MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

GDPR

Registro dei Trattamenti

Ai sensi dell'Art. 30 del R.E. 2016/679

Data Agg.to
01/09/2019

Il Dirigente scolastico

Visto il regolamento UE 2016/679, noto anche come GDPR (General Data Protection Regulation), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati;

Visto il decreto legislativo 7b dicembre 2006, n. 305 – "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli artt. 20 e 21 del D.Lgs del 30 giugno 2003, n.196, recante il Codice in materia di protezione di dati personali;

Visto il Decreto Legislativo 10 agosto 2018 n. 101 recante le Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Visto l'art. 30 del Regolamento UE 2016/679 GDPR

adotta il seguente **Registro dei Trattamenti,** allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Istituto Scolastico - indispensabile per ogni valutazione e analisi del rischio, che contiene le informazioni relative ai dati del titolare, le finalità del trattamento, alle categorie degli interessati e dei dati trattati, le categorie dei destinatari, le misure di sicurezza tecniche ed organizzative, ma anche

1. NOME E DATI DEL TITOLARE DEL TRATTAMENTO

IL TITOLARE DEL TRATTAMENTO:
ISTITUTO COMPRENSIVO ANZIO III– Via Machiavelli s.n.c. – C.M. RMIC8C700E
00043 Anzio (RM)
TEL. 069873212- FAX Fax 069874249
e-mail: rmic8c700e@istruzione.it-posta certificata: rmic8c700e@pec.istruzione.it

Legale Rappresentante
Dirigente Scolastico Dott.ssa Maria Teresa D'Orso

2. INDICAZIONI RELATIVE AI DATI TRATTATI

In questa parte del documento vengono fornite informazioni essenziali in merito ai dati personali trattati, con riferimento alla natura ed alla classificazione;

NATURA DEI DATI TRATTATI
La natura dei dati soggetti al trattamento da parte della scuola è la seguente:

- Documentazioni complete riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- Documenti prodotti dalle famiglie anche riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche;
- Documentazione riguardante il personale docente e non docente anche con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari;
- Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi
- Dati contabili e fiscali

TIPO DI DATI

Sulla scorta delle precisazioni sopra elencate, l'Istituzione Scolastica, sulla base di una prima ricognizione, con riserva della possibilità di procedere a successive integrazioni e/o correzioni dichiara, con riferimento ai destinatari o familiari 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:

- dati personali comuni (dati anagrafici o identificativi delle persone, indirizzi, recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione …);
- dati sensibili (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, appartenenza a categorie protette, portatore di handicap, stato di gravidanza, vita sessuale etc.);
- dati giudiziari (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato o indagato ai sensi degli artt. 60 o 61 del cod. proc. pen., avviso di garanzia, separazioni, affidamento dei figli, etc.).

Nel trattamento dei **dati di natura sensibile e giudiziaria**, così come definiti dall'art. 4 lettere d) ed e), verrà osservato il documento redatto da codesto istituto dal titolo "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dall'Istituto scolastico".

BANCHE DATI ATTIVATE

Le banche dati attivate sono quelle di seguito riportate:

- Alunni
- Dipendenti
- Protocollo
- Inventario
- Magazzino
- Rapporti con enti ed imprese
- Fornitori
- Bilancio
- Stipendi
- Registro di classe
- Registro degli insegnanti
- Registro infortuni alunni e dipendenti

FINALITÀ PERSEGUITA CON IL TRATTAMENTO DEI DATI

Nell'ambito della propria funzione istituzionale l'Istituto scolastico tratta dati personali di studenti, personale dipendente e fornitori, anche mediante strumenti informatici, per le seguenti finalità:

- Garanzia del servizio scolastico
- Gestione e formazione del personale
- Adempimenti assicurativi
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori
- Attività strumentali alle precedenti

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico.

AFFIDAMENTO DEI DATI A TERZI PER IL TRATTAMENTO:
Tutti i dati posseduti dalla scuola vengono trattati esclusivamente presso gli Uffici dell'Istituto e la piattaforma di gestione documentale messa a disposizione di un fornitore esterno e nessuna altra struttura concorre al trattamento dei dati raccolti dall'Istituto. I dati potranno essere comunicati a terzi solo nell'ambito dell'attività istituzionale dell'Istituto e comunque nei casi previsti dalla informativa fornita agli interessati od in seguito ad esplicito consenso espresso dagli stessi.

MODALITÀ DI TRATTAMENTO
I trattamenti sono realizzati prevalentemente:

- negli uffici di direzione e segreteria,
- nell' archivio della sede centrale,
- nelle aule scolastiche;
- sul sito della scuola.

I dati sono trattati con fascicoli e atti cartacei e con strumenti elettronici di elaborazione.
La conservazione ed il trattamento dei dati avviene nel modo seguente:

CARTACEO:

I dati in possesso della scuola sono conservati in locali e armadi dotati di chiusura a chiave ai quali hanno accesso esclusivamente le persone incaricate. Alcuni dati personali non sensibili possono essere riposti in armadi senza serratura ospitati in locali vigilati e sotto il controllo dei collaboratori scolastici anche dopo l'orario di chiusura degli uffici.
Per i dati sensibili si garantiranno maggiori misure di riservatezza con fascicolazione a parte, con eventuale cifratura o individuando criteri per criptare i dati stessi

MEDIANTE IL SISTEMA INFORMATICO:

Il controllo degli accessi alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autenticazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una credenziale logica costituita da un codice identificativo associato ad una password.
Il trattamento dei dati avviene attraverso modalità diverse:
strumenti elettronici collegati in rete fra loro e/o mediante collegamenti alla rete intranet, al Sidi, alla rete internet.
Inoltre, l'Istituzione scolastica si serve di software applicativi forniti da Axios. Attraverso tale software applicativo viene effettuata, altresì, in adempimento degli obblighi di legge, la conservazione a norma del protocollo.
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. I supporti di memorizzazione dei dati sono custoditi negli uffici della scuola siti al primo piano della Sede Centrale, ove si trova altresì una cassaforte

ELENCO DEI TRATTAMENTI DI DATI PERSONALI
Informazioni di base e descrizione degli strumenti utilizzati:

1		**2**		**3**	**4**	**5**
Identificativo del Trattamento		**Natura dei dati trattati**	**S G**	**Struttura di riferimento**	**Altre strutture concorrenti al trattamento**	**Descrizione degli strumenti utilizzati**
Descrizione Sintetica						
Tr.1	Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro del personale dipendente ecc	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati) r	Collaboratori del D.S., Collaboratori scolastici, RSPP e addetti SPP, Medico Competente	Documenti cartacei, registri e strumenti elettronici, marcatempo collegato al computer
Tr.2	DIPENDENTI E ASSIMILATI Gestione del contenzioso e	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)		Documenti cartacei e strumenti elettronici

	procedimenti disciplinari					
Tr.3	Organismi collegiali e commissioni istituzionali	S		Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei e strumenti elettronici
Tr.4	Attività propedeutiche all' avvio dell'anno scolastico	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Docenti, Collaboratori scolastici,	Documenti cartacei, registri e strumenti elettronici
Tr.5	Attività educativa, didattica e formativa, di valutazione	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Docenti, Collaboratori scolastici, membri esterni organi collegiali	Documenti cartacei, registri e strumenti elettronici
Tr.6	Scuole non statali (OPZIONALE, a seconda delle competenze del Dirigente)	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)		Documenti cartacei, registri e strumenti elettronici
Tr.7	Rapporti scuola – famiglie : gestione del contenzioso	S	G	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati), Docenti,		Documenti cartacei e strumenti elettronici
Tr.8	Fornitori e clienti			Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S., Docenti nelle commissioni, Membri di organi Collegiali, Collaboratori scolastici	Documenti cartacei e strumenti elettronici
Tr.9	Gestione finanziaria e contabile			Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S.	Documenti cartacei e strumenti elettronici
Tr.10	Gestione Istituzionale			Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati)	Collaboratori del D.S.	Documenti cartacei e strumenti elettronici
Tr.11	Gestione sito web dell’istituto			Dirigente Scolastico, Incaricati sito web	Azienda esterna	Documenti cartacei e strumenti elettronici

3. STRUTTURA ORGANIZZATIVA FUNZIONALE AL TRATTAMENTO DATI

Si riporta di seguito una sintetica descrizione della struttura organizzativa funzionale al trattamento dei dati con i riferimenti agli incarichi conferiti, ai trattamenti operati ed alle relative responsabilità:

Struttura:	**Trattamenti operati dalla struttura:**	**Compiti della struttura:**
Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
INCARICATI INTERNI, UNITA' ORGANIZZATIVE OMOGENEE:		
Collaboratori del DS	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr.10 Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc,)
Collaboratori sc. e personale ausiliario	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni,

	Se membri di commissione Tr.2 (dati sensibili o giudiziari).	docenti e familiari
Membri ESTERNI di Organi Collegiali	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
INCARICATI INTERNI CON COMPITI SPECIFICI O ULTERIORI:		
Incaricato del Backup periodico	Tutti, ma limitatamente alla funzione	Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali. .
Custode delle passwords	Tutti i trattamenti informatici , ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
Tecnico interno della Manutenzione del Software [se esistente]	Tutti, ma limitatamente alla funzione	Manutenzione del software e piccoli interventi sull'hardware
R.S.P.P. e Addetti al S.P.P., R.L.S.	I trattamenti relativi all'applicazione della normativa sulla sicurezza (attualmente Testo unico DLgs. 81/08) o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale

	Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	
RLS – rappresentante dei lavoratori per la sicurezza	Diritto di consultazione di tutti i documenti e materiali informatici strettamente inerenti alla funzione e risultanti come diritto di conoscenza	Contributo all'applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale; verifica ecc.
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap [se esistenti] creazione e gestione del sito web [se esistente]	tutti i trattamenti informatizzati e non relativi all'attività Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni con handicap didattico grave
Personale incaricato della creazione e gestione del sito web [se esistente]	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Tr.11 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
Altri eventuali dipendenti Incaricati		
RESPONSABILI INTERNI DI TRATTAMENTO:		
RESPONSABILE DI TRATTAMENTI: Direttore Servizi Generali Amm.vi	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Altro		
INCARICATI ESTERNI:		
Medico competente ai sensi del Dlgs 81/2008 [se esistente]	I trattamenti relativi all'applicazione della normativa 81/2008 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di laoro e nella scuola in generale

	alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	
RSPP o Addetto al S.P.P. ai sensi del Dlgs 81/2008.	I trattamenti relativi all'applicazione della normativa 81/2008 o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare: Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc. Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari Tr.3 Organismi collegiali e commissioni istituzionali Tr.4 Attività propedeutiche all' avvio dell'anno scolastico Tr.5 Attività educativa, didattica e formativa, di valutazione	Applicazione normativa Dlgs 81/2008 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
Incaricato Tecnico Esterno della Manutenzione del Software	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione del software dei computers

Incaricato Tecnico Esterno della Manutenzione dell'Hardware	tutti i trattamenti informatici, rigorosamente nei limiti relativi alle funzioni	Manutenzione dell'hardware dei computers
Docente o animatore Esterno	i seguenti trattamenti non informatici: Tr.4 - Attività propedeutiche all' avvio dell'anno scolastico Tr.5 - Attività educativa, didattica e formativa, di valutazione, rigorosamente nei limiti relativi alle funzioni	Attività di animazione a favore degli alunni della scuola
Incaricato per la creazione e gestione del sito web	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti attività: Tr.11 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
Altro Incaricato Esterno		
RESPONSABILI ESTERNI:		
RESPONSABILE ESTERNO DEL TRATTAMENTO : organizzazione per la manutenzione del Software	Tutti i trattamenti informatici , ma rigorosamente nei limiti della funzione	Manutenzione del software
RESPONSABILE ESTERNO DEL TRATTAMENTO : organizzazione per la manutenzione dell'Hardware	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Manutenzione dell'hardware dei computers
RESPONSABILE ERNO DEL TTAMENTO : organizzazione di Docenti imatori Esterni	I seguenti trattamenti informatici e Tr.4 - Attività propedeutiche vvio dell'anno scolastico Tr.5 - Attività educativa, tica e formativa, di valutazione, osamente nei limiti relativi alle oni	Gestione di attività teatrali , sportive, di orto psicologico, musicali o di animazione in re degli alunni dell'Istituto
RESPONSABILE ERNO DEL TTAMENTO : organizzazione per la zione e gestione del sito web	i trattamenti informatici, osamente nei limiti relativi alle enti funzioni: Tr.11 Gestione sito web dell'istituto	Creazione e gestione del sito web Istituto
RESPONSABILE ERNO DEL TTAMENTO : organizzazione Agenzia	tutti i trattamenti informatici e rigorosamente nei limiti relativi alle funzioni:	Organizzazione di visite d'istruzione ggi

viaggi, Gestori di trasporti [SE GESTISCONO DATI ULTERIORI RISPETTO A QUELLI MERAMENTE IDENTIFICATIVI	tr.5 - attività educativa, didattica e formativa, di valutazione, ma limitatamente a pochissimi dati tr.1 – gestione del personale, in quanto accompagnatori, ma limitatamente a pochissimi dati	
RESPONSABILE ESTERNO DEL TRATTAMENTO : Ente di certificazione di qualità [se esistente)	tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni	Verifica delle condizioni che consentono l'ottenimento del marchio di qualità
Altro RESPONSABILE ESTERNO DEL TRATTAMENTO : organizzazione ….[se esistente]		
AMMINISTRATORI DI SISTEMA ED ASSIMILATI		
Amministratore del sistema informatico	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Gestione del sistema informatico dell'istituto

A tutti i Preposti destinati al trattamento di dati mediante strumento elettronico, sono state conferite credenziali di autenticazioni mediante parola chiave. Al fine di meglio precisare la suddetta ripartizione delle funzioni si rinvia alla tabella seguente:

ASSISTENTI AMMINISTRATIVI

Struttura deputata al trattamento	*Incaricato*	*Trattamenti operati dalla struttura*	*Compiti della struttura*
Segreteria DIDATTICA e Protocollo		**Trattamenti strumentali allo svolgimento dei compiti istituzionali:** gestione della corrispondenza ricevuta ed inviata dal Dirigente dell'Istituzione Scolastica; tenuta del protocollo generale con conseguente registrazione della posta e delle comunicazioni di ufficio in entrata e in uscita	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel tratt amento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

Servizi inerenti l'offerta formativa Servizi strumentali agli organi collegiali Servizi inerenti la gestione amministrativa		**Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa:** raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'Istituzione Scolastica **Trattamenti strumentali alle attività degli organi collegiali ed attività connesse ai rapporti con organi pubblici:** composizione degli organi collegiali rappresentativi della comunità servita dall'offerta formativa, convocazione degli organi, raccolta delle delibere, raccolta degli atti concertati con altre istituzioni pubbliche. **Gestione Amministrativa:** Uscite didattiche	
Segreteria AMMINISTRATIVA e protocollo Gestione del personale		**Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di selezione ed amministrazione del personale:** registrazione delle presenza presso l'Istituzione Scolastica, assenze per malattia, esigenze familiari, espletamento funzioni politiche o sindacali etc.; aspetti economici e previdenziali: paghe	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base

Servizi amministrativi		contributi, etc.; raccolta di curricula riguardo a soggetti interessati all'espletamento di funzioni docenti **Trattamenti strumentali allo svolgimento dei compiti di gestione amministrativa**: tenuta dei dati connessi all'espletamento di procedimenti amministrativi, attività contrattuale, procedure di bilancio	dati (salvataggi, ripristini, ecc.)

Servizi inerenti l'ampliamento dell'offerta formativa Servizi inerenti la gestione amministrativa		**Trattamenti strumentali alla predisposizione e concreta erogazione dell'attività di ampliamento dell'offerta formativa:** documentazione concernente opzioni per insegnamenti facoltativi, contratti **Gestione Amministrativa:** Gestione dei beni Procedure di acquisto	
PROTOCOLLO ARCHIVIO		**Trattamenti strumentali allo svolgimento dei compiti istituzionali:** gestione della corrispondenza ricevuta ed inviata dal Dirigente dell'Istituzione Scolastica; tenuta del protocollo generale con conseguente registrazione della posta e delle comunicazioni di ufficio in entrata e in uscita	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

COLLABORATORI SCOLASTICI
I Collaboratori Scolastici, nei loro specifici incarichi o nelle loro mansioni generali previsti dal C.C.N.L. e dalla Contrattazione di Istituto nell'area specifica di appartenenza (accoglienza e sorveglianza nei confronti degli alunni, ausilio materiale nei confronti degli alunni in situazione di difficoltà, custodia e sorveglianza nei locali scolastici, vigilanza nei confronti del pubblico evitando ed inibendo l'intrusione di persone estranee, collaborazione con i docenti e con il personale di segreteria, pulizia dei locali), osserveranno la massima privacy, evitando di diffondere notizie che devono restare private, in particolare quando ricevono, per essere distribuite, circolari interne e comunicazioni in visione al personale docente.

DOCENTI
I docenti a tempo indeterminato o determinato e tutte le altre unità di personale che a qualunque titolo hanno rapporto di lavoro anche occasionale (stipule di contratti o convenzioni) con l'Istituzione Scolastica eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio. Il docente, per la sfera di competenza, rientra nell'ambito dei soggetti indicati dall'art. 29 del Regolamento UE 2016/679 che agiscono, nell'ambito del trattamento dei dati personali, sotto la diretta autorità del Titolare del trattamento sia per le categorie di dati cui può accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art. 4 del Codice, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.
I dati trattati dai docenti si rinvengono nei registri dei verbali degli OO.CC., nel registro elettronico, nelle diagnosi funzionali per la situazione di handicap, in eventuali certificati medici, etc. Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge.

SITO WEB, ALBO ON LINE
Il personale docente e gli alunni che si occupano del sito web della scuola e il personale amministrativo che si occupa dell'albo on line eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio. Entrambe le figure rientrano nell'ambito dei soggetti indicati dall'art. 29 del Regolamento UE 2016/679 che agiscono, nell'ambito del trattamento dei dati personali, sotto la diretta autorità del Titolare del trattamento sia per le categorie di dati cui possono accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art.4 del Codice, sia per le istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.
Tale personale riceverà specifica informazione/formazione da parte del Titolare del trattamento circa gli specifici doveri e gli adempimenti cui sono tenuti in ragione del loro ufficio, della riservatezza che si deve ai dati che trattano per il fatto di essere dipendenti di questa pubblica Istituzione Scolastica. Ad essi sarà consegnato una copia della normativa che riguarda la sicurezza del trattamento dei dati in vigore al momento della nomina. Tale nomina è a tempo indeterminato, decade per revoca, o con il venir meno dei compiti che giustificavano il trattamento

4. ANALISI DEI RISCHI INCOMBENTI SUI DATI

L'Istituzione Scolastica ha proceduto ad una ricognizione dei rischi che potrebbero comportare la distruzione, sottrazione, perdita, trattamento abusivo dei dati di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati.
Le fonti di rischio sono state accorpate in:

1) Comportamenti degli operatori
Sottrazione di credenziali di autenticazione; comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati; comportamenti dolosi dei soggetti legittimati; errori materiali.

2) Eventi relativi agli strumenti
Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software e firewall), spamming o tecniche di sabotaggio. Malfunzionamento, indisponibilità o usura fisica degli strumenti. Accessi abusivi negli strumenti elettronici. Intercettazione dei dati in occasione di trasmissione in rete.
3) Eventi relativi al contesto fisico-ambientale.
Distruzione o perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, seppur astrattamente preventivabili (incendi o allagamenti) di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele. Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica per lunghi periodi di tempo, in grado di pregiudicare la climatizzazione dei locali. Furto o danneggiamento degli strumenti elettronici di trattamento dei dati, in orario diverso da quello di lavoro. Accesso non autorizzato da parte di terzi – interni o esterni all'istituzione scolastica – mediante uso abusivo di credenziali di autenticazione, in funzione di danneggiamento o sottrazione dei dati. Errori umani nell'attivazione degli strumenti di protezione.
I suddetti rischi sono **stati ripartiti in classi di gravità, tenendo conto** della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:

A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Analisi dei rischi

EVENTO	**IMPATTO SULLA SICUREZZA DEI DATI**			**RIF. MISURE DI AZIONE**
	DESCRIZIONE		**GRAVITA' STIMATA**	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;	EE	Adozione di idonei dispositivi di protezione: software - firewall
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di	EE	Adozione di idonei dispositivi di protezione: software - firewall

		elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi		
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Adozione di idonei dispositivi di protezione: password
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	MA	Adozione di idonei dispositivi di protezione: firewall
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori;	MB	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di

		accesso altrui non autorizzato		memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	M	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Guasto ai sistemi complementari (impianto elettrico, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	A	Attività di controllo, assistenza e manutenzione periodica backup periodici gruppo di continuità posizionamento personal computer
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione

5. PROTEZIONE DELLE AREE E DEI LOCALI

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, sono state adottate le seguenti misure:

- le aree contenenti dati in supporto cartaceo (mobili ed armadi contenenti documenti) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso a persone non autorizzate;
- l'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale;
- il personale amministrativo, incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali;
- l'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici;
- installazione di antivirus sul server e sui pc client al fine di impedire ingressi di pirati o intercettazioni sulla rete informatica di questa istituzione scolastica con la configurazione di

password e impostazione di tutte le misure di sicurezza necessarie.
L'Istituzione Scolastica è dotata di impianto elettrico a norma e di appositi estintori.

6. TRATTAMENTI SENZA L´AUSILIO DI STRUMENTI ELETTRONICI

Relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nei seguenti:

- qualsiasi documento presentato alla scuola va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che l'istituzione scolastica consegni agli utenti va inserito, quando riservato o contenente documentazione sensibile, in apposite buste o cartelline non trasparenti.
- Le eventuali rubriche telefoniche in utilizzo su supporto cartaceo sono richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato (praticamente il primo foglio funge da copertina).
- Tutti i documenti cartacei sono custoditi in idonei armadi chiusi a chiave e posti in locali vigilati

7. TRATTAMENTI CON STRUMENTI ELETTRONICI

In primo luogo occorre osservare che i computer risultano tutti sollevati da terra, in modo da evitare eventuali danneggiamenti e perdite di dati dovute ad allagamenti.
In secondo luogo si evidenzia che il server è collegato a un gruppo di continuità che consente di prevenire la perdita di dati derivanti da sbalzi di tensione o da interruzione di corrente elettrica. Non appena si dovesse verificare la mancanza di energia elettrica si raccomanda di procedere alla rapida chiusura di qualunque sessione in corso, al salvataggio dei dati sul disco rigido e all'avvio della procedura di spegnimento del server.
Ulteriori garanzie sulla protezione delle basi dati sul server sono offerte dalla presenza di dischi rigidi che permetteno il recupero dei dati anche in presenza di un guasto su uno dei dischi. Nel caso in cui dovesse intervenire il guasto di uno dei dischi del server il responsabile del trattamento dovrà dare immediata comunicazione del fatto all'Amministratore del sistema informatico della rete di segreteria che dovrà procedere all'immediata duplicazione degli archivi del disco e alle operazioni necessarie al ripristino o alla sostituzione del disco difettoso.
Gli incaricati del trattamento hanno ricevuto adeguate istruzioni in merito al trattamento dei dati con lo strumento informatico anche in relazione ai possibili rischi alla integrità ed alla riservatezza dei dati trattati

8. SISTEMA DI AUTENTICAZIONE ED AUTORIZZAZIONE

Il trattamento di dati personali con strumenti informatici è limitato al personale **incaricato al trattamento** dotato di un codice per l'identificazione dell'incaricato associato ad una parola chiave riservata conosciuta solo dal medesimo.

Per quanto riguarda il **sistema di autorizzazione**, a ciascun **incaricato del trattamento** nominato dal DSGA sono dati i poteri di inserimento, accesso, modifica e cancellazione sui dati relativi a tutte le aree indipendentemente dalla struttura organizzativa cui sono assegnati. Tale scelta si è resa necessaria per garantire la continuità dell'attività amministrativa della segreteria consentendo la sostituzione del personale assente. Eventuali limitazioni all'accesso a determinati dati verranno all'occorrenza determinate modificando i permessi relativi alle password assegnate a ciascun incaricato.

Le credenziali di accesso rilasciate al personale docente permettono l'accesso all'applicazione registro elettronico e dei servizi di segreteria digitale eventualmente attivati ma non ai dati trattati dal personale amministrativo per lo svolgimento della propria attività.

9. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DELTRATTAMENTO E FORMAZIONE DEL PERSONALE

Al Titolare spetta il compito di provvedere all'opportuna formazione di tutti i soggetti designati al trattamento dei dati al fine di:

- garantire il massimo rispetto delle procedure elencate nel presente Documento;
- rendere edotto il personale sui rischi che incombono sui dati e le modalità su come prevenire i danni;
- informare il personale sulle responsabilità che ne derivano.

Il Titolare valuterà opportunamente il livello di preparazione dei singoli addetti in merito alle procedure (informatiche e non) utilizzate per il trattamento e la custodia dei dati; eventuali lacune saranno colmate con appositi interventi formativi volti a rendere i soggetti interessati idonei a svolgere gli incarichi loro assegnati.

10. PROGRAMMA DI REVISIONE ED ADEGUAMENTO

Il presente documento costituisce una prima versione del registro dei trattamenti redatta in occasione della piena operatività del Regolamento UE 2016/679 intervenuta il 25/05/2016 cui seguiranno aggiornamenti a seguito di integrazioni o modifiche nel rispetto delle indicazioni fornite dal Garante per l'area istruzione.

Il Dirigente Scolastico
Dott.ssa Maria Teresa D'Orso

(firma autografa sostituita a mezzo stampa

ai sensi dell'art. 3 c.2 del D.Lgs 39/93)

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

PROCEDURA PER DATA BREACH

Definizioni

La presente procedura è adottata dall'Istituto con sede legale in Anzio**.**
Il Titolare del trattamento ha nominato un Responsabile del trattamento (DPO), individuato nella Società Euservice srl via Dante Alighieri, 12 - 00027 Roviano (RM) - P.IVA 08879271008 nella persona dell'Ing. Angelo Leone

Ai fini della presente procedura, valgono le seguenti definizioni:

a) Titolare del trattamento: "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri".

b) Responsabile del trattamento: "La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento ai sensi dell'art. 28 GDPR".

c) Incaricato del trattamento: "La persona fisica che nell'ambito della struttura aziendale del Titolare è autorizzata a effettuare attività di trattamento di dati personali".

d) DPO: "Il Responsabile del trattamento come individuato dalla Sezione 4 (artt. 37-39) del Regolamento (UE) n. 2016/679".

e) Dato personale: "Qualunque informazione relativa a persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, generica, psichica, economica, culturale o sociale".

f) Trattamento: "qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica,

l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".

La gestione dei data breach

Ai sensi dell'art. 33 del Regolamento (UE) n. 2016/679, il Titolare del trattamento, in caso sia consapevole di una violazione dei Dati personali trattati, è tenuto: (i) a informare l'Autorità di controllo (il Garante per la protezione dei dati personali, nel caso del territorio italiano) entro e non oltre le 72 ore - preferibile il rispetto del termine delle 48 ore indicato nel Provvedimento del Garante del 2 luglio 2015 allegato - successive all'avvenuta conoscenza della violazione. Si precisa che il Titolare non è tenuto alla notifica se sia improbabile che la violazione dei Dati personali presenti un rischio per i diritti e le libertà degli Interessati - e, (ii) nel caso in cui tale violazione sia suscettibile di comportare un rischio elevato per i diritti e le libertà degli interessati, a informare senza ritardo anche gli stessi Interessati.

A tal fine, il Titolare del trattamento, come sopra identificato, ha previsto un apposito processo per la gestione e la notifica in caso di Data Breach.

Al fine di rendere effettivo il processo di notifica, è altresì importante che tutti coloro che nell'ambito del rapporto di lavoro e/o di collaborazione trattano Dati personali del Titolare del trattamento siano previamente sensibilizzati e partecipino attivamente a tale processo, segnalando tempestivamente ogni caso di violazione di cui siano venuti a conoscenza e ogni evento che potrebbe potenzialmente condurre ad una violazione.

Data Breach e potenziali scenari

Il GDPR definisce violazione dei dati personali o Data Breach "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati*" (art. 4, n. 12). Le indicazioni di cui alla presente sezione della Procedura valgono per qualsiasi tipologia di Dato personale.

Eventi di Data Breach possono riguardare sia casi cui è connesso un rischio marginale (es. perdita di una chiavetta USB di un dipendente), che casi più critici di furto o perdita di intere basi dati, quali, a titolo esemplificativo, le banche dati gestite dal Titolare del trattamento.

Nel caso si verificasse una delle casistiche riportate di seguito, o un analogo scenario, è fondamentale chiedersi se e quale tipo di Dati personali sono coinvolti nell'evento, e, di conseguenza, procedere alla segnalazione:

- ✓ furto o smarrimento di laptop, smartphone, tablet aziendali contenenti Dati personali;
- ✓ furto o smarrimento di documenti cartacei contenenti Dati personali;
- ✓ furto o smarrimento di dispositivi portatili di archiviazione non criptati, come chiavette USB e hard disk esterni, contenenti Dati personali;
- ✓ perdita o modifica irreparabile di archivi contenenti Dati personali in formato cartaceo o digitale (ad esempio, a causa di una errata cancellazione o modifica dai sistemi o dagli archivi digitali aziendali che non possa essere ripristinata attraverso l'uso di un backup);
- ✓ diffusione impropria di Dati personali, per mezzo di:
  - o invio di e-mail contenente Dati personali al destinatario errato;
  - o invio di e-mail con un file contenente Dati personali allegato erroneamente;
  - o esportazione fraudolenta o errata di Dati personali dai sistemi aziendali;

- ✓ richiesta di invio di documenti e file contenenti Dati personali da parte di un esterno che si finge fraudolentemente un collega, collaboratore e/o altro soggetto e conseguente invio allo stesso di tali documenti e file;
- ✓ segnalazione da parte di un fornitore di un evento di Data Breach sui propri sistemi che ha interessato o potrebbe potenzialmente interessare Dati personali del Titolare deltrattamento.

1. Processo di gestione del Data Breach

Al fine di consentire una gestione efficace e tempestiva delle violazioni dei Dati personali, il Titolare del trattamento adotta un processo strutturato per la gestione dei casi di Data Breach che prevede:

- ✓ Rilevazione e segnalazione del Data Breach;
- ✓ Analisi del Data Breach;
- ✓ Risposta e notifica del Data Breach;
- ✓ Registrazione del Data Breach.

2. Rilevazione e segnalazione del Data Breach

La rilevazione e segnalazione del Data Breach è un obbligo per tutti i dipendenti e/o collaboratori del Titolare del trattamento.

Nel caso in cui si verifichi uno degli eventi sopradescritti descritti o in tutti gli altri casi in cui il soggetto che tratta dati personali sia consapevole di altri eventi potenzialmente rischiosi per i documenti e gli archivi, è tenuto a informare immediatamente il Dirigente Scolastico il quale provvede – senza indugio – a darne notizia al responsabile per la protezione dei dati personali (DPO).

Nel caso di un incidente informatico, dovrà essere compilata scheda su apposito registro informatico la cui struttura è allegata al presente atto (ALLEGATO 1). Al registro andranno allegate tutte le comunicazioni relative all'incidente (ad es. denuncia all'autorità giudiziaria, notifica al Garante Privacy e relativa corrispondenza, comunicazioni agli interessati, ecc.).

In tale Registro dovranno essere inseriti tutti gli eventi che determinano o configurano anomalie rispetto alla normale gestione dei sistemi informatici (ad esempio: Virus, perdita di dati, alterazione di dati, attacchi alla rete, furti di credenziali, ecc.).

3. Analisi del Data Breach

A seguito della rilevazione e/o segnalazione, il Dirigente Scolastico – sentito il Responsabile per la protezione dei dati personali - effettua una valutazione al fine di verificare che nell'incidente rilevato siano stati effettivamente violati Dati personali trattati dall'Istituto.

La suddetta analisi è finalizzata alla raccolta ed identificazione delle seguenti informazioni:

- ✓ categorie di Interessati cui i Dati personali violati si riferiscono (ad esempio, utenti, dipendenti, fornitori, etc.);
- ✓ categorie di Dati personali compromessi (ad esempio, Dati personali, Dati sensibili, Dati giudiziari);
- ✓ tipologia di Data Breach: violazione della riservatezza, disponibilità o integrità (ad esempio,

accesso non autorizzato, perdita, alterazione, furto, *disclosure*, distruzione, etc.).

Nell'ambito di tale analisi, il Titolare del trattamento – con il supporto del DPO - identifica le azioni di prima risposta da intraprendere nell'immediato per contenere gli impatti della violazione dei Dati personali.

Nell'ambito dell'analisi della violazione, vengono identificate anche le seguenti informazioni:

- ✓ identificabilità degli Interessati i cui dati rappresentano l'oggetto della violazione;
- ✓ misure di sicurezza tecniche e organizzative che potrebbero aver parzialmente o *in toto* mitigato gli impatti relativi al Data Breach;
- ✓ ritardi nella rilevazione del Data Breach;
- ✓ numero di individui interessati.

Sulla base dei suddetti parametri, il Titolare del trattamento competente procede alla valutazione della gravità del Data Breach relativamente ai diritti ed alle libertà degli Interessati, a seconda della natura dei Dati personali (ad esempio, Dati Sensibili e/o Giudiziari), delle misure di sicurezza adottate, della tipologia di interessati (ad esempio, minori o altri soggetti vulnerabili).

4. Risposta e notifica del Data Breach

La precedente fase di analisi fornisce al Titolare del trattamento gli strumenti necessari a identificare e valutare le conseguenze negative e gli impatti causati dalla violazione di Dati personali rilevata.

Nel caso in cui dovesse risultare improbabile che il Data Breach presenti rischi per i diritti e le libertà degli interessati, la notifica all'Autorità Garante risulta essere non obbligatoria. Tale valutazione è condivisa con il DPO.

Qualora al contrario dovesse risultare possibile che il Data Breach presenti rischi per i diritti e le libertà degli Interessati, il Dirigente Scolastico, con il supporto del DPO, procedere a predisporre la notifica all'Autorità Garante secondo il modello allegato al presente atto (ALLEGATO 2).

La notifica viene effettuata all'Autorità Garante entro 72 ore dal momento in cui il Data Breach è stato rilevato.

La suddetta notifica contiene almeno le seguenti informazioni:

- ✓ natura della violazione dei dati personali (*disclosure*, perdita, alterazione, accesso non autorizzato, etc.);
- ✓ tipologie di Dati personali violati;
- ✓ categorie e numero approssimativo di Interessati cui i dati compromessi si riferiscono;
- ✓ nome e dati di contatto del DPO, che sarà l'interfaccia per Titolare del trattamento nei confronti dell'Autorità di controllo;
- ✓ probabili conseguenze della violazione dei Dati personali;
- ✓ descrizione delle misure che il Titolare del trattamento ha adottato o è in procinto di adottare al fine di mitigare le conseguenze del Data Breach;
- ✓ ove la stessa non sia presentata entro 48/72 ore dalla rilevazione, i motivi dell'eventuale ritardo nella comunicazione.

Qualora non sia stato possibile fornire contestualmente tutte le informazioni obbligatorie, il Dirigente Scolastico raccoglie quanto prima le informazioni supplementari e provvede a integrare, senza ritardo, la notifica già inoltrata all'Autorità di Controllo.

Oltre a notificare il Data Breach all'Autorità Garante, il Titolare del trattamento è tenuto a valutare l'esigenza di procedere con la denuncia all'Autorità Giudiziaria competente, nonché con la notifica del Data Breach anche ai soggetti interessati i cui dati siano stati violati.

Per stabilire se sia necessario provvedere alla notifica agli Interessati, il Titolare del trattamento, di concerto con il DPO, deve valutare i seguenti fattori:

- ✓ il trattamento può comportare discriminazioni, furto d'identità, perdite finanziare, disturbi psicologici, pregiudizio alla reputazione, perdita di riservatezza dei Dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo;
- ✓ gli Interessati rischiano di essere privati dei loro diritti, delle libertà o venga loro impedito l'esercizio del controllo sui Dati personali che li riguardano;
- ✓ sono trattati Dati personali che rivelano l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi a condanne penali e a reati o alle relative misure di sicurezza;
- ✓ in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;
- ✓ sono trattati Dati personali di persone fisiche vulnerabili, in particolare minori;
- ✓ il trattamento riguarda una notevole quantità di Dati personali e un vasto numero di Interessati.

La notifica agli Interessati deve, pertanto, avvenire nel caso in cui la violazione di Dati personali presenti un rischio elevato per i diritti e le libertà delle persone fisiche, a meno che non sia verificata almeno una delle seguenti condizioni:

- ✓ sono state applicate adeguate misure tecniche e organizzative per proteggere i dati prima della violazione, in particolare quelle in grado di renderle non intelligibili per soggetti terzi non autorizzati (ad esempio, misure di cifratura);
- ✓ a valle della rilevazione del Data Breach, sono state adottate misure per impedire il concretizzarsi dei rischi per i diritti e le libertà degli Interessati;
- ✓ la notifica del Data Breach a tutti gli Interessati singolarmente comporta uno sforzo sproporzionato rispetto al rischio. In tal caso occorrerà comunque procedere a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati siano comunque informati con analoga efficacia.

Il Dirigente Scolastico, di concerto con il DPO, valuta di volta in volta, sulla base della tipologia e del numero di Interessati, il canale di comunicazione che appare più opportuno per trasmettere la notifica agli stessi.
In ogni caso la notifica agli Interessati deve contenere quanto meno:

- ✓ nome e dati di contatto del DPO;
- ✓ descrizione delle probabili conseguenze della violazione;

- ✓ descrizione delle misure adottate o che l'Istituto intende adottare per porre rimedio alla violazione e ridurre gli effetti negativi.

5. Data Breach relativo a dati personali trattati in qualità di Responsabile del trattamento

Qualora, a seguito di una segnalazione o nel corso dell'analisi preliminare di cui al precedente paragrafo 4, il Dirigente Scolastico rilevasse che la violazione qualificabile come Data Breach riguarda dati personali di titolarità di un soggetto terzo trattati dall'istituto in qualità di Responsabile del trattamento, procedono a informare senza ingiustificato ritardo il soggetto terzo titolare del trattamento.

Nel dettaglio, la comunicazione al soggetto titolare del trattamento dovrà contenere quanto meno le seguenti informazioni (oltre a quelle eventualmente richieste dallo stesso soggetto terzo titolare del trattamento):

- ✓ Descrizione della natura della violazione dei dati personali comprensiva, ove possibile, di informazioni in merito alle categorie e al numero di Interessati nonché alle categorie e al volume approssimativo di dati personali oggetto di violazione;
- ✓ Nome e dati di contatto del DPO;
- ✓ Descrizione delle possibili conseguenze della violazione;
- ✓ Descrizione di eventuali misure già adottate o di cui si prevede l'adozione per porre rimedio alla violazione di dati personali e per attenuarne i possibili effetti negativi.

La comunicazione, nel testo convalidato dal DPO, sarà inviata al soggetto titolare del trattamento entro 48 ore dall'avvenuta rilevazione della violazione o nel minore termine eventualmente indicato dal soggetto titolare del trattamento.

6. Prescrizioni per la prevenzione di Data Breach

L'Istituto adotta specifiche strategie per prevenire o minimizzare il verificarsi di Data Breach.

In primo luogo, occorre che tutti gli Incaricati del Trattamento siano consapevoli dei Dati personali che trattano attraverso i propri strumenti (anche cartacei) e dispositivi o a cui hanno accesso tramite i sistemi del Titolare del trattamento. A tal fine, la presente procedura viene loro comunicata dal Titolare del trattamento essi dovranno custodire tali Dati personali ed i relativi documenti con cura e in modo responsabile sia all'interno che all'esterno della propria area di lavoro. Si precisa che i soggetti in questione sono già stati istruiti per mezzo di nomina ad Incaricati del trattamento e devono attenersi alle prescrizioni approvate con il Disciplinare.

ALL 1

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO ANZIO III
Via Machiavelli s.n.c. tel.06/9873212 - Fax 06/9873540 – rmic8c700e@istruzione.it
00040 Lavinio di ANZIO - ROMA
C.M. RMIC8C700E C.F. 90000150582

REGISTRO INCIDENTI INFORMATICI

Numero Incidente	**20---/0001**

A. Rilevazione dell'incidente

A1 Data e ora dell'incidente	
A2 Chi ha rilevato per primo l'incidente? Nominativo e riferimenti	
A3 Data e ora di avvio della gestione dell'incidente	
A4 Note e/o breve descrizione dell'incidente	

B. Descrizione dell'incidente

B1 Origine dell'incidente (interna o esterna). Dettagliare bene l'origine	
B2 Sistemi/Applicazioni interessati dall'incidente	
B3 Causa dell'incidente (se più cause indicare la prevalente)	

B4 Stato attuale (situazione diagnosticata)	
B5 Tempi previsti per la soluzione	
B6 Note	

C. Caratterizzazione dell'incidente

C1 Tipo Incidente (virus, attacco, alterazione dati, guasto apparati, sottrazione informazioni, blocchi, malfunzionamenti, ecc.)	
C2 Sistemi colpiti e/o applicazioni colpite	
C3 Funzioni aziendali colpite	
C4 L'entità dell'incidente è tale da farlo rientrare nell'attenzione GDPR? SI/NO	
C5 Numero Clienti/Utenti oppure Numero Dipendenti colpiti dall'incidente (perdita e/o alterazione dati), ecc..	
C6 Tipologia di dati coinvolti	
C7 Tipologia di soggetti coinvolti	
C8 Note	

D. Risoluzione dell'incidente

D1 Misure tampone intraprese nell'immediato	
D2 Ulteriori misure pianificate per la chiusura dell'incidente o poste in essere per evitare il ripetersi dell'incidente	
D3 Sono state allertate le strutture deputate ad attivare le eventuali comunicazioni GDPR? SI/NO	
D4 Se SI, quando? (Data e Ora)	
D5. Se NO, spiegare le motivazioni di mancata comunicazione	
D6 Chiusura incidente (Data e Ora)	

D7Note	

ALL 2

COMUNICAZIONE DI DATA BREACH AL GARANTE PRIVACY

1. Titolare del trattamento

Ragione sociale/Nome e Cognome: _____
C.F./P.IVA: _____
Stato: _____
CAP:_____Città:_____Provincia:_____
Telefono: _____
Email:_____
PEC: _____

2. Responsabile della protezione dei dati (o nel caso in cui non sia presente il RPD, i riferimenti di un altro soggetto presso cui ottenere più informazioni)

Denominazione:_____
Telefono:_____
Cellulare:_____
Email:_____
PEC: _____

3. Quando si è verificata la violazione di dati personali?

- □ Il _____
- □ Tra il_____e il _____
- □ In un tempo non ancora determinato
- □ È possibile che sia ancora in corso

4. Dove è avvenuta la violazione dei dati? (Specificare se sia avvenuta a seguito di smarrimento di dispositivi o di supporti portatili)

5. Modalità di esposizione al rischio

Tipo di violazione

- □ Lettura (presumibilmente i dati non sono stati copiati);
- □ Copia (i dati sono ancora presenti sul sistema del titolare);
- □ Alterazione (i dati sono presenti sui sistemi ma sono stati alterati);
- □ Cancellazione (i dati non sono più sui sistemi del titolare e non li ha neppure l'autore della violazione);
- □ Furto (i dati non sono più sui sistemi del titolare e li ha l'autore della violazione);
- □ Altro (specificare).

6. Dispositivo oggetto della violazione

- ☐ Computer;
- ☐ Rete;
- ☐ Dispositivo mobile;
- ☐ File o parte di un file;
- ☐ Strumento di backup;
- ☐ Documento cartaceo;
- ☐ Altro (specificare).

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione

8. Quali sono le possibili conseguenze derivanti dalla violazione?

9. Indicare le categorie di interessati colpiti dalla violazione

10. Quante persone sono state colpite dalla violazione dei dati personali?

- ☐ n._____persone;
- ☐ circa_____persone;
- ☐ un numero ancora sconosciuto di persone.

11. Numerosità dei dati di cui si presume la violazione

_____

12. Che tipo di dati sono oggetto di violazione?

- ☐ Dati anagrafici;
- ☐ Indirizzo di posta elettronica;
- ☐ Numero di telefono;
- ☐ Dati di accesso e di identificazione (user name, password, customer ID, altro);

- ☐ Dati relativi a minori;
- ☐ Dati particolari di cui all'art. 9 Reg. UE 2016/679;
- ☐ Dati giudiziari;
- ☐ Copia per immagine su supporto informatico di documenti analogici;
- ☐ Ancora sconosciuto;
- ☐ Altro (specificare).

13. Livello di gravità della violazione dei dati personali (secondo la valutazione del titolare)

- ☐ Basso/trascurabile;
- ☐ Medio;
- ☐ Alto;
- ☐ Molto alto.

14. Misure tecniche e organizzative applicate ai dati oggetto di violazione

15. La violazione è stata comunicata anche agli interessati?

- ☐ Si, è stata comunicata in data_____;
- ☐ No, perché_____.

16. Qual è il contenuto della comunicazione resa agli interessati?

17. Quale canale è stato utilizzato per la comunicazione agli interessati?

18. La violazione coinvolge interessati che si trovano in altri Paesi UE?

- ☐ Si;
- ☐ No.

19. La comunicazione è stata effettuata alla competenti autorità di altri Paesi UE?

- ☐ Si (specificare quali);
- ☐ No.

20. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione di dati e prevenire simili violazioni future?

IL TITOLARE
(da firmare digitalmente)