Privacy

Regolamento UE 2016/679 (GDPR) e D.lgs. n° 196 del 30/06/2003 modificato dal D.lgs. n° 101 del 10/08/2018

DPIA

(VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI)

TITOLARE	Istituto delle Suore dell'Immacolata – Carinola
Legale rappresentante	Clara Squarzieri

SEDE	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Contatti	- E-mail: economato@immacolatine.it - Tel. 0823 939246

CONTITOLARE	Istituto delle Suore dell'Immacolata
Legale rappresentante	Clara Squarzieri

SEDE	Via Padre Giovanni Semeria, 32 - 16131 Genova, IT
Contatti	- E-mail: economato@immacolatine.it - Tel. 010 358234

DPO	Manca Efisio
Contatti	- E-mail: privacylab@duplicar.it - Telefono: 010 511544/258

Elenco attività sottoposte a DPIA	

Luogo e data, Ge 01.09.2020

PREMESSA:

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. Pag. 3 / 26

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	Molto 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:

PROBABILITA'						
	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 ≤ LR ≤ 3)*
Molto - Basso	*(4 ≤ LR ≤ 6)*
Rilevante	*(8 ≤ LR ≤ 12)*
Alto	*(15 ≤ LR ≤ 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.

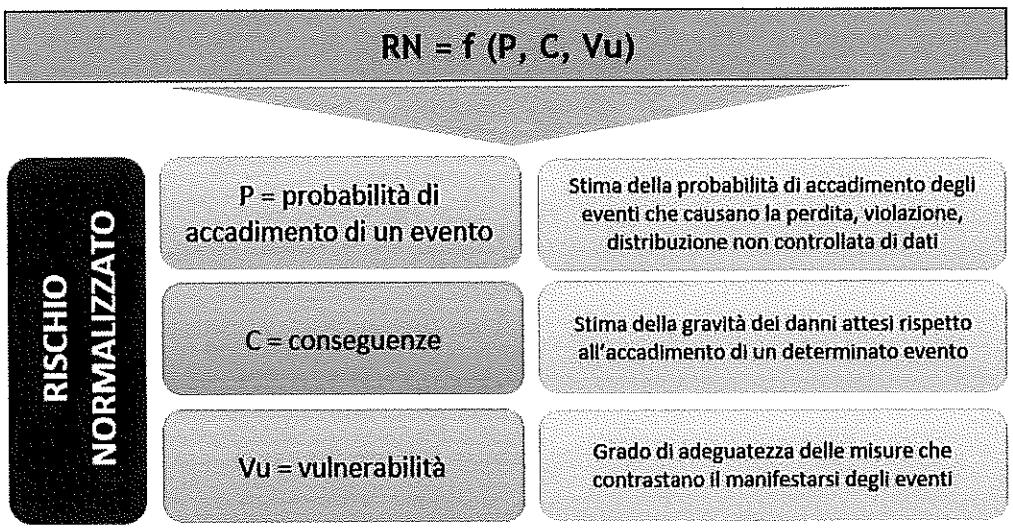
3° STEP: DPIA – valutazione del rischio normalizzato

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 prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 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
Vu = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri 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:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	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

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

PROBABILITA'					
	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, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, 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.

Vu	1	1 < RN ≤ 2	3 ≤ RN ≤ 4	6 ≤ RN ≤ 9	12 ≤ RN ≤16
	0,5	0,5 < RN ≤ 1	1,5 ≤ RN ≤ 2	3 < RN ≤ 5	6 ≤ RN ≤ 8
	0,25	0,25 ≤ RN ≤ 0,5	0,75 ≤ RN ≤ 1	1,5 ≤ RN < 3	3 ≤ RN ≤ 4
		1 ≤ Ri ≤ 2	3 ≤ Ri ≤ 4	6 ≤ Ri ≤ 9	12 ≤ Ri ≤16
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	Valori di riferimento
Molto Basso	*0,25 ≤ RN ≤ 1*
Basso	*1 < RN < 3*
Rilevante	*3 ≤ RN ≤ 9*
Alto	*12 ≤ RN ≤ 16*

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

1. **NG30 – Consegna Cedolini**
2. **EL05 – Sistema dell'Istruzione**

1. NG30 - Consegna Cedolini

Reparti Interessati:	• Amministrazione

Personale coinvolto	
Referente del trattamento	Responsabile di Sede
Persone autorizzate	Si è provveduto a far sottoscrivere idoneo patto di riservatezza mediante "Nomina ad addetto al Trattamento", sono stati impartite istruzioni atte a garantire la riservatezza dei Dati Personali trattati per conto del Titolare del trattamento. Sono anche stati organizzati corsi di formazione in materia di protezione dei dati personali.
Responsabili Esterni del Trattamento	Nessuno
Altro	Amministrativo

Processo di trattamento	
Descrizione	Il trattamento ha per oggetto la consegna dei cedolini dei dipendenti in forma cartacea, l'operazione è svolta esclusivamente dal Responsabile di sede o suo delegato.
Fonte dei dati personali	- Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	- Norme di Legge - Consenso

Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	- Norme di Legge - Consenso
Finalità del trattamento	- Invio telematico dei cedolini alle sedi competenti
Tipo di dati personali	Nominativo; Codice fiscale ed altri numeri di identificazione personale; Sesso m/f; Tessera sanitaria; Indirizzo e-mail Numero di Telefono, IBAM.
Categorie di interessati	- Dipendenti
Categorie di destinatari	- Responsabili Interni
Informativa	Si
Profilazione	No
Dati particolari	No
Consenso minori	No
Frequenza trattamento	Mensile
Termine cancellazione dati	Trattamento con durata prestabilita pari a 1 Mese
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Consegna manuale
Strutture informatiche di archiviazione	
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Personale con diritti di accesso	Amministrativo
Software utilizzati	Non applicabile
NAS	Non applicabile
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Frequenza di backup	Non applicabile
Personale con diritti di accesso	Amministrativo

Software utilizzati	Non applicabile
Strutture informatiche di backup	
NAS	Non applicabile
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Frequenza di backup	Non applicabile
Tempo di storicizzazione	annuale
Personale con diritti di accesso	Amministrativo
Note	
Software utilizzati	Non applicabile

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- È applicata una procedura per la gestione degli accessi
- È eseguita la DPIA
- È presente una politica per la sicurezza e la protezione dei dati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate ogni 6 mesi
- Le procedure sono riesaminate con cadenza predefinita
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Viene eseguita opportuna manutenzione

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
Dispositivi antincendio	• Agenti fisici (incendio, attacchi esterni)	Adeguate
È applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
È 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
È presenta una politica per la sicurezza e la protezione dei dati	• 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.) • Eventi naturali (terremoti, 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
I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, attacchi esterni)	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Le password sono modificate ogni 6 mesi	• 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
Le procedure sono riesaminate con cadenza predefinita	• 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)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, ecc.)	Adeguate
Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• 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
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	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	Limitate	Rilevante
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**
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Gravi	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**
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**
Probabile	Limitate	Rilevante
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**
Rilevante	0,25	Basso

Considerazioni:A valle della DPIA l'attività **"NG30–Consegna Cedolini"**risulta a rischio:

BASSO

Considerazioni del DPO: Il trattamento dei dati relativo a "**Consegna Cedolini**" risulta rispettoso del principio di proporzionalità, in virtù del fatto che non vengono in alcun modo trattati dati eccedenti e non pertinenti rispetto alla finalità perseguita.
In ragione di quanto esposto nella presente valutazione di impatto risultano gestiti e presidiati i rischi legati al trattamento.
Il trattamento è stato inoltre valutato anche dal punto di vista della conservazione del dato, nel rispetto del principio di limitazione e minimizzazione del trattamento.
I dati vengono trattati (come da specifiche riportate all'interno della valutazione) e a cura di soggetti autorizzati al trattamento, da Responsabili Esterni del Trattamento regolarmente Nominati oltre che dal Medico Competente Dott.ssa Greco Stella.

Firma del Titolare del Trattamento

Firma del Referente del Trattamento

Firma del DPO

2. EL05 - Sistema dell'Istruzione

Reparti Interessati:	• Amministrazione • Didattico • Servizi

Personale coinvolto	
Referente del trattamento	Responsabile di sede
Persone autorizzate	Si è provveduto a far sottoscrivere idoneo patto di riservatezza mediante "Nomina ad addetto al Trattamento", sono stati impartite istruzioni atte a garantire la riservatezza dei Dati Personali trattati per conto del Titolare del trattamento. Sono anche stati organizzati corsi di formazione in materia di protezione dei dati personali.
Responsabili Esterni del Trattamento	- Master Training S.r.l. - Duplicar S.r.l. - Pellegrini S.p.A. - Wingsoft Technology - Docenti (esterni) - Namirial S.p.a.
Altro	Inoltre potrebbero avere accesso ai dati: Amministratori di Sistema, Aziende o professionisti nello svolgimento dei loro compiti di assistenza e manutenzione delle strutture informatiche; Personale incaricato dell'acquisizione e dell'invio di tutta la documentazione istituzionale.

Processo di trattamento	
Descrizione	Il trattamento ha per oggetto le attività di gestione delle strutture dei servizi per l'infanzia e degli istituti di istruzione primaria e secondaria inferiore di competenza. Dati degli alunni, relativi a specifiche situazioni patologiche e/o disabilità, certificati di vaccinazione, allergie alimentari che afferiscono a categorie di particolare sensibilità, sono comunicati direttamente dalla famiglia, raccolti in formato cartaceo, digitalizzati ed eventualmente segnalati al docente di sostegno. Le scelte effettuate per il servizio di mensa (pasti vegetariani o rispondenti a convinzioni religiose) possono rivelare le convinzioni religiose, filosofiche o di altro genere, così come l'origine etnica o razziale è desumibile dalla nazionalità. Tutte o parte delle informazioni raccolte possono essere comunicate a gestori del servizio mensa

	esterni all'istituto o soggetti che provvedono all'erogazione del servizio di trasporto scolastico.
Fonte dei dati personali	- Raccolti direttamente
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	- Norme di Legge - Consenso
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	- Norme di Legge - Consenso
Finalità del trattamento	- Istruzione e cultura - Attività relativa alla gestione dei servizi per l'infanzia e delle scuole materne elementari, medie e superiori.
Tipo di dati personali	Convinzioni religiose; adesione ad organizzazioni a carattere religioso; Codice fiscale ed altri numeri di identificazione personale; Nominativo, indirizzo o altri elementi di identificazione personale; Origini razziali; Origini etniche; Convinzioni filosofiche o di altro genere; adesione ad organizzazioni a carattere filosofico; Stato di salute - patologie attuali, patologie pregresse, terapie in corso; Dati relativi alla situazione reddituale
Categorie di interessati	- Scolari, Studenti e famiglie di questi.
Categorie di destinatari	- Organi istituzionali; Organismi sanitari, personale medico e paramedico; Cooperative sociali e ad altri enti; Gestori esterni delle mense e società di trasporto; enti convenzionati; Gestori esterni del servizio di trasporto scolastico.
Informativa	Si
Profilazione	No
Dati particolari	Si
Consenso minori	Si
Frequenza trattamento	giornaliero
Termine cancellazione dati	I dati vengono trattati per tutto il percorso scolastico dell'alunno e successivamente storicizzati.
Trasferimento dati (paesi terzi)	No
Autorizzazione del Garante	Non presente

Modalità di elaborazione dati: Mista - elettronica e cartacea	
Strumenti	Elettronici e cartacei
Strutture informatiche di archiviazione	
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Personale con diritti di accesso	Dirigenti, Insegnanti, Operatori.
Software utilizzati	Mastercon Pro, Microsoft 365
NAS	Struttura interna e Cloud
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Frequenza di backup	Giornaliera
Personale con diritti di accesso	Dirigenti, Insegnanti, Operatori.
Software utilizzati	Mastercon Pro, Microsoft 365
Strutture informatiche di backup	
NAS	Struttura interna e Cloud
Sede di riferimento	Corso Umberto I, 70 - 81030 Carinola (CE), IT
Frequenza di backup	giornaliera
Tempo di storicizzazione	annuale
Personale con diritti di accesso	- Master Training S.r.l. - Duplicar S.r.l.
Note	
Software utilizzati	Proprietario Mastercom Pro

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Poco probabile	Gravi	Rilevante

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati
- Dispositivi antincendio
- È applicata una procedura per la gestione degli accessi
- È eseguita la DPIA
- È presente una politica per la sicurezza e la protezione dei dati
- Esistono procedure e disposizioni scritte per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati
- Crittografati dei dati
- I documenti vengono firmati digitalmente
- I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili
- Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi
- Le password sono costituite da almeno otto caratteri alfanumerici
- Le password sono modificate ogni 6 mesi
- Le procedure sono riesaminate con cadenza predefinita
- Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee
- Sistemi di allarme e di sorveglianza anti-intrusione
- Sono applicate procedure di disaster recovey che garantiscono il ripristino dell'accesso ai dati in tempi ridotti
- Sono applicate regole per la gestione delle password.
- Sono definiti i ruoli e le responsabilità
- Sono definiti i termini di conservazione e le condizioni di impiego dei dati.
- Sono gestiti i back up
- Sono utilizzati software antivirus e anti intrusione
- Vengono registrati e conservati i Log file
- Viene eseguita opportuna manutenzione

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
Dispositivi antincendio	• Agenti fisici (incendio, attacchi esterni)	Adeguate
È applicata una procedura per la gestione degli accessi	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
È 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
È presenta una politica per la sicurezza e la protezione dei dati	• 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.) • Eventi naturali (terremoti, 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
Crittografia dei Dati	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
I documenti vengono firmati digitalmente	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Impianto elettrico dotato di misure salvavita atte anche ad evitare cortocircuiti e possibili incendi	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, attacchi esterni)	Adeguate
Le password sono costituite da almeno otto caratteri alfanumerici	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Le password sono modificate ogni 6 mesi	• 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
Le procedure sono riesaminate con cadenza predefinita	• 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)	Adeguate
Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	• Agenti fisici (incendio, attacchi esterni) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) • Eventi naturali (terremoti, ecc.)	Adeguate
Sono applicate procedure di disaster recovey che garantiscono il ripristino dell'accesso ai dati in tempi ridotti	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	Adeguate
Sono applicate regole per la gestione delle password.		Adeguate

Sono definiti i ruoli e le responsabilità	• Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Sono definiti i termini di conservazione e le condizioni di impiego dei dati.	• 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
Sono gestiti i back up	• Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) • Agenti fisici (incendio, attacchi esterni) • Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	Adeguate
Sono utilizzati software antivirus e anti intrusione	• 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
Vengono registrati e conservati i Log file	• Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) • Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
Viene eseguita opportuna manutenzione	• Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	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	Limitate	Rilevante
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**
Rilevante	0,25	Basso

PERICOLO		
Eventi naturali (terremoti, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Gravi	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**
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**
probabile	Limitate	Rilevante
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**
Rilevante	0,25	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	Limitate	Rilevante
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**
Rilevante	0,25	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	Limitate	Rilevante
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**
Rilevante	0,25	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**
Probabile	Limitate	Rilevante

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**
Rilevante	0,25	Basso

Considerazioni:A valle della DPIA l'attività **"EL05–Sistema dell'Istruzione"** risulta a rischio:

BASSO

Considerazioni del DPO: Il trattamento dei dati relativo a "**Sistema dell'Istruzione**" risulta rispettoso del principio di proporzionalità, in virtù del fatto che non vengono in alcun modo trattati dati eccedenti e non pertinenti rispetto alla finalità perseguita.
In ragione di quanto esposto nella presente valutazione di impatto risultano gestiti e presidiati i rischi legati al trattamento.
Il trattamento è stato inoltre valutato anche dal punto di vista della conservazione del dato, nel rispetto del principio di limitazione e minimizzazione del trattamento.
I dati vengono trattati (come da specifiche riportate all'interno della valutazione) e a cura di soggetti autorizzati al trattamento, da Responsabili Esterni del Trattamento regolarmente Nominati oltre che dal Medico Competente Dott.ssa Greco Stella.

Firma del Titolare del Trattamento

Firma del Referente del Trattamento

Firma del DPO