



# VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

*GDPR 2016/679*

Scuola/Organizzazione **DIREZIONE DIDATTICA 1° CIRCOLO "GIOVANNI XXIII"**  
**Pubblica Amministrazione**

<b>TITOLARE</b>	Conti Anna Maria
-----------------	------------------

<b>SEDE</b>	Principale Via G. Licata 18 - 92019 SCIACCA
-------------	--

Data revisione: 09/11/2021

## 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:

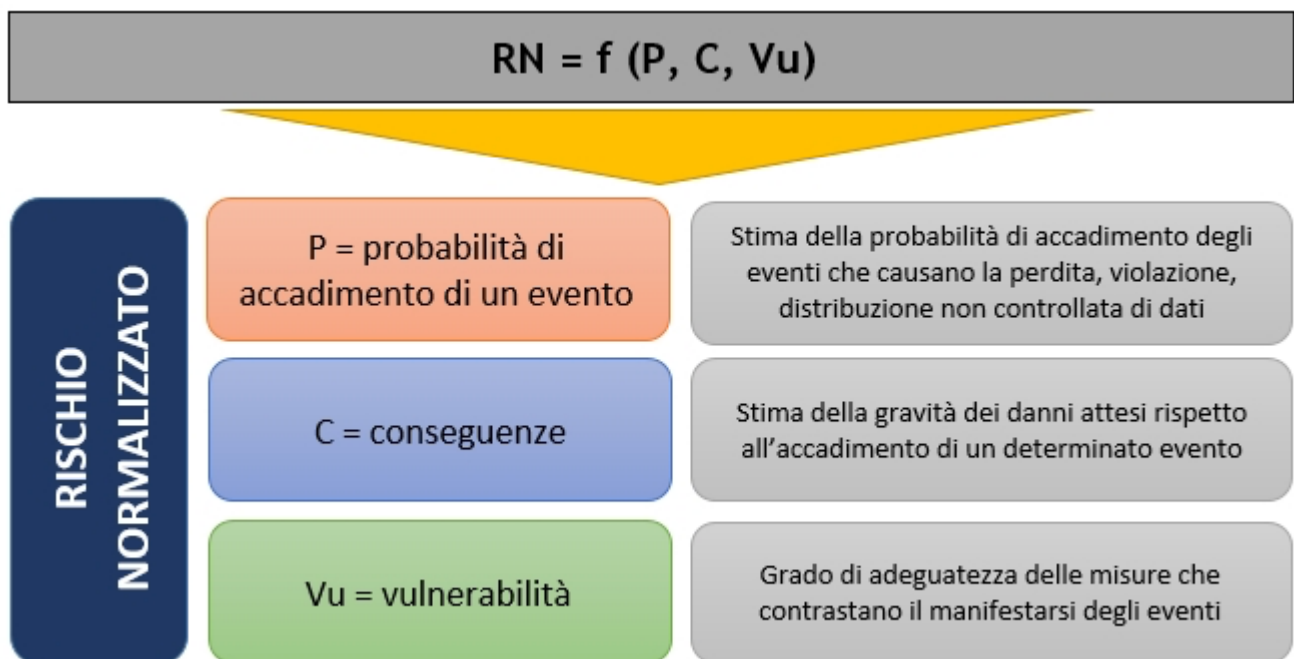
$$RN = f (P, C, Vu)$$

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 ≤ Ri ≤ 2)
Basso	(3 ≤ Ri ≤ 4)
Rilevante	(6 ≤ Ri ≤ 9)
Alto	(12 ≤ Ri ≤ 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)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>

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.

Vu	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
- Scuole ed Università
- Scuole ed Università
- Scuole ed Università

### Scuole ed Università

<b>Struttura</b>	Sede legale
<b>Personale coinvolto</b>	
<b>Responsabile del trattamento</b>	Conti Anna Maria
<b>Persone autorizzate</b>	Indelicato Raimondo - Barone Ignazia - Cusumano Francesca - Lo Giudice Pierangela - Marciante Vincenza - Tamburello Mario
<b>Clienti / Fornitori</b>	
<b>Altro</b>	

<b>Processo di trattamento</b>	
<b>Descrizione</b>	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
<b>Finalità del trattamento</b>	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
<b>Tipo di dati personali</b>	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
<b>Categorie di interessati</b>	Dipendenti Collaboratori Familiari dell'interessato

	Docenti
<b>Categorie di destinatari</b>	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
<b>Informativa</b>	Non necessaria
<b>Consenso</b>	Non necessario
<b>Frequenza trattamento</b>	
<b>Termine cancellazione dati</b>	
<b>Trasferimento dati (paesi terzi)</b>	No
<b>Autorizzazione del Garante</b>	Non presente

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

<b>VALUTAZIONE DEL LIVELLO DI RISCHIO</b>		
<b>PROBABILITÀ</b>	<b>CONSEGUENZE</b>	<b>LIVELLO DI RISCHIO</b>
Improbabile	Marginali	Accettabile

<b>MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE</b>
<ul style="list-style-type: none"> <li>- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati</li> <li>- E' applicata una gestione della password degli utenti.</li> <li>- E' eseguita la DPIA.</li> <li>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.</li> <li>- Sono definiti i ruoli e le responsabilità.</li> <li>- Sono gestiti i back up</li> <li>- Sono stabiliti programmi di formazione e sensibilizzazione.</li> <li>- Viene eseguita una regolare formazione del personale.</li> </ul>

## **VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE**

<b>MISURE DI SIUREZZA</b>	<b>PERICOLI ASSOCIATI</b>	<b>LIVELLO DI ADEGUATEZZA</b>
Autorizzazione del singolo	• Azioni non autorizzate (Errori	Adeguate

incaricato al trattamento e alla modifica dei dati	volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
E' eseguita la DPIA.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	<ul style="list-style-type: none"> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> <li>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)</li> <li>• Agenti fisici (incendio, allagamento, attacchi esterni)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate

Sono stabiliti programmi di formazione e sensibilizzazione.	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Viene eseguita una regolare formazione del personale.	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate

## VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> </ul>		
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		
<ul style="list-style-type: none"> <li>Perdita</li> <li>Distruzione non autorizzata</li> <li>Modifica non autorizzata</li> <li>Divulgazione non autorizzata</li> <li>Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		

<ul style="list-style-type: none"> <li>Modifica non autorizzata</li> </ul>		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
VALUTAZIONE RISCHIO NORMALIZZATO		
Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi		
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

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

Personale coinvolto	
Responsabile del trattamento	Conti Anna Maria
Persone autorizzate	Indelicato Raimondo - Barone Ignazia - Cusumano Francesca - Lo Giudice Pierangela - Marciante Vincenza - Tamburello Mario
Clienti / Fornitori	
Altro	

Processo di trattamento	
Descrizione	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi
Finalità del trattamento	<p>Programmazione delle attività (pianificazione e monitoraggio del lavoro)</p> <p>Istituzione ed assistenza scolastica</p> <p>Libri ed altre attività editoriali</p> <p>Verifica dell'idoneità al servizio</p> <p>Contratto di assunzione</p> <p>Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati)</p> <p>Relazioni con il pubblico</p>
Tipo di dati personali	<p>Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)</p> <p>Curriculum di studi e accademico, pubblicazioni, articoli, monografie, relazioni, materiale audiovisivo, titoli di studio, ecc.</p> <p>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)</p> <p>Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)</p> <p>Codice fiscale ed altri numeri di identificazione personale (carte sanitarie)</p> <p>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)</p>

	Personali
<b>Categorie di interessati</b>	Dipendenti Collaboratori Familiari dell'interessato Docenti
<b>Categorie di destinatari</b>	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
<b>Informativa</b>	Non necessaria
<b>Consenso</b>	Non necessario
<b>Frequenza trattamento</b>	
<b>Termine cancellazione dati</b>	
<b>Trasferimento dati (paesi terzi)</b>	No
<b>Autorizzazione del Garante</b>	Non presente

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

<b>VALUTAZIONE DEL LIVELLO DI RISCHIO</b>		
<b>PROBABILITÀ</b>	<b>CONSEGUENZE</b>	<b>LIVELLO DI RISCHIO</b>
Improbabile	Marginali	Accettabile

<b>MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE</b>
<ul style="list-style-type: none"> <li>- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati</li> <li>- E' applicata una gestione della password degli utenti.</li> <li>- E' eseguita la DPIA.</li> <li>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.</li> <li>- Sono definiti i ruoli e le responsabilità.</li> <li>- Sono gestiti i back up</li> <li>- Sono stabiliti programmi di formazione e sensibilizzazione.</li> <li>- Viene eseguita una regolare formazione del personale.</li> </ul>

## 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	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> <li>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
E' eseguita la DPIA.	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	<ul style="list-style-type: none"> <li>Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> <li>Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> <li>Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)</li> <li>Agenti fisici (incendio,</li> </ul>	Adeguate



	allagamento, attacchi esterni) <ul style="list-style-type: none"> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	
Sono stabiliti programmi di formazione e sensibilizzazione.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Viene eseguita una regolare formazione del personale.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate

## VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Poco probabile	Trascurabili	Molto basso

<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<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

<b>PERICOLO</b>		
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<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

<b>PERICOLO</b>		
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
Probabilità	Conseguenza	Rischio intrinseco - Ri
Improbabile	Trascurabili	Molto basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
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

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

Personale coinvolto	
Responsabile del trattamento	Conti Anna Maria
Persone autorizzate	Indelicato Raimondo - Barone Ignazia - Cusumano Francesca - Lo Giudice Pierangela - Marciante Vincenza - Tamburello Mario
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)

	<p>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</p>
<b>Categorie di interessati</b>	<p>Dipendenti  Collaboratori  Familiari dell'interessato  Docenti</p>
<b>Categorie di destinatari</b>	<p>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</p>
<b>Informativa</b>	Non necessaria
<b>Consenso</b>	Non necessario
<b>Frequenza trattamento</b>	
<b>Termine cancellazione dati</b>	
<b>Trasferimento dati (paesi terzi)</b>	No
<b>Autorizzazione del Garante</b>	Non presente

<b>Modalità di elaborazione dati: Mista - elettronica e cartacea</b>	
<b>Strumenti</b>	Software gestionale
<b>Strutture informatiche di archiviazione</b>	
<b>Argo</b>	Struttura esterna
Sede di riferimento	Argosoft Srl
Personale con diritti di accesso	
<b>Strutture informatiche di backup</b>	
<b>Argo</b>	Struttura esterna
Sede di riferimento	Argosoft 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
<ul style="list-style-type: none"> <li>- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati</li> <li>- E' applicata una gestione della password degli utenti.</li> <li>- E' eseguita la DPIA.</li> <li>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.</li> <li>- Sono definiti i ruoli e le responsabilità.</li> <li>- Sono gestiti i back up</li> <li>- Sono stabiliti programmi di formazione e sensibilizzazione.</li> <li>- Viene eseguita una regolare formazione del personale.</li> </ul>

### 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	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
E' eseguita la DPIA.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate

Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.	<ul style="list-style-type: none"> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate
Sono definiti i ruoli e le responsabilità.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> <li>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)</li> <li>• Agenti fisici (incendio, allagamento, attacchi esterni)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Viene eseguita una regolare formazione del personale.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate

## VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> </ul>		

<ul style="list-style-type: none"> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Rischio intrinseco - Ri</b>
Poco probabile	Trascurabili	Molto basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
<b>Rischio intrinseco - Ri</b>	<b>Vulnerabilità - Vu</b>	<b>Rischio normalizzato - RN</b>
Molto basso	0,25	Molto basso

<b>PERICOLO</b>		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Rischio intrinseco - Ri</b>
Improbabile	Trascurabili	Molto basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
<b>Rischio intrinseco - Ri</b>	<b>Vulnerabilità - Vu</b>	<b>Rischio normalizzato - RN</b>
Molto basso	0,25	Molto basso

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

## Scuole ed Università

<b>Struttura</b>	Sede legale
<b>Personale coinvolto</b>	
<b>Responsabile del trattamento</b>	Conti Anna Maria
<b>Persone autorizzate</b>	Indelicato Raimondo - Barone Ignazia - Cusumano Francesca - Lo Giudice Pierangela - Marciante Vincenza - Tamburello Mario
<b>Clienti / Fornitori</b>	
<b>Altro</b>	
<b>Processo di trattamento</b>	
<b>Descrizione</b>	Trattamento di dati personali dei dipendenti: Docenti, Ricercatori, Dirigenti, Tecnici ed Amministrativi



<b>Finalità del trattamento</b>	<p>Programmazione delle attività (pianificazione e monitoraggio del lavoro)</p> <p>Reclutamento, selezione, valutazione e monitoraggio del personale: test attitudinali</p> <p>Istituzione ed assistenza scolastica</p> <p>Libri ed altre attività editoriali</p> <p>Ordine e sicurezza pubblica (misure di sicurezza, accertamento e repressione reati)</p> <p>Relazioni con il pubblico</p>
<b>Tipo di dati personali</b>	<p>Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali)</p> <p>Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare)</p> <p>Convinzioni religiose, adesioni ad organizzazioni a carattere religioso</p> <p>Dati identificativi (ragione o denominazione sociale, ovvero nome e cognome delle persone fisiche, indirizzo sede, telefono, fax, e-mail, dati fiscali, ecc.)</p> <p>Personali</p>
<b>Categorie di interessati</b>	<p>Dipendenti</p> <p>Collaboratori</p> <p>Familiari dell'interessato</p> <p>Docenti</p>
<b>Categorie di destinatari</b>	<p>Soggetti che svolgono attività di archiviazione della documentazione</p> <p>Organizzazioni sindacali e patronati</p> <p>Familiari dell'interessato</p> <p>Datore di lavoro</p> <p>Clients ed utenti</p> <p>Responsabili interni</p> <p>Associazioni ed enti locali</p>
<b>Informativa</b>	Non necessaria
<b>Consenso</b>	Non necessario
<b>Frequenza trattamento</b>	
<b>Termine cancellazione dati</b>	
<b>Trasferimento dati (paesi terzi)</b>	No
<b>Autorizzazione del Garante</b>	Non presente

<b>Modalità di elaborazione dati: Mista - elettronica e cartacea</b>	
<b>Strumenti</b>	Software gestionale
<b>Strutture informatiche di archiviazione</b>	
<b>Argo</b>	Struttura esterna
Sede di riferimento	Argosoft Srl
Personale con diritti di accesso	
<b>Strutture informatiche di backup</b>	
<b>Argo</b>	Struttura esterna
Sede di riferimento	Argosoft Srl
Frequenza di backup	1 giorni
Tempo di storicizzazione	7 giorni
Personale con diritti di accesso	
Note	

<b>VALUTAZIONE DEL LIVELLO DI RISCHIO</b>		
<b>PROBABILITÀ</b>	<b>CONSEGUENZE</b>	<b>LIVELLO DI RISCHIO</b>

Improbabile	Marginali	Accettabile
-------------	-----------	-------------

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
<ul style="list-style-type: none"> <li>- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati</li> <li>- E' applicata una gestione della password degli utenti.</li> <li>- E' eseguita la DPIA.</li> <li>- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati.</li> <li>- Sono definiti i ruoli e le responsabilità.</li> <li>- Sono gestiti i back up</li> <li>- Sono stabiliti programmi di formazione e sensibilizzazione.</li> <li>- Viene eseguita una regolare formazione del personale.</li> </ul>

### 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	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
E' applicata una gestione della password degli utenti.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
E' eseguita la DPIA.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> <li>• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)</li> </ul>	Adeguate
Esistono procedure e disposizioni scritte per	<ul style="list-style-type: none"> <li>• Problemi tecnici (Anomalie e malfunzionamento software,</li> </ul>	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.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Sono gestiti i back up	<ul style="list-style-type: none"> <li>• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)</li> <li>• Agenti fisici (incendio, allagamento, attacchi esterni)</li> <li>• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)</li> </ul>	Adeguate
Sono stabiliti programmi di formazione e sensibilizzazione.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate
Viene eseguita una regolare formazione del personale.	<ul style="list-style-type: none"> <li>• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)</li> </ul>	Adeguate

## VALUTAZIONE DEI RISCHI

PERICOLO		
Agenti fisici (incendio, allagamento, attacchi esterni)		
RISCHI		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> <li>• Accesso dati non autorizzato</li> </ul>		
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		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> <li>• Divulgazione non autorizzata</li> </ul>		

<ul style="list-style-type: none"> <li>• Accesso dati non autorizzato</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Rischio intrinseco - Ri</b>
Poco probabile	Marginali	Basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
<b>Rischio intrinseco - Ri</b>	<b>Vulnerabilità - Vu</b>	<b>Rischio normalizzato - RN</b>
Basso	0,25	Molto basso

<b>PERICOLO</b>		
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)		
<b>RISCHI</b>		
<ul style="list-style-type: none"> <li>• Perdita</li> <li>• Distruzione non autorizzata</li> <li>• Modifica non autorizzata</li> </ul>		
<b>VALUTAZIONE RISCHIO INTRINSECO</b>		
<b>Probabilità</b>	<b>Conseguenza</b>	<b>Rischio intrinseco - Ri</b>
Improbabile	Trascurabili	Molto basso
<b>VALUTAZIONE RISCHIO NORMALIZZATO</b>		
<i>Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi</i>		
<b>Rischio intrinseco - Ri</b>	<b>Vulnerabilità - Vu</b>	<b>Rischio normalizzato - RN</b>
Molto basso	0,25	Molto basso

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