamento.

Il salvataggio dei dati dovrà avvenire con cadenza almeno settimanale. La procedura di Backup è dettagliata nell'allegato LBK e sarà resa nota a tutti gli incaricati del backup.

Protezione da virus informatici o intrusioni non autorizzate nella propria rete informatica.

Il Responsabile del trattamento o il Titolare incaricano l'amministratore del sistema ad approntare tutte le misure di sicurezza idonee a prevenire e ridurre infezioni da Virus informatici o da intrusioni non autorizzate nel sistema.

L'amministratore provvederà a dettagliare nell'allegato EPA tutte le misure adottate compresi l'utilizzo di appositi programmi Antivirus, Firewall e qualsiasi ulteriore soluzione informatica che ritenesse opportuna per diminuire la vulnerabilità del sistema. E' anche compito dell'amministratore pianificare il lavoro relativo all'installazione degli aggiornamenti messi a disposizione delle case produttrici di software per correggere i difetti dei programmi o dei sistemi operativi utilizzati. L'amministratore può prevedere anche che il periodico aggiornamento dei programmi utilizzati per garantire la sicurezza informatica avvenga in un arco di tempo inferiore a quanto previsto dal D. Lgs 30/06/2003 n. 196.

Tutte le misure di sicurezza previste dall'amministratore di sistema dovranno essere periodicamente valutate per adattare la procedura all'evoluzione tecnologica. L'amministratore di sistema dovrà provvedere ad istruire adeguatamente eventuali incaricati al trattamento e consegnargli copia degli allegati EPA (elenco programmi antivirus).

In caso di infezione del sistema da parte di Virus informatici, l'amministratore del sistema dovrà tempestivamente adottare tutte le misure idonee per isolare il sistema ed evitare che il danno venga esteso ad altri elaboratori; dovrà quindi individuare le cause di tale infezione e provvedere a rimuoverle.

Sistema di autenticazione informatica.

Così come previsto dall'Allegato B al D. Lgs 196/2003, il trattamento dei dati personali con strumenti elettronici è consentito solo agli incaricati dotati di credenziali di autenticazione che consentono il superamento di una procedura di autenticazione. Il Responsabile del trattamento (o in mancanza, il Titolare), in accordo con gli Amministratori di sistema, definisce le modalità di assegnazione delle credenziali di autenticazione agli incaricati del trattamento. Le credenziali possono consistere nell'assegnazione di User ID e password o nell'utilizzo di dispositivi associati ad un codice identificativo o anche ad una caratteristica biometrica. Ad ogni soggetto autorizzato all'accesso alle banche dati possono essere assegnate anche più credenziali per l'autenticazione in base alle esigenze organizzative o al numero di banche dati gestite. Se fra le credenziali è prevista l'assegnazione di una password, questa non deve essere di lunghezza inferiore agli otto caratteri (o al numero massimo possibile se lo strumento elettronico utilizzato non lo consente).

Al primo utilizzo delle password, l'incaricato provvederà a modificarla e successivamente la modificherà periodicamente con cadenza almeno semestrale, a meno che la banca dati non contenga dati sensibili; in quest'ultimo caso la parola chiave andrà modificata ogni tre mesi. Ogni persona incaricata al trattamento dei dati deve adottare tutte le cautele possibili per



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

garantire la segretezza delle credenziali di autenticazione assegnate.

Per ciò che concerne la gestione dei dati non trattati con strumenti elettronici, viene appositamente definita la modalità di trattamento e i vari supporti utilizzati. Vengono altresì definite tutte le misure di sicurezza da adottare per evitare l'accidentale perdita o danneggiamento dei dati. Tutte le modalità di trattamento dati senza l'ausilio di strumenti elettronici e della loro sicurezza sono dettagliate nell'allegato LTC.

L'allegato LTC conterrà le modalità di accesso ai locali dove fisicamente vengono gestite le banche dati, sia nel caso di dati trattati con l'ausilio di strumenti elettronici che con altri strumenti. Sarà cura del Responsabile (o in assenza, del Titolare) redigere tale documento.

In ogni caso è fatto divieto a qualunque soggetto di divulgare informazioni concernenti i dati oggetto del trattamento, effettuarne copie di qualsiasi natura (su supporti cartacei, informatici, audiovisivi, ecc.) e distruggere, sottrarre o manipolare il contenuto delle banche dati se non espressamente autorizzato dal Responsabile o dal Titolare.

CRITERI DI RIPRISTINO DATI DANNEGGIATI

In caso di distruzione o danneggiamento dei dati oggetto del trattamento, ogni incaricato, di concerto con l'amministratore del sistema, provvederà a ripristinare i dati mediante utilizzo delle copie di backup realizzate in conformità a quanto descritto nell'allegato LBK. L'amministratore può anche prevedere l'utilizzo di altri strumenti in suo possesso (supporti cartacei, e-mail, registrazioni audiovisive, ecc.) per ricostruire nel modo più fedele possibile i dati distrutti o danneggiati, sia quelli trattati con l'ausilio di strumenti elettronici che quelli trattati con altri tipi di strumenti. In caso di distruzione o danneggiamento degli strumenti utilizzati per l'accesso ai dati, l'Amministratore di sistema (o in mancanza un incaricato nominato dal Responsabile o dal Titolare) provvederà tempestivamente al ripristino del normale stato di utilizzo dei suddetti strumenti o alla loro sostituzione.

La procedura di ripristino o di accesso ai dati avverrà comunque in tempi compatibili con i diritti degli interessati in conformità al punto 23 dell'allegato B del D. Lgs 196/2003.

Ad ogni evento che comporti distruzione, danneggiamento o problemi di accesso ai dati dovrà essere opportunamente aggiornata l'analisi dei rischi di cui al punto III del presente DPSS.

PIANO DI FORMAZIONE DEGLI INCARICATI

L'istituzione scolastica intende aderire alle iniziative formative organizzate dalla direzione regionale del Ministero dell'Istruzione dell'Università e della Ricerca Scientifica, tenendo anche conto dell'economicità di un'azione organizzata su base regionale, rispetto ad una gestione in proprio delle attività formative. L'istituzione opera integrale rinvio alla programmazione della Direzione regionale, riservandosi comunque di agire in via suppletiva, qualora, per ragione organizzative od economiche, non sia possibile far partecipare il proprio personale alle attività di formazione necessarie per adempiere alle prescrizioni ordinamentali. A tal fine il titolare del trattamento sarà tenuto a curare l'effettiva esecuzione dell'attività formativa da parte del personale coinvolto secondo i piani di formazione dettagliati nell'allegato EPF.

DATI AFFIDATI ALL'ESTERNO DELLA STRUTTURA

Qualora il trattamento dei dati venisse affidato in parte o in toto a soggetti esterni alla struttura, la nomina di tali soggetti avverrà per iscritto mediante apposita lettera di incarico. Sarà cura del Titolare conservare in luogo sicuro copia di tale lettera.

La scelta dei Responsabili del trattamento dati in esterno deve ricadere su soggetti che forniscano i requisiti di affidabilità previsti dal D. Lgs 196/2003 (art. 29 comma 2).

Sarà compito del Responsabile esterno nominare gli incaricati e impartire loro la dovuta istruzione per garantire il trattamento e la conservazione dei dati in modo puntuale, lecito e sicuro.

Ogni trattamento di dati affidato a terzi verrà elencato nell'apposito allegato ITE. Nello stesso documento dovranno essere riportati anche i luoghi dove vengono fisicamente trattati e conservati i dati. Al Titolare del trattamento spetta il compito di vigilare sull'operato del Responsabile esterno affinché non vengano mai meno le misure minime di sicurezza dei dati.

VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI

L'Istituzione scolastica ha affidato all'esterno, nei termini risultanti dall'allegato ITE i trattamenti di dati personali sensibili o giudiziari, effettuato con strumenti elettronici, previa assunzione da parte dell'affidatario nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo degli impegni derivanti dalle seguenti dichiarazioni:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

Prot. n. 6257/A35

essere;

4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire (allertare) immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

CIFRATURA DEI DATI RELATIVI ALLO STATO DI SALUTE

Qualora la tipologia dei dati trattati comprendesse anche quelli di tipo sanitario relativi allo stato di salute o alla vita sessuale nell'allegato LTS verranno previste idonee misure per gestire la separazione dei dati dall'individuazione diretta dell'interessato ed individuare i casi in cui necessita la loro cifratura.

ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI

I trattamenti di dati personali con strumenti diversi da quelli elettronici sono effettuati dagli incaricati seguendo le istruzioni scritte ad essi impartite con il documento di cui all'allegato LTC, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ha carattere annuale. Gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solamente alle persone preventivamente autorizzate.

Faedis, 02/12/2011

IL DIRIGENTE SCOLASTICO
prof.ssa Laura Bertoli



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
(art. 34 Decreto Legislativo n. 196/2003)

ELENCO ALLEGATI

Elenco lettere di incarico

- IRE - Lettera di incarico del responsabile del trattamento dei dati e mansioni assegnate;
- ITR - Nomina dell'incaricato del trattamento dei dati e mansioni assegnate;
- IAS - Lettera di incarico dell'amministratore del sistema e mansioni assegnate;
- ICC - Lettera di incarico al custode delle credenziali di autenticazione e mansioni assegnate;
- IAC - Nomina del responsabile degli accessi ai locali;
- ITE - Lettera di incarico del responsabile esterno del trattamento dei dati e mansioni assegnate
(redatta solo all'occorrenza).
- ECR - Sistema di autorizzazione e criteri di assegnazione delle password degli incaricati;
- LAP - Criteri di assegnazione delle password nei sistemi di elaborazione;
- LPD - Modalità di protezione dei dati;
- LTS - Ulteriori misure in caso di trattamento di dati sensibili o giudiziari;
- LTC - Modalità di trattamento dei dati senza l'ausilio di strumenti elettronici.

Elenco allegati

- EUF - Elenco sedi ed uffici nei quali avviene il trattamento dei dati;
- EUE - Elenco sedi ed uffici nei quali avviene il trattamento dei dati affidato all'esterno della struttura
del titolare (redatto solo all'occorrenza);
- EIN - Elenco degli incaricati al trattamento dei dati personali;
- EPF - Piano di formazione degli incaricati;
- EDB - Elenco dei trattamenti di dati personali (elenco banche dati);
- ELA - Elenco elaboratori;
- EPA - Elenco programmi adottati per la sicurezza dei dati trattati con strumenti elettronici;
- LBK - Procedura di backup e ripristino dati;
- EAR - Analisi dei rischi incombenti sui dati (EAR/AP rischi applicazioni, EAR/SO rischi sistema
operativo, EAR/HD rischi hardware EAR/LOC rischi dei locali);



ISTITUTO COMPRENSIVO DI FAEDIS
Piazza Mons. Pelizzo n. 11 - 33040 FAEDIS (UD)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

Allegato
EUF

ELENCO UFFICI

NOME UFFICIO	SEDE UFFICIO COMPETENTE	DESCRIZIONE UFFICIO	RESPONSABILE UFFICIO
SEGRETERIA I.C. FAEDIS Piazza mons. Pelizzo 11 - 33040 FAEDIS	SEGRETERIA I.C. FAEDIS	Svolgimento di attività amministrativo contabile, relativa alle aree Alunni, Personale, Bilancio e Contabilità dell' I.C. di Faedis	CUDICIO ORIANA
UFFICIO DIRIGENTE SCOLASTICO Piazza mons. Pelizzo 11 - 33040 FAEDIS	UFFICIO DIRIGENTE SCOLASTICO	Attività dirigenziale dell' I.C. di Faedis	BERTOLI LAURA
SCUOLA INFANZIA ATTIMIS Via Ristori 16 - 33040 ATTIMIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola dell'infanzia.	BERTOLI LAURA
SCUOLA INFANZIA CAMPEGLIO Via S. Michele 1 - 33040 CAMPEGLIO	SCUOLA I.C. FAEDIS	Attività didattica di scuola dell'infanzia.	BERTOLI LAURA
SCUOLA INFANZIA FAEDIS Via Pranuf 19 - 33040 FAEDIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola dell'infanzia.	BERTOLI LAURA
SCUOLA INFANZIA POVOLETTO Via Cividina, 15 - 33040 POVOLETTO	SCUOLA I.C. FAEDIS	Attività didattica di scuola dell'infanzia.	BERTOLI LAURA
SCUOLA PRIMARIA ATTIMIS Via Ristori 16 - 33040 ATTIMIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola primaria.	BERTOLI LAURA
SCUOLA PRIMARIA FAEDIS Via Pranuf 19 - 33040 FAEDIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola primaria.	BERTOLI LAURA
SCUOLA PRIMARIA POVOLETTO Via Casali Merlo 1 - Loc. Marsure - 33040 FAEDIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola primaria.	BERTOLI LAURA
SCUOLA SECONDARIA DI 1° GRADO FAEDIS Via Pranuf 15 - 33040 FAEDIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola secondaria di primo grado.	BERTOLI LAURA
SCUOLA SECONDARIA DI 1° GRADO POVOLETTO Via della Locanda 26 - Loc. Marsure - 33040 FAEDIS	SCUOLA I.C. FAEDIS	Attività didattica di scuola secondaria di primo grado.	BERTOLI LAURA



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

INCARICO DEL RESPONSABILE DEL TRATTAMENTO DEI DATI
E MANSIONI ASSEGNATE

Prot. n. 6257/A35

Faedis, 02/12/2011

Alla Sig.ra **CUDICIO ORIANA**,

ai sensi dell'art 29 del D. Lgs 196/2003, la sottoscritta prof.ssa Laura Bertoli in qualità di Titolare del trattamento dei dati, Le affida l'incarico di Responsabile del Trattamento dei dati della sede **SEGRETERIA I.C. FAEDIS presso Piazza mons. Pelizzo 11 - 33040 FAEDIS**.

Accettando questo incarico il Responsabile si impegna ad eseguire il trattamento dei dati conformemente al dettato legislativo e nel pieno rispetto del Documento Programmatico Sulla Sicurezza dei dati, del quale riceve copia, nella piena consapevolezza degli obblighi assunti e delle responsabilità che ne derivano.

L'incarico assegnatoLe riguarda il trattamento dei dati trattati con le seguenti autorizzazioni:

- inserimento
- modifica
- lettura
- eliminazione
- stampa

Le persone che Lei nominerà per l'espletamento di specifiche mansioni saranno scelte fra soggetti con comprovate qualità morali e professionali che garantiscano idonea garanzia del rispetto delle norme vigenti in materia di trattamento dei dati. Sull'operato dei soggetti incaricati Lei vigilerà costantemente al fine di evitare che vengano disattese le norme relative all'utilizzo delle banche dati, con particolare riguardo al profilo della sicurezza. Di ogni incarico assegnato Lei provvederà a consegnare al Titolare copia delle relative lettere.

Oltre a quanto sopra riportato, Le sono assegnate le seguenti mansioni:

- individuare e nominare per iscritto, qualora lo ritenesse opportuno, uno o più Incaricati al trattamento;
- individuare e nominare per iscritto, qualora lo ritenesse opportuno, uno o più Amministratori di sistema;
- individuare e nominare per iscritto, qualora lo ritenesse opportuno, un custode delle Password;
- individuare e nominare per iscritto, qualora lo ritenesse opportuno, uno o più incaricati alla manutenzione degli strumenti utilizzati per il trattamento e la custodia dei dati;
- autorizzare gli incaricati all'utilizzo degli strumenti per l'accesso alle banche dati e, con l'eventuale cooperazione dell'Amministratore del sistema, assegnare loro le credenziali di autenticazione per il superamento delle procedure di autenticazione;
- verificare lo stato di efficienza di tutti gli strumenti informatici utilizzati per la sicurezza dei dati pianificando con l'eventuale Amministratore di sistema la periodicità degli aggiornamenti da eseguire per quanto riguarda i programmi Antivirus o qualsiasi altra soluzione informatica ritenuta idonea a diminuire i rischi di infezioni del sistema o accessi non autorizzati;
- garantire agli interessati il pieno esercizio dei diritti previsti dall'artt. 7, 8, 9 e 10 del D. Lgs 196/2003;
- attuare gli obblighi relativi all'informativa sulla privacy in fase di acquisizione del consenso;
- collaborare con il Garante per l'espletamento delle sue funzioni di accertamento, ispezione e controllo;
- informare tempestivamente il Titolare del trattamento di qualunque circostanza rilevante in merito ai rischi sulla sicurezza dei dati, ad eventuali danni subiti dalle banche dati o dagli strumenti utilizzati per la loro gestione o custodia, alle revoche degli incarichi assegnati e a qualsiasi modifica che si renda necessaria nelle procedure elencate nel Documento Programmatico Sulla Sicurezza.

La qualifica assegnataLe è da intendersi tacitamente rinnovata ogni anno sino a revoca dell'incarico comunicata dal Titolare per iscritto o con idonei mezzi informatici.

Il Titolare del trattamento _____

Prof.ssa Laura Bertoli

Il Responsabile per accettazione _____

Cudicio Oriana



ISTITUTO COMPRENSIVO DI FAEDIS

Piazza Mons. Pelizzo n. 11 - 33040 FAEDIS (UD)

**Allegato
IAS/1**

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

Art. 34 Decreto Legislativo n. 196/2003

**INCARICO A CUSTODE DELLE CREDENZIALI DA PARTE DEL RESPONSABILE AL TRATTAMENTO DEI DATI
DELLA SEDE**

La sottoscritta **Sig.ra CUDICIO ORIANA** in qualita di Responsabile del trattamento dei dati della sede

"SEGRETERIA I.C. FAEDIS",

DICHIARA

di provvedere personalmente a svolgere l'incarico di:

CUSTODE DELLE CREDENZIALI

come specificato negli allegati sotto descritti IAS e ICC

Faedis,02/12/2011

Il Responsabile del trattamento

Cudicio Oriana



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI
SENSIBILI O GIUDIZIARI

Sede SEGRETERIA I.C. FAEDIS

Piazza mons. Pelizzo 11 - 33040 FAEDIS

Protezione dei dati

Al fine di proteggere le Banche Dati da intrusioni di soggetti o programmi non autorizzati al trattamento, sono utilizzati appositi strumenti software dettagliati nel modello EPA ed è nominato uno o più soggetti "Responsabili degli accessi ai locali" (modello IAC) il quale si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate al trattamento.

Protezione dei supporti rimovibili

I supporti rimovibili sono affidati in custodia all'incaricato del trattamento. Il responsabile degli accessi si assicurerà che i supporti rimovibili non saranno condotti al di fuori dei locali in cui i dati sono assegnati come da "Elenco sedi ed Uffici nei quali avviene il trattamento dei dati" (modello EUF) al punto "Elenco uffici dove si svolge il trattamento dei dati".

Distruzione dei supporti rimovibili

I supporti rimovibili che contengono dati non più utilizzati sono distrutti cancellando i dati in essi contenuti ove questo sia possibile. Nel caso di supporti non riscrivibili questi sono distrutti fisicamente.

Dati relativi allo stato di salute e la vita sessuale

In applicazione dell'Art 22 c.6 Dlgs 196/2003 e dell'allegato B punto 24, i dati relativi allo stato di salute e alla vita sessuale dell'interessato sono trattati in forma anonima prevedendo la separazione dei dati sensibili dai dati identificativi, questa procedura viene effettuata dall'applicativo fornito dal MIUR - SISSI IN RETE. Qualora si rendesse necessario l'individuazione dell'interessato, questa avviene in maniera indiretta recuperando dai dati identificativi il codice identificativo univoco e ricercando i dati sensibili che corrispondono a detto codice univoco.

Faedis,02/12/2011

Il Responsabile del trattamento

Cudicio Oriana

L'Amministratore di Sistema

Click Idea Di Bragalini Tatiana



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI
SENSIBILI O GIUDIZIARI

Sede UFFICIO DIRIGENTE SCOLASTICO

Piazza mons. Pelizzo 11 - 33040 FAEDIS

Protezione dei dati

Al fine di proteggere le Banche Dati da intrusioni di soggetti o programmi non autorizzati al trattamento, sono utilizzati appositi strumenti software dettagliati nel modello EPA ed è nominato uno o più soggetti "Responsabili degli accessi ai locali" (modello IAC) il quale si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate al trattamento.

Protezione dei supporti rimovibili

I supporti rimovibili sono affidati in custodia all'incaricato del trattamento. Il responsabile degli accessi si assicurerà che i supporti rimovibili non saranno condotti al di fuori dei locali in cui i dati sono assegnati come da "Elenco sedi ed Uffici nei quali avviene il trattamento dei dati" (modello EUF) al punto "Elenco uffici dove si svolge il trattamento dei dati".

Distruzione dei supporti rimovibili

I supporti rimovibili che contengono dati non più utilizzati sono distrutti cancellando i dati in essi contenuti ove questo sia possibile. Nel caso di supporti non riscrivibili questi sono distrutti fisicamente.

Dati relativi allo stato di salute e la vita sessuale

In applicazione dell'Art 22 c.6 D.Lgs 196/2003 e dell'allegato B punto 24, i dati relativi allo stato di salute e alla vita sessuale dell'interessato sono trattati in forma anonima prevedendo la separazione dei dati sensibili dai dati identificativi, questa procedura viene effettuata dall'applicativo fornito dal MIUR - SISSI IN RETE. Qualora si rendesse necessario l'individuazione dell'interessato, questa avviene in maniera indiretta recuperando dai dati identificativi il codice identificativo univoco e ricercando i dati sensibili che corrispondono a detto codice univoco.

Faedis, 02/12/2011

Il Titolare del trattamento _____

Bertoli Laura

L'Amministratore di Sistema _____



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' TRATTAMENTO DATI SENZA L'AUSILIO
DI STRUMENTI ELETTRONICI

Sede SEGRETERIA I.C. FAEDIS

Piazza mons. Pelizzo 11 - 33040 FAEDIS

Nel caso il trattamento dei dati si svolga senza l'ausilio di strumenti elettronici tutti gli incaricati al trattamento sono tenuti ad attenersi alle seguenti istruzioni:

Modalità di accesso ai locali

Si rimanda a quanto descritto nel Modello LPD.

Modalità di accesso ai dati

Gli incaricati devono operare sui dati osservando scrupolosamente i limiti descritti nel Modello ECR.

Modalità di consultazione

La consultazione dei dati avviene in maniera riservata assicurandosi che nessun altro, ad esclusione dell'incaricato, possa prendere visione del documento in trattamento.

Custodia e responsabilità del supporto

Sara cura dell'incaricato assicurare che i dati personali affidategli non siano consultati da altri non autorizzati. Durante una sessione di trattamento l'incaricato ha l'obbligo di non lasciare incustoditi i dati personali e di riporli alla fine del trattamento.

Divieto di copia e riproduzione

E' fatto divieto all'incaricato di fare delle copie o riprodurre i documenti trattati. Fatto salvo il caso in cui l'oggetto del trattamento non sia esplicitamente la copia o la riproduzione al fine di garantire i diritti dell'interessato, oppure sia stato straordinariamente autorizzato dal titolare o dal responsabile del trattamento.

Trattamento di dati relativi alla vita sessuale e/o allo stato di salute

I dati relativi allo stato di salute sono trattati con le modalità previste nel Modello LTS.

Faedis,02/12/2011

Il Responsabile del trattamento

Cudicio Oriana



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' TRATTAMENTO DATI SENZA L'AUSILIO
DI STRUMENTI ELETTRONICI

Sede SCUOLA I.C. FAEDIS

Piazza mons. Pelizzo 11 - 33040 FAEDIS

Nel caso il trattamento dei dati si svolga senza l'ausilio di strumenti elettronici tutti gli incaricati al trattamento sono tenuti ad attenersi alle seguenti istruzioni:

Modalità di accesso ai locali

Si rimanda a quanto descritto nel Modello LPD.

Modalità di accesso ai dati

Gli incaricati devono operare sui dati osservando scrupolosamente i limiti descritti nel Modello ECR.

Modalità di consultazione

La consultazione dei dati avviene in maniera riservata assicurandosi che nessun altro, ad esclusione dell'incaricato, possa prendere visione del documento in trattamento.

Custodia e responsabilità del supporto

Sarà cura dell'incaricato assicurare che i dati personali affidategli non siano consultati da altri non autorizzati. Durante una sessione di trattamento l'incaricato ha l'obbligo di non lasciare incustoditi i dati personali e di riporli alla fine del trattamento.

Divieto di copia e riproduzione

E' fatto divieto all'incaricato di fare delle copie o riprodurre i documenti trattati. Fatto salvo il caso in cui l'oggetto del trattamento non sia esplicitamente la copia o la riproduzione al fine di garantire i diritti dell'interessato, oppure sia stato straordinariamente autorizzato dal titolare o dal responsabile del trattamento.

Trattamento di dati relativi alla vita sessuale e/o allo stato di salute

I dati relativi allo stato di salute sono trattati con le modalità previste nel Modello LTS.

Faedis,02/12/2011

Il Titolare del trattamento

_____ *Bertoli Laura*



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' TRATTAMENTO DATI SENZA L'AUSILIO
DI STRUMENTI ELETTRONICI

Sede UFFICIO DIRIGENTE SCOLASTICO

Piazza mons. Pelizzo 11 - 33040 FAEDIS

Nel caso il trattamento dei dati si svolga senza l'ausilio di strumenti elettronici tutti gli incaricati al trattamento sono tenuti ad attenersi alle seguenti istruzioni:

Modalità di accesso ai locali

Si rimanda a quanto descritto nel Modello LPD.

Modalità di accesso ai dati

Gli incaricati devono operare sui dati osservando scrupolosamente i limiti descritti nel Modello ECR.

Modalità di consultazione

La consultazione dei dati avviene in maniera riservata assicurandosi che nessun altro, ad esclusione dell'incaricato, possa prendere visione del documento in trattamento.

Custodia e responsabilità del supporto

Sarà cura dell'incaricato assicurare che i dati personali affidategli non siano consultati da altri non autorizzati. Durante una sessione di trattamento l'incaricato ha l'obbligo di non lasciare incustoditi i dati personali e di riporli alla fine del trattamento.

Divieto di copia e riproduzione

E' fatto divieto all'incaricato di fare delle copie o riprodurre i documenti trattati. Fatto salvo il caso in cui l'oggetto del trattamento non sia esplicitamente la copia o la riproduzione al fine di garantire i diritti dell'interessato, oppure sia stato straordinariamente autorizzato dal titolare o dal responsabile del trattamento.

Trattamento di dati relativi alla vita sessuale e/o allo stato di salute

I dati relativi allo stato di salute sono trattati con le modalità previste nel Modello LTS.

Faedis,02/12/2011

Il Titolare del trattamento

Bertoli Laura



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' DI PROTEZIONE DEI DATI E DEI LOCALI

Sede SEGRETERIA I.C. FAEDIS

Piazza mons. Pelizzo 11 - 33040 FAEDIS

In esecuzione del punto 19.4 dell'allegato B al Dlgs 196/2003, al fine di garantire l'integrità e la disponibilità dei dati, la protezione delle aree e dei locali, si definiscono le seguenti misure di sicurezza:

Protezione dei locali e degli accessi

Durante il normale orario di lavoro un apposito soggetto incaricato per iscritto e denominato "Responsabile degli accessi ai locali" si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate al loro trattamento.

Protezione delle banche dati e degli schedari

Nel caso di banca dati cartacea, gli schedari (o altro contenitore) di dati personali devono essere protetti da lucchetti, serrature o misure di protezione equivalenti (vedi modello EUF) .

Nel caso di banca dati in formato elettronico i dati sono protetti tramite la predisposizione di un apposito sistema di credenziali di accesso (vedi modello EUF).

Protezione delle banche dati fuori dall'orario di lavoro

Fuori dall'orario di lavoro, nel caso di banche dati non protette da strumenti elettronici per il controllo degli accessi si adottano le seguenti misure: per ogni locale è tenuto, in loco, un registro degli accessi in cui i soggetti, preventivamente autorizzati, sono obbligati ad iscrivere la data e l'ora dell'avvenuto accesso, la banca dati utilizzata, il proprio codice di identificazione (o in alternativa il nome e cognome), il soggetto (titolare o responsabile) che ha autorizzato l'accesso.

Nel caso di accesso ai dati fuori dall'orario di lavoro o, in casi speciali o particolari, l'incaricato ha l'obbligo di farsi autorizzare dal responsabile (o dal titolare) la sessione di trattamento. L'autorizzazione può essere anche verbale purché l'incaricato abbia cura di annotarla nel registro degli accessi.

Faedis,02/12/2011

Il Responsabile del trattamento

Cudicio Oriana



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' DI PROTEZIONE DEI DATI E DEI LOCALI

Sede SCUOLA I.C. FAEDIS

Piazza mons. Pelizzo 11 - 33040 FAEDIS

In esecuzione del punto 19.4 dell'allegato B al Dlgs 196/2003, al fine di garantire l'integrità e la disponibilità dei dati, la protezione delle aree e dei locali, si definiscono le seguenti misure di sicurezza:

Protezione dei locali e degli accessi

Durante il normale orario di lavoro un apposito soggetto incaricato per iscritto e denominato "Responsabile degli accessi ai locali" si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate al loro trattamento.

Protezione delle banche dati e degli schedari

Nel caso di banca dati cartacea, gli schedari (o altro contenitore) di dati personali devono essere protetti da lucchetti, serrature o misure di protezione equivalenti (vedi modello EUF) .

Nel caso di banca dati in formato elettronico i dati sono protetti tramite la predisposizione di un apposito sistema di credenziali di accesso (vedi modello EUF).

Protezione delle banche dati fuori dall'orario di lavoro

Fuori dall'orario di lavoro, nel caso di banche dati non protette da strumenti elettronici per il controllo degli accessi si adottano le seguenti misure: per ogni locale è tenuto, in loco, un registro degli accessi in cui i soggetti, preventivamente autorizzati, sono obbligati ad iscrivere la data e l'ora dell'avvenuto accesso, la banca dati utilizzata, il proprio codice di identificazione (o in alternativa il nome e cognome), il soggetto (titolare o responsabile) che ha autorizzato l'accesso.

Nel caso di accesso ai dati fuori dall'orario di lavoro o, in casi speciali o particolari, l'incaricato ha l'obbligo di farsi autorizzare dal responsabile (o dal titolare) la sessione di trattamento. L'autorizzazione può essere anche verbale purché l'incaricato abbia cura di annotarla nel registro degli accessi.

Faedis,02/12/2011

Il Titolare del trattamento

_____ *Bertoli Laura*



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI
Art. 34 Decreto Legislativo n. 196/2003

MODALITA' DI PROTEZIONE DEI DATI E DEI LOCALI

Sede UFFICIO DIRIGENTE SCOLASTICO

Piazza mons. Pelizzo 11 - 33040 FAEDIS

In esecuzione del punto 19.4 dell'allegato B al Dlgs 196/2003, al fine di garantire l'integrità e la disponibilità dei dati, la protezione delle aree e dei locali, si definiscono le seguenti misure di sicurezza:

Protezione dei locali e degli accessi

Durante il normale orario di lavoro un apposito soggetto incaricato per iscritto e denominato "Responsabile degli accessi ai locali" si occupa di verificare che le persone che accedono ai locali siano state preventivamente autorizzate al loro trattamento.

Protezione delle banche dati e degli schedari

Nel caso di banca dati cartacea, gli schedari (o altro contenitore) di dati personali devono essere protetti da lucchetti, serrature o misure di protezione equivalenti (vedi modello EUF) .

Nel caso di banca dati in formato elettronico i dati sono protetti tramite la predisposizione di un apposito sistema di credenziali di accesso (vedi modello EUF).

Protezione delle banche dati fuori dall'orario di lavoro

Fuori dall'orario di lavoro, nel caso di banche dati non protette da strumenti elettronici per il controllo degli accessi si adottano le seguenti misure: per ogni locale è tenuto, in loco, un registro degli accessi in cui i soggetti, preventivamente autorizzati, sono obbligati ad iscrivere la data e l'ora dell'avvenuto accesso, la banca dati utilizzata, il proprio codice di identificazione (o in alternativa il nome e cognome), il soggetto (titolare o responsabile) che ha autorizzato l'accesso.

Nel caso di accesso ai dati fuori dall'orario di lavoro o, in casi speciali o particolari, l'incaricato ha l'obbligo di farsi autorizzare dal responsabile (o dal titolare) la sessione di trattamento. L'autorizzazione può essere anche verbale purché l'incaricato abbia cura di annotarla nel registro degli accessi.

Faedis,02/12/2011

Il Titolare del trattamento

_____ *Bertoli Laura*