



VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

GDPR 2016/679

Scuola/Organizzazione **Istituto Comprensivo Statale “G. Tomasi di Lampedusa”
Pubblica Amministrazione**

TITOLARE

Laura Carmen Sanfilippo

SEDE

Principale
Viale Pirandello, n. 3 92020 - Palma di Montechiaro (AG)

Data revisione: 21/09/2026

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

- a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
- c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento (**C**). Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$LR = P \times C$$

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi
5	Gravissime

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
Conseguenze						

Entità Rischio	Valori di riferimento
Accettabile	$(1 \leq LR \leq 3)$
Medio - basso	$(4 \leq LR \leq 6)$
Rilevante	$(8 \leq LR \leq 12)$
Alto	$(15 \leq LR \leq 25)$

Si ricava, così, per ogni attività di trattamento un **Livello di Rischio** (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA - valutazione del rischio normalizzato

Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevedono due o più criteri di obbligo DPIA.

Nel caso in cui, quindi, l'indice di rischio si colloca nel range $15 \div 25$, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

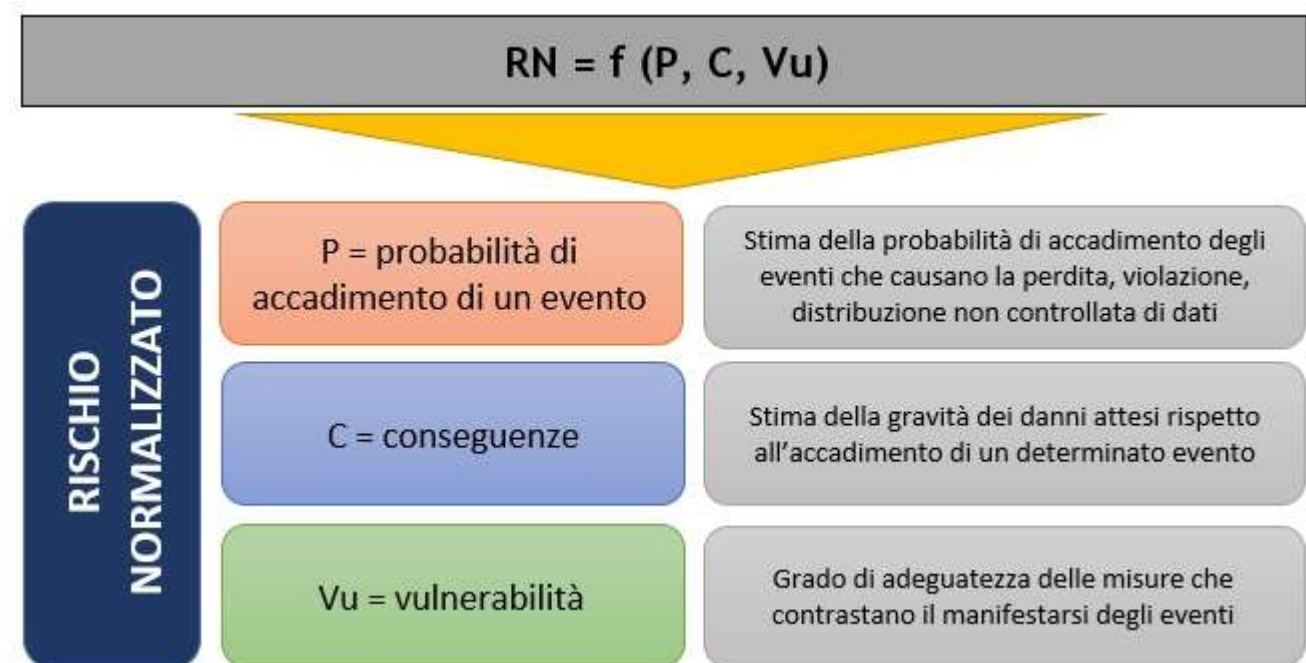
Il rischio viene calcolato in funzione dei 3 fattori seguenti:

$$RN = f(P, C, Vu)$$

Dove:

P = probabilità

C = conseguenze generate dall'evento



V = vulnerabilità rispetto al grado di adeguatezza delle misure

In prima battuta viene ricavato il rischio intrinseco R_i come prodotto della probabilità P e delle conseguenze C , in base agli indici numerici assegnati ad entrambi i fattori.

Alla probabilità P è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	Improbabile
2	Poco probabile
3	Probabile
4	Quasi certo

Alle conseguenze (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	Trascurabili
2	Marginali
3	Limitate
4	Gravi

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

P R O B A B I L I T À	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	Valori di riferimento
Molto basso	$(1 \leq Ri \leq 2)$
Basso	$(3 \leq Ri \leq 4)$
Rilevante	$(6 \leq Ri \leq 9)$
Alto	$(12 \leq Ri \leq 16)$

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità (Vu)** è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

V u	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Scuole ed Università - Protocollo
- Scuole ed Università - Bilancio
- Scuole ed Università - Gestione alunni
- Scuole ed Università - Registro Elettronico
- Scuole ed Università - Intelligenza Artificiale

Scuole ed Università - Protocollo

Struttura	Sede legale
Personale coinvolto	
Responsabile del trattamento	Dsga Lombardo Giovanni
Persone autorizzate	Dsga Lombardo Giovanni Ass. Amm.va Vella Rosetta Ass. Amm.vo Di Caro Giuseppe Ass. Amm.vo Russo Calogero Ass. Amm.vo Palumbo Angelo Ass. Amm.va Contino Ivana Ass. Amm.vo Cancilla Pasquale
Clienti / Fornitori	
Altro	

Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Finalità del trattamento	Programmazione delle attività (pianificazione e monitoraggio del lavoro) Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali Istituzione ed assistenza scolastica Libri ed altre attività editoriali Verifica dell'idoneità al servizio Contratto di assunzione Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati) Relazioni con il pubblico
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Dati identificativi (ragione o denominazione sociale, ovvero nome e

	cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Personalì
Categorie di interessati	Dipendenti Collaboratori Familiari dell'interessato Docenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Rappresentante dei lavoratori per la sicurezza Familiari dell'interessato Datore di lavoro Clienti ed utenti Responsabili interni Associazioni ed enti locali
Informativa	Non necessaria
Consenso	Non necessario
Frequenza trattamento	
Termine cancellazione dati	
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Personale con diritti di accesso	Dsga Lombardo Giovanni Ass. Amm.va Vella Rosetta Ass. Amm.vo Di Caro Giuseppe Ass. Amm.vo Russo Calogero Ass. Amm.vo Palumbo Angelo Ass. Amm.va Contino Ivana Ass. Amm.vo Cancilla Pasquale
Strutture informatiche di backup	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Dsga Lombardo Giovanni Ass. Amm.va Vella Rosetta Ass. Amm.vo Di Caro Giuseppe Ass. Amm.vo Russo Calogero Ass. Amm.vo Palumbo Angelo Ass. Amm.va Contino Ivana Ass. Amm.vo Cancilla Pasquale
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- E' applicata una gestione della password degli utenti.
- E' eseguita la DPIA.
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.
- Sono definiti i ruoli e le responsabilità.
- Sono gestiti i back up
- Sono stabiliti programmi di formazione e sensibilizzazione.
- Viene eseguita una regolare formazione del personale.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' applicata una gestione della password degli utenti.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
E' eseguita la DPIA.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate

Sono definiti i ruoli e le responsabilità.	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	- Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) - Agenti fisici (incendio, allagamento, attacchi esterni) - Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita una regolare formazione del personale.	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
- Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)

RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		

Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

Suole ed Università - Bilancio

Struttura	Sede legale
Personale coinvolto	
Responsabile del trattamento	D.sga Giovanni Lombardo
Persone autorizzate	Giovanni Lombardo Palumbo Angelo
Clienti / Fornitori	
Altro	
Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Finalità del trattamento	Programmazione delle attività (pianificazione e monitoraggio del lavoro) Istituzione ed assistenza scolastica Libri ed altre attività editoriali Verifica dell'idoneità al servizio Contratto di assunzione Ordine e sicurezza pubblica (misure di sicurezza, accertamento e

	repressione reati) Relazioni con il pubblico
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Personalì
Categorie di interessati	Dipendenti Collaboratori Familiari dell'interessato Docenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Rappresentante dei lavoratori per la sicurezza Organismi paritetici in materia di lavoro Organizzazioni sindacali e patronati Familiari dell'interessato Datore di lavoro Clienti ed utenti Responsabili interni Associazioni ed enti locali
Informativa	Non necessaria
Consenso	Non necessario
Frequenza trattamento	
Termine cancellazione dati	
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Personale con diritti di accesso	
Strutture informatiche di backup	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO

PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - E' applicata una gestione della password degli utenti. - E' eseguita la DPIA. - Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati. - Sono definiti i ruoli e le responsabilità. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione. - Viene eseguita una regolare formazione del personale.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' applicata una gestione della password degli utenti.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
E' eseguita la DPIA.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate

Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono definiti i ruoli e le responsabilità.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita una regolare formazione del personale.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN

Basso	0,25	Molto basso
-------	------	-------------

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita		

• Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

Scuole ed Università - Gestione alunni

Struttura	Sede legale
Personale coinvolto	
Responsabile del trattamento	D.sga Giovanni Lombardo
Persone autorizzate	Dsga Lombardo Giovanni Ass. Amm.va Vella Rosetta Ass. Amm.vo Di Caro Giuseppe Ass. Amm.vo Russo Calogero Ass. Amm.vo Palumbo Angelo Ass. Amm.va Contino Ivana Ass. Amm.vo Cancilla Pasquale
Clienti / Fornitori	

Altro	
-------	--

Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Finalità del trattamento	Igiene e sicurezza del lavoro Programmazione delle attività (pianificazione e monitoraggio del lavoro) Attività di previdenza Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali Istituzione ed assistenza universitaria Istituzione ed assistenza scolastica Libri ed altre attività editoriali Verifica dell'idoneità al servizio Contratto di assunzione Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati) Relazioni con il pubblico Informazione scientifica e giuridica
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc. Lavoro (occupazione attuale e precedente, informazioni sul reclutamento, sul tirocinio o sulla formazione professionale, informazioni sulla sospensione o interruzione del rapporto di lavoro o sul passaggio ad altra occupazione, curriculum vitae) Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Dati identificativi dell'orientamento sessuale Codice fiscale ed altri numeri di identificazione personale (carte sanitarie) Convinzioni religiose, adesioni ad organizzazioni a carattere religioso Origini razziali o etniche Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Giudiziari Particolari (sensibili) Personalì
Categorie di interessati	Dipendenti Collaboratori Familiari dell'interessato Docenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Rappresentante dei lavoratori per la sicurezza Organismi paritetici in materia di lavoro Organizzazioni sindacali e patronati Familiari dell'interessato Datore di lavoro Clienti ed utenti Responsabili interni Associazioni ed enti locali
Informativa	Non necessaria
Consenso	Non necessario

Frequenza trattamento	
Termine cancellazione dati	
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Argo	Struttura Esterna
Sede di riferimento	Argo Software srl
Personale con diritti di accesso	
Strutture informatiche di backup	
Argo	Struttura Esterna
Sede di riferimento	Argo Software srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - E' applicata una gestione della password degli utenti. - E' eseguita la DPIA. - Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati. - Sono definiti i ruoli e le responsabilità. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione. - Viene eseguita una regolare formazione del personale.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' applicata una gestione della password degli utenti.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e	Adeguate

	malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	
E' eseguita la DPIA.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono definiti i ruoli e le responsabilità.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita una regolare formazione del personale.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

--	--	--

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
- Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
- Perdita - Distruzione non autorizzata - Modifica non autorizzata		

• Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN

		RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**

Scuole ed Università - Registro elettronico

Struttura	Sede legale
Personale coinvolto	
Responsabile del trattamento	D.sga Lombardo Giovanni
Persone autorizzate	Dsga Lombardo Giovanni Ass. Amm.va Vella Rosetta Ass. Amm.vo Di Caro Giuseppe Ass. Amm.vo Russo Calogero Ass. Amm.vo Palumbo Angelo Ass. Amm.va Contino Ivana Ass. Amm.vo Cancilla Pasquale Tutti i docenti
Clienti / Fornitori	
Altro	

Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Finalità del trattamento	Programmazione delle attività (pianificazione e monitoraggio del lavoro) Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali Istituzione ed assistenza scolastica Libri ed altre attività editoriali Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati) Relazioni con il pubblico
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Convinzioni religiose, adesioni ad organizzazioni a carattere religioso Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.) Personalì
Categorie di interessati	Dipendenti Collaboratori Familiari dell'interessato Docenti
Categorie di destinatari	Soggetti che svolgono attività di archiviazione della documentazione Organizzazioni sindacali e patronati Familiari dell'interessato

	Datore di lavoro Clienti ed utenti Responsabili interni Associazioni ed enti locali
Informativa	Non necessaria
Consenso	Non necessario
Frequenza trattamento	
Termine cancellazione dati	
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Personale con diritti di accesso	Dsga Lombardo Giovanni
Strutture informatiche di backup	
Argo	Struttura esterna
Azienda proprietaria	Argo Software Srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	Dsga Lombardo Giovanni
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - E' applicata una gestione della password degli utenti. - E' eseguita la DPIA. - Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati. - Sono definiti i ruoli e le responsabilità. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione. - Viene eseguita una regolare formazione del personale.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

E' applicata una gestione della password degli utenti.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
E' eseguita la DPIA.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono definiti i ruoli e le responsabilità.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

Viene eseguita una regolare formazione del personale.	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
- Perdita - Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
- Perdita - Distruzione non autorizzata - Modifica non autorizzata - Divulgazione non autorizzata - Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o

componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri

Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO <i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

Suole ed Università - intelligenza artificiale

Struttura	Sede legale
-----------	-------------

Personale coinvolto	
Responsabile del trattamento	Lombardo Giovanni
Persone autorizzate	Lombardo Giovanni Cacciatore Licinia
Clienti / Fornitori	
Altro	

Processo di trattamento	
Descrizione	Uso di strumenti di Intelligenza Artificiale per supportare l'attività didattica, la valutazione degli studenti, l'organizzazione scolastica e la gestione dei dati in ambito educativo.
Finalità del trattamento	- Supporto didattico personalizzato tramite sistemi di IA. - Analisi delle performance scolastiche per migliorare i processi educativi. - Automazione di procedure amministrative. - Comunicazione scuola-famiglia. - Sicurezza informatica e protezione dei dati.
Tipo di dati personali	Dati identificativi degli studenti e personale scolastico. - Dati relativi al percorso scolastico e valutazioni. - Dati comportamentali derivanti da piattaforme di apprendimento. - Eventuali dati sensibili (es. BES/DSA) trattati nel rispetto delle normative
Categorie di interessati	Dipendenti Collaboratori Familiari dell'interessato Docenti
Categorie di destinatari	- Fornitori di servizi digitali e piattaforme IA. - Personale scolastico autorizzato. - Autorità competenti nei limiti previsti dalla legge.
Informativa	Fornita agli interessati
Consenso	Richiesto quando necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno trattati per tutto il tempo necessario allo svolgimento del rapporto commerciale in essere e per i successivi dieci anni dalla data di acquisizione degli stessi.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Software gestionale

Strutture informatiche di archiviazione	
Sede di riferimento	Principale
Personale con diritti di accesso	
Strutture informatiche di backup	
Sede di riferimento	Principale
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	
Note	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	CONSEGUENZE	LIVELLO DI RISCHIO
Improbabile	Marginali	Accettabile

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
- Backup periodico giornaliero su server sicuri. - Accessi regolamentati tramite credenziali. - Procedure per la protezione dei dati e risposta agli incidenti. - E' eseguita la DPIA. - Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati. - Sono definiti i ruoli e le responsabilità. - Sono gestiti i back up - Sono stabiliti programmi di formazione e sensibilizzazione. - Viene eseguita una regolare formazione del personale.

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SIUREZZA	PERICOLI ASSOCIATI	LIVELLO DI ADEGUATEZZA
Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' eseguita la DPIA.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Esistono procedure e disposizioni scritte per	• Problemi tecnici (Anomalie e malfunzionamento software,	Adeguate

l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	problemi hardware o componenti servizio IT)	
Sono definiti i ruoli e le responsabilità.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, allagamento, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita una regolare formazione del personale.	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Marginali	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

PERICOLO		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata		

• Accesso dati non autorizzato		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Marginali	Basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Basso	0,25	Molto basso

PERICOLO		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata • Modifica non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
Rischio intrinseco - Ri	Vulnerabilità - Vu	Rischio normalizzato - RN
Molto basso	0,25	Molto basso

A valle della DPIA l'attività risulta a rischio **Molto basso**