



FONDI
STRUTTURALI
EUROPEI

pon
2014-2020



PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)



I.C. 3 "Karol Wojtyła"

via Salvemini - 80022 Arzano - Napoli -

☎ 0817311069/0815736043 Fax: 08119562349

✉ NAIC8FS008@istruzione.it - 🌐 www.ic3karolwojtyla.gov.it



UNI-EN-ISO 9004:2009

ISTITUTO COMPRENSIVO - "3 - KAROL WOJTYLA"-ARZANO
Prot. 0004775 del 11/12/2019
01-01 (Uscita)

Regolamento per l'attuazione del Reg. UE 2016/679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali

Sistema per la Gestione della Sicurezza delle Informazioni

Approvato dal Consiglio d'Istituto del 19/12/2018 con delibera n. 20

REDAZIONE		VERIFICA	APPROVAZIONE
DSGA		RDP	Titolare Trattamento
FIRMA		FIRMA	FIRMA
REV.	MOTIVO REVISIONE	DATA	
00	Prima emissione	02/01/2019	



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Indice

SEZIONE 1 – PARTE GENERALE	4
Art. 1 - Premessa.....	4
Art. 2 - Obiettivo del presente Regolamento	5
Art. 3 - Liceità dei trattamenti.....	6
Art. 4 - Titolare del trattamento.....	6
Art. 5 - Finalità del trattamento	8
Art.6 - Responsabile del trattamento	8
Art.7 - Responsabile della protezione dati.....	11
Art. 8 – Persona autorizzata al trattamento dei dati	13
Art.9 - Registro delle attività di trattamento.....	14
Art. 10 - Informativa agli interessati	15
Art.11 - Consenso al trattamento dei dati.....	15
Art. 12 - Non applicabilità del requisito della portabilità dei dati	16
Art. 13 - Tempi di conservazione dei dati e regole di scarto	16
SEZIONE 2 – SICUREZZA.....	17
Art.14 - Sicurezza del trattamento.....	17
Art.15 - Valutazioni d'impatto sulla protezione dei dati	18
Art. 16 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati.....	22
Art. 17 - Registro delle violazioni dei dati.....	24
Art. 18 - Il modello RMS – Report Monitoraggio della Sicurezza.....	24
Art. 19 - Il RGS – Riesame Gestione della Sicurezza	25
Art. 20 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati	25



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 21 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR
..... 26

Art. 22 - Verifiche e certificazioni periodiche da parte del Responsabile della protezione dei dati
..... 26

Art. 23 - Gestione della sicurezza secondo codici di comportamento o meccanismi di
certificazione 27



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

SEZIONE 1 – PARTE GENERALE

Art. 1 - Premessa

Il 24 Maggio 2016 è entrato ufficialmente in vigore, divenuto operativo dal 25 maggio 2018, il Regolamento Europeo per la Protezione dei Dati n. 2016/679 - anche noto come GDPR (General Data Protection Regulation) - che abroga la Direttiva 95/46/CE sulla protezione dei dati personali ed affianca la normativa nazionale in materia privacy contenuta nel D.lgs. 196/2003 (Codice privacy).

Successivamente è stato pubblicato nella Gazzetta Ufficiale n.205 del 4 settembre 2018 il Decreto legislativo 10 agosto 2018 n.101 *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, che adegua il D.Lgs. 196/03.

Il Decreto, infatti, entrato in vigore il 19 settembre 2018, dispone l'esecuzione nell'ordinamento italiano del Regolamento (UE) 2016/679 attraverso totali modifiche e abrogazioni inerenti il Codice in materia di protezione dei dati personali Decreto legislativo 30 giugno 2003, n. 196.

Con l'adozione del nuovo Regolamento privacy e del successivo Decreto legislativo 10 agosto 2018 n.101 si è inteso creare un quadro giuridico armonizzato e garantire un'applicazione uniforme delle regole in materia di trattamento dati su tutto il territorio dell'Unione Europea, al fine di sviluppare il mercato unico europeo e rafforzare la protezione dei diritti degli interessati.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 2 - Obiettivo del presente Regolamento

Il presente regolamento ha come obiettivo quello di individuare con precisione le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali, nell'ambito specifico dell'Istituto, si raggiunge e si mantiene nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR e si imposta un SGSI - Sistema per la Gestione della Sicurezza delle Informazioni affinché si possa dimostrare, in caso di controlli o ispezioni da parte degli organismi preposti, che l'Istituto è in regola con le prescrizioni del succitato Regolamento UE 2016/679.

L'adozione del presente regolamento permette di raggiungere i seguenti obiettivi:

- implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in base al quale il titolare deve non solo essere conforme alle prescrizioni del GDPR, ma deve anche essere in grado di dimostrare la conformità raggiunta;
- indicare metodologie e prassi operative specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico dell'Istituto;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati
- impostare un SGSI - Sistema di Gestione della Sicurezza delle Informazioni che permetta di dimostrare che l'Istituto è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR e conforme a riconosciuti standard di sicurezza a livello internazionale.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 3 - Liceità dei trattamenti

Per ciascun trattamento effettuato, deve essere verificata e documentata per iscritto la liceità del trattamento stesso; nel caso di un soggetto pubblico come l'Istituto, la liceità del trattamento deve essere individuata nella base giuridica che giustifica/richiede il trattamento specifico.

La base giuridica può essere costituita da:

- funzioni istituzionali dell'Istituto, oppure
- norme di legge di rango primario.

Si dovrà inoltre verificare che non sussistano norme di legge che vietino esplicitamente il trattamento.

Art. 4 - Titolare del trattamento

1. L'Istituto Comprensivo 3 "Karol Wojtyła", rappresentato ai fini previsti dal GDPR dal Dirigente Scolastico, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare").

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 GDPR: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al GDPR.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 del GDPR, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura,



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

- a) le informazioni indicate dall'art. 13 GDPR, qualora i dati personali siano raccolti presso lo stesso interessato;
- b) le informazioni indicate dall'art. 14 GDPR, qualora i dati personali non sono stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, GDPR, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento, tenuto conto di quanto indicato dal successivo art. 9.

6. Il Titolare, inoltre, provvede a:

- a) designare i Responsabili del trattamento che sono preposti al trattamento dei dati, contenuti nelle banche dati esistenti, nelle articolazioni organizzative di loro competenza;
- b) nominare il Responsabile della protezione dei dati;
- c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Istituto, relativamente alle banche dati gestite da soggetti esterni all'Istituto, in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;
- d) predisporre l'elenco dei Responsabili del trattamento dell'Istituto, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata all'Istituto da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui all'art. 26 del GDPR. L'accordo definisce le responsabilità di



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del GDPR, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. L'Istituto favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del GDPR e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 5 - Finalità del trattamento

Questo Istituto Scolastico procederà al trattamento, secondo la definizione dei dati personali definiti come comuni (dati anagrafici, fiscali, ecc.), e di quei dati definiti sensibili per il corretto svolgimento delle attività didattiche.

In particolare tratta dati idonei a rivelare informazioni sullo stato di salute (certificati medici, infortunio, ecc.), sulle condizioni alimentari, sulle convinzioni religiose, nei limiti in cui il trattamento è necessario per ottemperare alle attività didattiche, organizzative e amministrative previste da questa scuola.

I soggetti cui sono riferiti i dati personali trattati consistono in: alunni, familiari degli alunni, clienti, fornitori, e tutti gli altri soggetti che per fini istituzionali hanno rapporti, in essere o futuri, con questa scuola.

Il trattamento riguarderà unicamente le finalità rientranti tra quelle istituzionali della scuola e per le quali sono raccolti solo i dati strettamente necessari per tutta la durata del rapporto scolastico, le esigenze contrattuali ed anche oltre, nei limiti necessari per l'espletamento di obblighi di legge e per finalità amministrative.

Art.6 - Responsabile del trattamento



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

1. Il DSGA (Direttore dei Servizi Generali ed Amministrativi) è nominato unico Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza.

Tuttavia in seno all'Istituto è possibile nominare Responsabile del trattamento, il Responsabile del Servizio Tecnico e ciascun Responsabile di plesso.

Secondo la tipologia di dati trattati e dei trattamenti effettuati, è possibile designare Responsabile esterno del trattamento dei dati il soggetto esterno all'Istituto coinvolto a vario titolo nelle varie operazioni di trattamento dei dati, come ad esempio ditte incaricate dei servizi di assistenza e manutenzione dei degli apparati hardware oppure delle piattaforme software, con particolare riferimento alle piattaforme in cloud (es. registro elettronico, protocollo informatico in cloud, etc.).

Tali designazioni sono effettuate mediante opportuna nomina che disciplina:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;
- il tipo di dati personali oggetto di trattamento e le categorie di interessati;
- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

2. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.
3. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, GDPR; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla Commissione europea.
4. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare e il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

5. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

6. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle attività di trattamento svolte per conto del Titolare;
- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;
- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;
- alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;
- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;
- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "data breach"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

rischi per i diritti e le libertà degli interessati.

Art.7 - Responsabile della protezione dati

1. Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato dal Titolare del Trattamento.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare e al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del GDPR e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento.

Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al GDPR;



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36 GDPR, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi.

L'assenza di conflitti d'interessi è strettamente connessa agli obblighi di indipendenza del RPD.

2. Il Titolare e il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni che abbiano per oggetto questioni inerenti la protezione dei dati personali;
- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;
- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;
- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo. In tal senso il RPD:

- a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare e al Responsabile del trattamento.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti.

5. La figura di RPD è incompatibile con chi determina le finalità o i mezzi del trattamento;

6. Il Titolare e il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte del Dirigente e/o Responsabili, anche considerando l'attuazione delle attività necessarie per la protezione dei dati;
- tempo sufficiente per l'espletamento dei compiti affidati al RPD;
- supporto adeguato in termini di infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero *(in relazione alle dimensioni organizzative dell'Istituto)*;
- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Istituto;
- accesso garantito ai settori funzionali dell'Istituto così da fornirgli supporto, informazioni e input essenziali.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per l'adempimento dei propri compiti.

Fermo restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare del trattamento/Dirigente Scolastico o al Responsabile del trattamento.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il GDPR e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art. 8 – Persona autorizzata al trattamento dei dati

Mentre il D.Lgs. 196/2003 prevedeva esplicitamente la figura dell'incaricato del trattamento dei



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

dati, il GDPR tratta la figura dell'incaricato in termini più generali, all'art. 29 – Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento, laddove specifica che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Nel caso dell'Istituto, per chiarezza si continuerà ad usare la dicitura "Persona autorizzata al trattamento dei dati", intendendo con tale locuzione i soggetti di cui all'art. 29 del GDPR.

Art.9 - Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti informazioni:

- a) il nome e i dati di contatto dell'Istituto, del Titolare del trattamento, del Responsabile del trattamento, del Contitolare del trattamento, dell'eventuale RPD designato;
- b) le finalità del trattamento;
- c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- d) le categorie di destinatari cui i dati personali sono stati o saranno comunicati;
- e) l'eventuale trasferimento di dati personali verso un paese terzo o una organizzazione internazionale;
- f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- g) il richiamo alle misure di sicurezza tecniche e organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato ai sensi del precedente art. 2, presso l'Istituto in forma telematica/cartacea;

3. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 10 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs.196/2003, l'informativa contenga le seguenti informazioni:

- i dati di contatto del responsabile della protezione dei dati
- la base giuridica del trattamento
- il tempo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo
- gli ulteriori diritti dell'interessato introdotti dal GDPR.

Art.11 - Consenso al trattamento dei dati

Il GDPR mantiene un principio chiave introdotto dall'art. 18 del D.Lgs. 196/2003, e cioè che i soggetti pubblici non devono richiedere il consenso dell'interessato. Pertanto, sia nei moduli cartacei sia nei form web, non si dovrà chiedere il consenso dell'interessato (mentre invece è necessario fornire l'informativa).

In via del tutto residuale, è consentito che l'Istituto possa chiedere il consenso dei genitori, laddove trattasi di servizi opzionali, di cui i genitori o tutori degli alunni potrebbero decidere di non usufruire; in tali casi tuttavia, il consenso ha, di fatto, la valenza di documentare e tenere traccia del fatto che la famiglia/il tutore ha deciso di usufruire del servizio. Tali casistiche residuali sono precisamente individuate e codificate, e si possono ricondurre alle tre seguenti fattispecie:

- decisione di avvalersi del servizio di ristorazione scolastica
- decisione di partecipare a gite scolastiche, e di conseguenza di aderire a forme di assicurazione
- decisione di avvalersi del servizio di trasporto scolastico, e di conseguenza di aderire a forme di assicurazione.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 12 - Non applicabilità del requisito della portabilità dei dati

L'art. 20 del GDPR prevede astrattamente il diritto, da parte dell'interessato, alla portabilità dei dati. Tuttavia l'Istituto non è tenuto a soddisfare le richieste di portabilità dei dati, in quanto:

- la portabilità dei dati non si applica ai dati in formato cartaceo
- la portabilità dei dati non si applica ai trattamenti che prescindono dal consenso.

Art. 13 - Tempi di conservazione dei dati e regole di scarto

Per quanto riguarda i tempi di conservazione dei dati e le relative regole di scarto, si applicano le prescrizioni emesse dall'articolazione regionale di riferimento della Soprintendenza Archivistica e/o quelle recepite a livello di Regolamento di Protocollo e di Manuale per la Gestione dei Flussi Documentali.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

SEZIONE 2 - SICUREZZA

Art.14 - Sicurezza del trattamento

1. L'istituto, nella persona del Dirigente scolastico e ciascun Responsabile del trattamento, mette in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche e organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono:

- la pseudonimizzazione;
- la minimizzazione;
- la cifratura dei dati personali;
- la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico;
- una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro);
- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al GDPR in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o a un meccanismo di certificazione approvato.
5. L'istituto, nella persona del Dirigente scolastico e ciascun Responsabile del trattamento, si obbliga ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per suo conto ed abbia accesso a dati personali.
6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale dell'Istituto, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
7. Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi.

Art.15 - Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 del GDPR, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.
2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'art. 35, pp. 4-6, del GDPR.
3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

fisiche. Fermo restando quanto indicato dall'art. 35, p. 3 del GDPR, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

- a) trattamenti valutativi o di scoring, compresa la profilazione e attività predittive, concernenti 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 dell'interessato;
- b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;
- c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;
- d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9 del GDPR;
- e) trattamenti di dati su larga scala, tenendo conto: del numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;
- f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- g) dati relativi ad interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Istituto, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;
- h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;
- i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale, condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA a un altro soggetto, interno o esterno all'Istituto.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi o l'Amministratore di Sistema, se nominati, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile della sicurezza dei sistemi informativi o l'Amministratore di Sistema, se nominati, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

- se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, GDPR;
- se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;
- se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

- se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

7. La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

gravità dei rischi o, in modo più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il GDPR, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

9. Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

10. La DPIA deve essere effettuata, con eventuale riesame delle valutazioni condotte, anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

Art. 16 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati

1. Per violazione dei dati personali (in seguito "data breach") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dall'Istituto.
2. Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Dirigente Scolastico e al



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare se vi sia stata effettivamente una violazione, la portata e le conseguenze, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

3. I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del GDPR, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;
- perdita del controllo dei dati personali;
- limitazione dei diritti, discriminazione;
- furto o usurpazione d'identità;
- perdite finanziarie, danno economico o sociale.
- decifratura non autorizzata della pseudonimizzazione;
- pregiudizio alla reputazione;
- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

4. Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati, conseguente alla violazione rilevata, è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;
- riguardare categorie particolari di dati personali;
- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);
- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);
- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

5. La notifica deve avere il contenuto minimo previsto dall'art. 33 del GDPR, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

6. Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del GDPR.

Art. 17 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati

Art. 18 - Il modello RMS - Report Monitoraggio della Sicurezza

La sicurezza può continuamente essere compromessa da una serie di eventi che possono accadere. Questi eventi devono pertanto essere tracciati ed essere oggetto di analisi periodica.

La tracciatura degli eventi si effettua compilando il Modello RMS - Report Monitoraggio della Sicurezza, con frequenza mensile; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 19 - Il RGS - Riesame Gestione della Sicurezza

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno quadrimestrale, all'interno di un documento denominato RGS - Riesame Gestione della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto all'attenzione del Dirigente Scolastico, del DSGA, del responsabile della sicurezza dei sistemi informativi o l'Amministratore di Sistema, se nominati. All'interno del RGS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel semestre di riferimento, come ad esempio:

- l'esternalizzazione di un nuovo trattamento di dati
- la predisposizione di una procedura operativa o di un regolamento ad- hoc
- la predisposizione di una lettera di nomina
- la predisposizione di una nuova informativa
- la predisposizione di comunicazioni ai dipendenti o agli interessati
- il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati
- l'analisi di una richiesta di accesso ai dati
- la revisione dei Registri dei trattamenti dei dati
- lo svolgimento di un DPIA - Data Protection Impact Assessment
- la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo

Art. 20 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Poiché l'art. 32 del GDPR lascia un ampio margine di discrezione sulle prassi da mettere in atto per assicurare un adeguato livello di sicurezza, in fase di prima applicazione del GDPR e per un periodo transitorio di 24 mesi dall'approvazione del presente Regolamento, dovranno comunque essere messe in atto le misure minime di sicurezza previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003, nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), nonché le misure minime di sicurezza per tutte le PA previste dalla Circolare AGID 2/2017.

Art. 21 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR

In caso di verifiche da parte del Garante per la protezione dei dati o della Guardia di Finanza o delle autorità preposte, L'Istituto deve essere in grado di dimostrare che ha messo in atto un sistema di gestione della sicurezza tale da soddisfare i requisiti previsti dall'art. 32 del GDPR.

A tal fine è di fondamentale importanza quanto enunciato dall'art. 32, comma 3, del GDPR, laddove si specifica che l'adesione a codici di condotta approvati o ad uno schema di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

Art. 22 - Verifiche e certificazioni periodiche da parte del Responsabile della protezione dei dati

In ottemperanza a quanto previsto dagli artt. 37, 38 e 39 del GDPR, il Responsabile della protezione dei dati è tenuto ad effettuare, con frequenza almeno quadrimestrale, verifiche finalizzate a verificare e certificare il fatto che i trattamenti e le prassi messe in atto dall'Istituto sono conformi a quanto prescritto dal GDPR; oppure, in caso di non conformità, il Responsabile della protezione dei dati è tenuto a documentare le non conformità riscontrate e ad individuare e descrivere le misure correttive da mettere in atto, specificando inoltre il termine entro il quale le suddette misure devono essere messe in atto e i soggetti coinvolti.



ISTITUTO COMPRENSIVO

3 "Karol Wojtyła"

via Salvemini - 80022 Arzano (Napoli)

☎ 0817311069-fax:08119562349

codice fiscale:93006830637

✉ naic8fs008@istruzione.it - www.ic3karolwojtyla.it



UNI-EN-ISO 9004:2009

Art. 23 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione

Coerentemente con quanto previsto dall'art. 32 comma 3 del GDPR, l'Istituto ha facoltà di ricorrere a codici di condotta e a schemi di certificazione per dimostrare la conformità ai requisiti di cui all'art. 32 comma 1 del GDPR.

Dato che ad oggi i suddetti codici di condotta e/o meccanismi di certificazione approvati non sono stati ancora emessi dall'Autorità Garante per la protezione dei dati personali, viene data facoltà al Responsabile della protezione dei dati di valutare, proporre e coordinare l'adesione a schemi internazionali di certificazione di sicurezza, al fine di poter dimostrare la conformità ai requisiti dell'art. 32 del GDPR - Sicurezza del trattamento, secondo il principio di responsabilizzazione ("accountability"), e di mettere in atto un SGSI - Sistema per la Gestione della Sicurezza delle Informazioni conforme (ad esempio) ai seguenti standard internazionali di sicurezza:

- ISO / IEC 27001 (norma vera e propria)
- ISO / IEC 27002 (best practice e raccomandazioni in materia di sicurezza)
- Annex-A ("Control Objectives and Controls").