VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Azienda/Organizzazione	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" **Istituto e scuola pubblica di ogni ordine e grado**

TITOLARE AMELIA CAPOZZI

I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"

SEDE Piazza Ugenti, 17
70025 **Grumo Appula** - BA

Data revisione: 26/01/2023

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 X 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:

Probabilità	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.

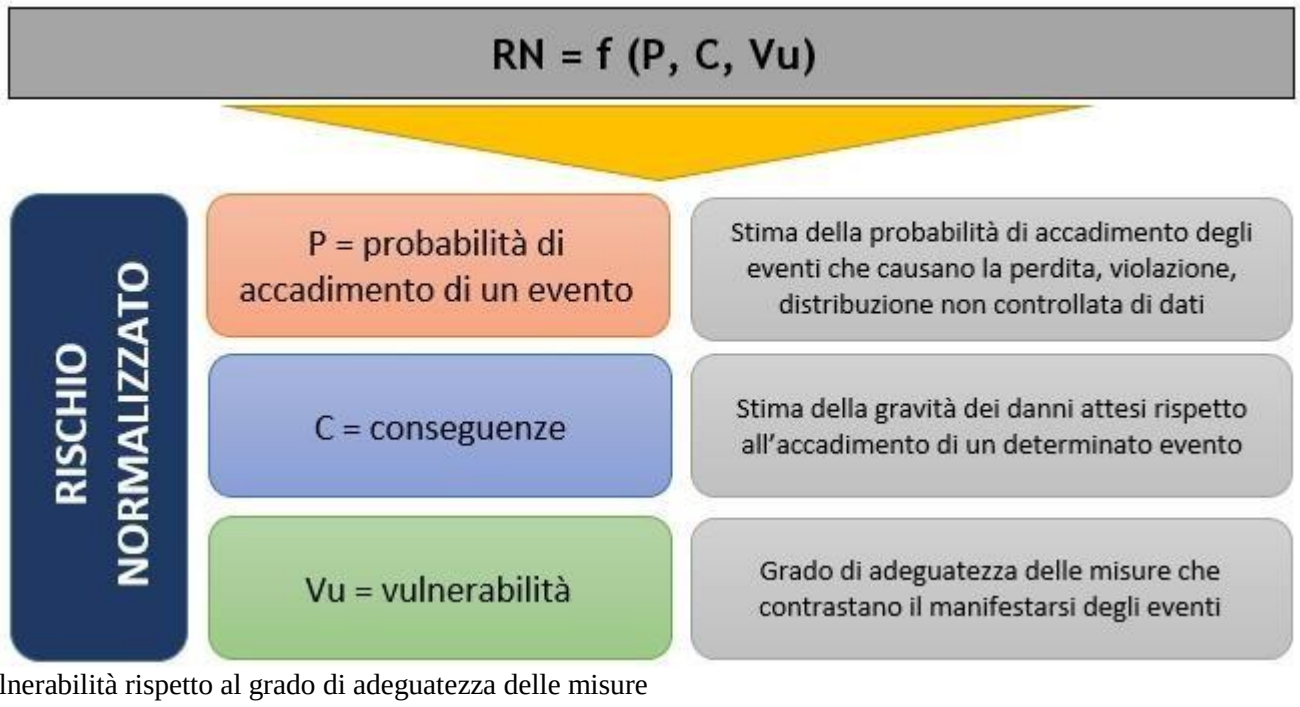
3 STEP: DPIA – valutazione del rischio normalizzato
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca 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



V = 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:

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*** ≤ 2*)*
Basso	*(*$3 \leq$ ***Ri*** ≤ 4*)*
Rilevante	*(*$6 \leq$ ***Ri*** ≤ 9*)*
Alto	*(*$12 \leq$ ***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)	• 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.

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

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

- Personale - Titolare del trattamento
- Alunni - Titolare del trattamento
- Alunni BES - Titolare del trattamento
- DDI - Titolare del trattamento
- Fornitori – Titolare del trattamento

PERSONALE - Titolare del trattamento

Gestione personale		
GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - PERSONALE
	Date	Creato il 26/01/2023
	Stato	attivo
	Modalità di gestione	Browser- Java - Lettore PDF - Live Care: Software di assistenza Remota - Software Gestionale: Axios - Suite Office o equivalenti
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Centinaia
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione, Direttore servizi generali amministrativi, Sicurezza luoghi di lavoro, Ufficio personale, Ufficio alunni, Ufficio protocollo, Nucleo Interno di Valutazione, Ufficio affari generali
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione, Tutti gli autorizzati di Direttore servizi generali amministrativi, Tutti gli autorizzati di Sicurezza luoghi di lavoro, Tutti gli autorizzati di Ufficio personale, Tutti gli autorizzati di Ufficio alunni, Tutti gli autorizzati di Ufficio protocollo, Tutti gli autorizzati di Nucleo Interno di Valutazione, Tutti gli autorizzati di Ufficio affari generali
OPERAZIONI	Elementi organigramma	Operazioni
	Direzione	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Direttore servizi generali amministrativi	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Sicurezza luoghi di lavoro	Comunicazione, Consultazione, Organizzazione, Raccolta, Uso
	Ufficio personale	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio alunni	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio protocollo	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Nucleo Interno di Valutazione	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio affari generali	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione e del merito - MI, Ministero delle economie e delle finanze, Portale SIDI, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	Gestione degli aspetti relativi al trattamento giuridico ed economico del personale e verifica del possesso dei requisiti per l'assunzione. (Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale)

	Tipologie	Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) giudiziari particolari (sensibili) personali adesioni a sindacati o organizzazioni a carattere sindacale convinzioni religiose, adesioni ad organizzazioni a carattere religioso.
CATEGORIE	Interessati	Familiari dell'interessato dipendenti, candidati per eventuale rapporto di lavoro
	Dati personali	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).
	Destinatari	-
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (“principio di limitazione della conservazione”, art. 5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' applicata una gestione della password degli utenti - E' applicata una procedura per la gestione degli accessi - E' eseguita la DPIA - E' presenta una politica per la sicurezza e la protezione dei dati - Esistono procedure e disposizioni scritti per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati - Esistono procedure per l'individuazione del custode delle password - I dati sono crittografati - 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 atti anche ad evitare cortocircuiti e possibili incendi - Le password sono costituite da almeno otto caratteri alfanumerici - Le password sono modificate ogni 7 mesi - Le procedure sono riesaminate con cadenza predefinita - L'impianto elettrico è certificato ed a norma - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Registrazione e de registrazione degli utenti - Sistemi di allarme e di sorveglianza anti-intrusione - Sono applicate procedure di disaster recovery 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili - Sono utilizzati software antivirus e anti intrusione - Vengono registrati e conservati i Log file - Viene eseguita opportuna manutenzione	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

ALUNNI - Titolare del trattamento

Gestione alunni

GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - ALUNNI
	Date	26/01/2023
	Stato	attivo
	Modalità di gestione	Browser- Java - Lettore PDF - Live Care: Software di assistenza Remota - Software Gestionale: Axios - Suite Office o equivalenti
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Centinaia
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione, Direttore servizi generali amministrativi, Sicurezza luoghi di lavoro, Ufficio alunni, Ufficio protocollo, Didattica, Referente Covid, Nucleo Interno di Valutazione, Ufficio affari generali
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione, Tutti gli autorizzati di Direttore servizi generali amministrativi, Tutti gli autorizzati di Sicurezza luoghi di lavoro, Tutti gli autorizzati di Ufficio alunni, Tutti gli autorizzati di Ufficio protocollo, Tutti gli autorizzati di Didattica, Tutti gli autorizzati di Referente Covid, Tutti gli autorizzati di Nucleo Interno di Valutazione, Tutti gli autorizzati di Ufficio affari generali
OPERAZIONI	Elementi organigramma	Operazioni
	Direzione	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Direttore servizi generali amministrativi	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Sicurezza luoghi di lavoro	Conservazione, Consultazione, Organizzazione, Raccolta, Uso
	Ufficio alunni	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio protocollo	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Didattica	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Referente Covid	Estrazione, Consultazione, Comunicazione
	Nucleo Interno di Valutazione	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio affari generali	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione e del merito- MI, Ministero delle economie e delle finanze, Portale SIDI, pagoPA, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	Predisposizione delle graduatorie, smistamento e accettazione delle domande di iscrizione sulla base della disponibilità di posti e dei criteri di precedenza, deliberati dal Consiglio di Istituto, in caso di richieste eccedenti. Perfezionamento dell'iscrizione per la successiva gestione amministrativa dell'alunno con riferimento ai servizi connessi alla didattica. Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi e adempimento degli obblighi previsti dal D.M.)92/2016. Fotografiche e/o video che ritraggano l'alunno e/o i suoi familiari durante lo svolgimento di attività scolastiche curriculari ed extracurriculari inserite nel PTOF possano essere utilizzate per fini istituzionali e di documentazione, quali la pubblicazione sul giornalino scolastico o altre testate giornalistiche locali e nazionali, su poster o manifesti dell'istituto, anche in occasione di partecipazione a fiere e stand dell'orientamento, o sul sito web dell'istituto. In tal caso il trattamento avrà durata temporanea e prevedrà immagini e video che

		ritraggano gli alunni solo in atteggiamenti ‘positivi’. (Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale)
	Tipologie	Dati di contatto e foto, Accessi e presenze, Account utente, Allergie consumatori finali,
		Allergie minori, Anagrafiche, Anamnesi medica, Appartenenza a categorie protette, Certificati di malattia, Certificati medici, Città, Cittadinanza, Classe, Codice fiscale, Cognome e nome, Composizione nucleo familiare, Copia certificati scolastici, Comune di nascita, Comune di residenza, Condizioni di pagamento, Confessione religiosa, Copia di documenti d'identità in formato digitale e cartaceo, Data e luogo di nascita, Dati anagrafici, Dati anagrafici dei genitori, Orientamento religioso, Dati relativi alla famiglia e a situazioni personali (stato civile, minori, figli, soggetti a carico, consanguinei, altri appartenenti al nucleo familiare) Giudiziari Esiti scolastici degli alunni Dati sulla salute Origini razziali o etniche Convinzioni religiose, adesioni ad organizzazioni a carattere religioso
CATEGORIE	Interessati	Alunni, Familiari
	Dati personali	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).
	Destinatari	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) SIDI ALBO ON LINE della scuola (solo i dati relativi agli esiti scolastici) Altre strutture del sistema della Pubblica Istruzione, altre strutture pubbliche, INAIL, Azienda Sanitaria pubblica competente, Società di Assicurazione per polizza infortuni, Agenzie viaggi (Dati Personali).
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (“principio di limitazione della conservazione”, art. 5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO	Questo trattamento non prevede alcun trasferimento verso organizzazioni	

ORGANIZZAZIONI INTERNAZIONALI	internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati, Dispositivi antincendio, E' applicata una gestione della password degli utenti, E' applicata una procedura per la gestione degli accessi, E' eseguita la DPIA, E' presenta una politica per la sicurezza e la protezione dei dati, Esistono procedure e disposizioni scritti per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati, Esistono procedure per l'individuazione del custode delle password, I dati sono crittografati, 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 atti anche ad evitare cortocircuiti e possibili incendi, Le password sono costituite da almeno otto caratteri alfanumerici, Le password sono modificate ogni 7 mesi, Le procedure sono riesaminate con cadenza predefinita, Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee, Registrazione e de registrazione degli utenti, Sistemi di allarme e di sorveglianza anti- intrusione, Sono applicate procedure di disaster recovery 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili, Sono utilizzati software antivirus e anti intrusione, Vengono registrati e conservati i Log file, Viene eseguita opportuna manutenzione, L'impianto elettrico è certificato ed a norma	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

ALUNNI BES - Titolare del trattamento

Gestione Alunni BES		
GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - ALUNNI BES
	Date	Creato il 26/01/2023
	Stato	attivo
	Modalità di gestione	Browser- Java - Lettore PDF - Live Care: Software di assistenza Remota - Software Gestionale: Axios - Suite Office o equivalenti
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Decine
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione, Direttore servizi generali amministrativi, Ufficio alunni, Ufficio protocollo, Didattica, Area BES, Ufficio affari generali
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione, Tutti gli autorizzati di Direttore servizi generali amministrativi, Tutti gli autorizzati di Ufficio alunni, Tutti gli autorizzati di Ufficio protocollo, Tutti gli autorizzati di Didattica, Tutti gli autorizzati di Area BES, Tutti gli autorizzati di Ufficio affari generali
OPERAZIONI	Elementi organigramma	Operazioni
	Direzione	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Direttore servizi generali amministrativi	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio alunni	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio protocollo	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Didattica	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Area BES	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio affari generali	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Strutturazione, Uso
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione e del merito- MI, Ministero delle economie e delle finanze, Portale SIDI, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi e adempimento degli obblighi previsti dal D.M.)92/2016. Assegnazione del docente di sostegno Elaborazione del Profilo dinamico funzionale e stesura del Piano educativo individualizzato. Passaggio di competenza del fascicolo alla nuova scuola nel caso di passaggio a scuola di diverso ordine e grado o di trasferimento ad altra scuola. Saranno rese disponibili nella partizione del Sistema SIDI - Anagrafe degli alunni con disabilità, tramite le quali sarà possibile consultare la documentazione necessaria da parte degli operatori e degli utenti autorizzati. In fase di definizione la versione digitale dei modelli PEI che saranno da compilarsi in modalità telematica con accesso tramite sistema SIDI da parte delle Istituzioni scolastiche e dei componenti dei rispettivi GLO. (Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale)

	Tipologie	Dati idonei a rilevare lo stato di disabilità degli alunni, indispensabili per la loro integrazione scolastica, privi degli elementi identificativi degli alunni stessi (la certificazione dello stato di handicap o dello stato di handicap in situazione di gravità ai sensi della legge 5 febbraio 1992, n. 105, la diagnosi funzionale dell'alunno cui provvede l'unità multidisciplinare prevista dall'articolo 7, comma 2, del decreto del Presidente della Repubblica 25 febbraio 1995,ilconseguente profilo dinamico-funzionale e il piano educativo individualizzato).
	Interessati	Alunni, Familiari
CATEGORIE	Dati personali	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).
	Destinatari	-
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art. 5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati, Dispositivi antincendio, E' applicata una gestione della password degli utenti, E' applicata una procedura per la gestione degli accessi, E' eseguita la DPIA, E' presenta una politica per la sicurezza e la protezione dei dati, Esistono procedure e disposizioni scritti per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati, Esistono procedure per l'individuazione del custode delle password, I dati sono crittografati, 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 atti anche ad evitare cortocircuiti e possibili incendi, Le password sono costituite da almeno otto caratteri alfanumerici, Le password sono modificate ogni 7 mesi, Le procedure sono riesaminate con cadenza predefinita, Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee, Registrazione e de registrazione degli utenti, Sistemi di allarme e di sorveglianza anti- intrusione, Sono applicate procedure di disaster recovery 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili, Sono utilizzati software antivirus e anti intrusione, Vengono registrati e conservati i Log file, Viene eseguita opportuna manutenzione, L'impianto elettrico è certificato ed a norma	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

AUSILIARI - Titolare del trattamento

Gestione ausiliari		
GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - AUSILIARI
	Date	Creato il 26/01/2023
	Stato	Attivo
	Modalità di gestione	Browser - Java - Lettore PDF - Suite Office e equivalenti, elenchi cartacei.
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Decine
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Area ausiliari
	Autorizzati al trattamento	Tutti gli autorizzati di Area ausiliari
OPERAZIONI	Elementi organigramma	Operazioni
	Area ausiliari	Comunicazione
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione e del merito - MI, Ministero delle economie e delle finanze, Piattaforma nazionale Digital Green Certificate (Pndgc) - Sogei, Portale SIDI, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	Dati relativi agli alunni e famiglie (recapiti telefonici), dati relativi al personale (recapiti telefonici), corrispondenze. (Ai sensi dell'art.5 GDPR, i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali)
	Tipologie	Dati anagrafici, Dati di contatto e foto
CATEGORIE	Interessati	Alunni, Famiglie, Personale
	Dati personali	Dati anagrafici, Dati di contatto e foto
	Destinatari	-
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Dati anagrafici, Dati di contatto e foto	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione, art.5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	Autorizzazione del singolo incaricato al trattamento dati consentito, Ai sensi dell'art.5 GDPR, i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

DDI - Titolare del trattamento

Didattica digitale integrata		
GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - DDI
	Date	Creato il 26/01/2023
	Stato	Attivo
	Modalità di gestione	Browser- Java - Lettore PDF - Live Care: Software di assistenza Remota - Software Gestionale: Axios - Suite Office o equivalenti
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Centinaia
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione, Direttore servizi generali amministrativi, Ufficio alunni, Ufficio protocollo, Didattica, Nucleo Interno di Valutazione, Team Digitale, Ufficio affari generali
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione, Tutti gli autorizzati di Direttore servizi generali amministrativi, Tutti gli autorizzati di Ufficio alunni, Tutti gli autorizzati di Ufficio protocollo, Tutti gli autorizzati di Didattica, Tutti gli autorizzati di Nucleo Interno di Valutazione, Tutti gli autorizzati di Team Digitale, Tutti gli autorizzati di Ufficio affari generali
OPERAZIONI	Elementi organigramma	Operazioni
	Direzione	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Direttore servizi generali amministrativi	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio alunni	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio protocollo	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Didattica	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Nucleo Interno di Valutazione	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Team Digitale	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio affari generali	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione - MI, Ministero delle economie e delle finanze, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	Attività istituzionali della Scuola Gestione amministrativa e didattica dello studente, anche per l'erogazione di servizi aggiuntivi e adempimento degli obblighi previsti dal D.M.)92/2016. Istituzione ed assistenza scolastica (Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale, Esecuzione di un contratto e/o misure precontrattuali)
	Tipologie	Dati di comunicazione elettronica Dati personali protetti dal segreto professionale Disegni, elaborati grafici e opere degli alunni.
	Interessati	Alunni, Familiari

CATEGORIE	Dati personali	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).
	Destinatari	-
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, ufficio scolastico regionale, ambiti territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Sidi, albo online della scuola (solo i dati relativi agli esiti scolastici), Altre strutture del sistema nazionale dell'istruzione, altre P.A., INAIL, azienda sanitaria pubblica competente, società di assicurazione per polizza infortuni, agenzie viaggi (dati personali).	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati ("principio di limitazione della conservazione", art. 5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati, Dispositivi antincendio, E' applicata una gestione della password degli utenti, E' applicata una procedura per la gestione degli accessi, E' eseguita la DPIA, E' presenta una politica per la sicurezza e la protezione dei dati, Esistono procedure e disposizioni scritti per l'individuazione delle modalità con le quali il titolare può assicurare la disponibilità dei dati, Esistono procedure per l'individuazione del custode delle password, I dati sono crittografati, 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 atti anche ad evitare cortocircuiti e possibili incendi, Le password sono costituite da almeno otto caratteri alfanumerici, Le password sono modificate ogni 7 mesi, Le procedure sono riesaminate con cadenza predefinita, Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee, Registrazione e deregistrazione degli utenti, Sistemi di allarme e di sorveglianza anti- intrusione, Sono applicate procedure di disaster recovery 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 presenti istruzioni per la custodia e l'uso dei supporti rimovibili, Sono utilizzati software antivirus e anti intrusione, Vengono registrati e conservati i Log file, Viene eseguita opportuna manutenzione, L'impianto elettrico è certificato ed a norma	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

FORNITORI- Titolare del trattamento

Gestione dei fornitori		
GENERALI	Identificativo	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto" - FORNITORI
	Date	Creato il 26/01/2023
	Stato	Attivo
	Modalità di gestione	Browser- Java - Lettore PDF - Live Care: Software di assistenza Remota - Software Gestionale: Axios - Suite Office o equivalenti
	Frequenza del trattamento	Ogni giorno
	Numerosità dei dati	Decine
	Forma del dato	Digitale e cartacea
	Elementi organigramma	Direzione, Direttore servizi generali amministrativi, Ufficio protocollo, Ufficio acquisti, Ufficio affari generali
	Autorizzati al trattamento	Tutti gli autorizzati di Direzione, Tutti gli autorizzati di Direttore servizi generali amministrativi, Tutti gli autorizzati di Ufficio protocollo, Tutti gli autorizzati di Ufficio acquisti, Tutti gli autorizzati di Ufficio affari generali
OPERAZIONI	Elementi organigramma	Operazioni
	Direzione	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Direttore servizi generali amministrativi	Archiviazione, Cancellazione, Comunicazione, Conservazione, Consultazione, Diffusione, Distruzione, Estrazione, Interconnessione, Limitazione, Modifica, Organizzazione, Raccolta, Raffronto, Registrazione, Strutturazione, Uso
	Ufficio protocollo	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio acquisti	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
	Ufficio affari generali	Comunicazione, Consultazione, Estrazione, Organizzazione, Raccolta, Registrazione, Uso
TITOLARI	I.C. "DevitoFrancesco - Giovanni XXIII - Binetto"	
CONTITOLARI	Ministero dell'Istruzione e del merito - MI, Ministero delle economie e delle finanze, Axios Italia Service Srl, G suite for education	
FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	Finalità	I dati personali da lei forniti saranno trattati per finalità connesse all'esecuzione del contratto di fornitura, compresa l'eventuale fase precontrattuale e, precisamente, inoltrare comunicazioni di vario genere e con diversi mezzi di comunicazione (telefono, telefono cellulare, sms, email, posta cartacea); formulare richieste o evadere richieste pervenute; scambiare informazioni finalizzate all'esecuzione del rapporto contrattuale, ivi comprese le attività per adempiere agli obblighi precontrattuali, contrattuali, fiscali e amministrativi derivanti da rapporti con lei, in essere. Effettuare le operazioni necessarie per l'evasione degli ordini e delle altre richieste, incluso la comunicazione dei dati da lei comunicati, ai terzi, quando necessario per l'adempimento contrattuale; incluso comunicazioni a banca e/o imprese di servizi per adempimenti finanziari collegati ai rapporti contrattuali instaurati. Adempiere a tutte le operazioni imposte dall'applicazione dei Sistemi di Gestione applicati in azienda (ad esempio, secondo UNI EN ISO 9001, ecc.). Adempiere agli obblighi previsti dalla legge, da un regolamento, dalla normativa comunitaria o da un ordine dell'Autorità, tra cui per aspetti Contabili, Fiscali. Prevenire o scoprire attività fraudolente o abusi dannosi. Esercitare i diritti del Titolare, ad esempio il diritto di difesa in giudizio. Avviare e

		gestire transazioni e pratiche risarcitorie in caso di danno e/o sinistri rilevati. I suoi dati potranno essere trattati per finalità interne di statistica e ricerca di mercato. (Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale, Esecuzione di un contratto e/o misure precontrattuali)
	Tipologie	Dati Anagrafici (Azienda o Professionista), identificativi e di recapito. Dati per verifica attività aziendale (DURC, visure camerali, certificato di Casellario Giudiziale e carichi pendenti, accertamenti sulla situazione societaria e personale delle controparti, certificazioni antimafia, offerta economica, verifica regolarità fiscale)
CATEGORIE	Interessati	Fornitori, Banche dati Ministeriali Soggetti Pubblici (ASL, Comune, Provincia, Ufficio scolastico regionale, Ambiti Territoriali, organi di polizia giudiziaria, organi di polizia tributaria, guardia di finanza, magistratura) Altre strutture del sistema della Pubblica Istruzione, altre strutture pubbliche, INAIL, Azienda Sanitaria pubblica competente, Società
		Di Assicurazione per polizza infortuni, Agenzie viaggi (Dati Personali). Autorità di vigilanza e controllo Conservazione del fascicolo (Digitale/Cartaceo) Banche e istituti di credito Organizzazioni sindacali e patronati
	Dati personali	Pubblicazione nelle sezioni ALBO ONLINE o AMMINISTRAZIONE TRASPARENTE dell'istituto
	Destinatari	-
CONSERVAZIONE	In caso di crash, dati disponibili entro	Entro il tempo strettamente necessario per il ripristino del servizio
	Pubblicazione nelle sezioni ALBO ONLINE o AMMINISTRAZIONE TRASPARENTE dell'istituto	I dati raccolti verranno conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (“principio di limitazione della conservazione”, art. 5, GDPR) e/o per il tempo necessario per obblighi di legge. La verifica sulla obsolescenza dei dati conservati in relazione alle finalità per cui sono stati raccolti viene effettuata periodicamente.
TRASFERIMENTI VERSO PAESI TERZI	Questo trattamento non prevede alcun trasferimento verso paesi terzi.	
TRASFERIMENTI VERSO ORGANIZZAZIONI INTERNAZIONALI	Questo trattamento non prevede alcun trasferimento verso organizzazioni internazionali.	
RISCHIO	Medio-Basso	
MISURE TECNICHE E ORGANIZZATIVE	- Autorizzazione del singolo incaricato al trattamento e alla modifica dei dati - Dispositivi antincendio - E' applicata una procedura per la gestione degli accessi - E' presenta 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 - Esistono procedure per l'individuazione del custode delle password - I dati sono crittografati - I documenti vengono firmati digitalmente - Impianto elettrico dotato di misure salvavita atti anche ad evitare cortocircuiti e possibili incendi - 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 - Le password sono modificate ogni 7 mesi - Porte dotate di serratura in tutti i locali contenenti fisicamente le banche dati elettroniche e cartacee - Registrazione e de registrazione degli utenti - Sono applicate regole per la gestione delle password. - Sono applicate procedure di disaster recovery che garantiscono il ripristino dell'accesso ai dati in tempi ridotti - 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. - Sono gestiti i back up - Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili - Le procedure sono riesaminate con cadenza predefinita - Sono utilizzati software antivirus e anti intrusione - Viene eseguita opportuna manutenzione - Vengono registrati e conservati i Log file - E' applicata una gestione della password degli utenti - L'impianto elettrico è certificato ed a norma - Le password sono costituite	

	da almeno otto caratteri alfanumerici	
IMPATTO	Necessita val. impatto	No
	Ultima eseguita il	26/01/2023
	Prossima da eseguire il	26/01/2024

VALUTAZIONE ADEGUATEZZA DELLE MISURE DI SICUREZZA ADOTTATE

MISURE DI SICUREZZA	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, allagamento, attacchi esterni)	Adeguate
E' applicata una gestione della password degli utenti	Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) 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
E' applicata una procedura per la gestione degli accessi	Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate
E' eseguita la DPIA	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
E' presenta una politica per la sicurezza e la protezione dei dati	Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) 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
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
Esistono procedure per l'individuazione del custode delle password	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Adeguate

I dati sono crittografati	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, allagamento, 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 3 mesi	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.)	Parzialmente Adeguate
Le procedure sono riesaminate con cadenza predefinita	Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	Parzialmente Adeguate
L'impianto elettrico è certificato ed a norma	Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) Agenti fisici (incendio, allagamento, attacchi esterni)	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

Registrazione e deregistrazione degli utenti	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.)	Adeguate
Sistemi di allarme e di sorveglianza anti-intrusione	Agenti fisici (incendio, allagamento, attacchi esterni) Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	Adeguate
Sono applicate procedure di disaster recovery 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.	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
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	Eventi naturali (terremoti, eruzioni vulcaniche, ecc.) Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT) Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.) Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Sono presenti istruzioni per la custodia e l'uso dei supporti rimovibili	Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.) Agenti fisici (incendio, allagamento, attacchi esterni)	Adeguate
Sono utilizzati software antivirus e anti intrusione	Compromissione informazioni (intercettazioni, rivelazione	Adeguate

	informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.) Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	
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**
Improbabile	Limitate	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	Basso

PERICOLO		
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)		
RISCHI		
• Perdita • Distruzione non autorizzata		
VALUTAZIONE RISCHIO INTRINSECO		
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	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	Limitate	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	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	Limitate	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	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	Limitate	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	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	Limitate	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	Basso

A valle della DPIA le attività risultano a rischio **Basso**.