

Documento di valutazione dei rischi

dell'I.c. “Santomasi Scacchi”

Gravina in Puglia (BA)

Sommario

Nel presente documento viene sintetizzata e descritta l'attività di **analisi e valutazione dei rischi** che l'Istituto Scolastico ha preliminarmente avviato e portato a conclusione, ai fini della predisposizione del modello organizzativo in materia di protezione dei dati personali.

1 METODOLOGIA DI VALUTAZIONE DEI RISCHI

1.1 Valutazione degli impatti sugli interessati

Per ciascun processo e tipologia di dato trattato deve essere effettuata un'analisi dei possibili **impatti sugli interessati** identificando un valore qualitativo secondo la seguente scala di valutazione:

ID	Impatto	Descrizione
4	Altissimo	Dati particolarmente delicati dal punto di vista della legislazione vigente in materia di privacy (es. dettaglio sullo stato di salute delle persone, abitudini sessuali, problemi di salute, ecc.) o idonei a rivelare aspetti particolarmente intimi della sfera personale di un individuo e/o dei suoi coniugi. Rientrano in tale categoria anche i trattamenti di dati per i quali una loro indisponibilità o violazione dell'integrità potrebbe comportare gravi violazioni per la dignità dell'individuo o rischi per la vita delle persone coinvolte.
3	Alto	Dati delicati dal punto di vista della legislazione vigente in materia di privacy (es. sensibili, biometrici, giudiziari, ecc.) o idonei a rivelare aspetti intimi della sfera personale di un individuo e/o dei suoi coniugi. Rientrano in tale categoria anche i trattamenti di dati per i quali una loro indisponibilità o violazione dell'integrità potrebbe comportare gravi disagi per la vita delle persone coinvolte.
2	Medio	Dati personali il cui impatto in caso di violazione potrebbe avere conseguenze non trascurabili per gli interessati (es. dati anagrafici, dati sulle abitudini, ecc.) sia in termini di riservatezza che di disponibilità ed integrità legate all'impossibilità o alla limitazione per l'erogazione di servizi contrattualizzati con gli stessi interessati
1	Basso	Dati personali in grado di identificare solo per via indiretta l'interessato attraverso id non direttamente riconducibili all'interessato separati da riferimenti anagrafici e di contatto e la cui disponibilità ed integrità non risulta critica per erogare un servizio o processo contrattualizzato

1.2 Valutazione della probabilità di accadimento

Per ciascun processo e tipologia di dato trattato deve altresì essere effettuata un'analisi della **probabilità di accadimento di eventi di rischio sugli interessati** identificando un valore qualitativo secondo la seguente scala di valutazione:

ID	Probabilità	Descrizione
3	Alto	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisi con frequenza pari ad almeno una volta negli ultimi 2 anni, oppure; Assenza di misure di sicurezza di base (es. misure idonee di sicurezza) o mancato adempimento di misure prescritte in apposti provvedimenti in materia di protezione dei dati personali da parte delle Autorità competenti
2	Medio	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisi con frequenza pari ad almeno una volta negli ultimi 5 anni, oppure;

		Presenza di misure di base (es. misure minime, ecc.) ed adempimento di provvedimenti prescrittivi in materia di privacy relativi al trattamento, ma senza ulteriori misure proattive atte a limitare i rischi (es. crittografia, pseudonimizzazione, ...)
1	Basso	Eventi di violazione di aspetti di riservatezza, integrità e disponibilità verificatisi con frequenza pari ad almeno una volta negli ultimi 10 anni, oppure; Presenza di misure di base (es. misure minime, ecc.) ed adempimento di provvedimenti prescrittivi in materia di privacy relativi al trattamento, e di ulteriori misure proattive atte a limitare i rischi (es. crittografia, pseudonimizzazione, ...)

1.3 Valutazione del rischio del processo di trattamento

Dall'incrocio dei parametri di *Impatto* e *Probabilità* sulla base della seguente matrice, si ricava un indice di rischio del processo di trattamento:

Livello di Rischio		Impatto			
		Basso	Medio	Alto	Altissimo
		1	2	3	4
Probabilità	Alto	3	2 - Medio	2 - Medio	3 - Alto
	Medio	2	1 – Basso	2 - Medio	2 - Medio
	Basso	1	1 – Basso	2 - Medio	2 - Medio

I valori di rischio rilevati vanno confrontati con le misure di cui è prevista l'attuazione per contrastare gli eventi potenziali identificati per i diritti e le libertà degli interessati e garantire la *compliance*.

1.4 Valutazione delle misure di trattamento del rischio

Se il valore del sistema di controllo di cui si prevede l'attuazione assume un valore almeno pari alla classe di rischio del processo, si può ritenere che i rischi rilevati siano ragionevolmente sotto controllo ed il processo di trattamento possa essere avviato/continuato.

In caso contrario occorre determinare misure di controllo che consentano di elevare l'efficacia del sistema di controllo.

Di seguito è riportata la scala di valutazione del sistema di misure che si intende adottare:

4 – Misure ad Altissima Efficacia	L'insieme di controlli implementati nell'area di processo sono in linea con le migliori pratiche disponibili sul mercato
3 – Misure ad Alta Efficacia	È presente un sistema di controllo in linea con le buone pratiche organizzative e tecniche mediamente presenti sul mercato e pertanto presenti alcune aree di potenziale vulnerabilità a fronte di minacce evolute (es. attacchi mirati)
2 – Misure ad Efficacia Media	È presente un sistema di controllo minimale, che consente di contrastare le minacce note e derivanti da vulnerabilità ampiamente

	conosciute
1 – Misure inefficaci	Non sono presenti misure di controllo o sono inefficaci per contrastare i rischi rilevati e garantire la conformità del trattamento

2 ANALISI DEI PROCESSI DI TRATTAMENTO

In considerazione dell’attività svolta, i dati abitualmente trattati dall’Istituto Scolastico sono strettamente connessi allo svolgimento della funzione istituzionale e pertanto tali dati riguardano:

- a) Gestione dati dipendenti/collaboratori/consulenti
- b) Gestione dei dati relativi agli alunni e alle loro famiglie
- c) Gestione dati fornitori

Per ogni processo di trattamento nel seguito si è pertanto proceduto a fornire:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l’interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi per i diritti e le libertà degli interessati

Si procederà successivamente alla disamina delle misure per affrontare i rischi attualmente adottate e di quelle da adottare.

2.1 *Gestione dati dipendenti/collaboratori/consulenti nell’ambito rapporto lavorativo e/o di collaborazione*

2.1.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati dei dipendenti - collaboratori - consulenti, di natura personale, sensibile e giudiziaria con lo scopo di dare corretta esecuzione al rapporto di lavoro e/o collaborazione.

L’Istituto Scolastico gestisce tali dati al fine di consentire ai dipendenti/collaboratori/consulenti l’esercizio di tutti i diritti di legge e previsti dai CCNL con riferimento alle funzioni espletate, nella qualità di datore di lavoro, nonché di controllare nei limiti di legge l’attività svolta dai dipendenti. Pertanto il trattamento di tali dati avviene per finalità specifiche, esplicite e legittime e legislativamente e contrattualmente previste.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata del rapporto di lavoro e successivamente all’eventuale risoluzione del rapporto per il tempo previsto dalla normativa fiscale e lavoristica ai fini della prescrizione dei relativi diritti.

L’accesso a tali dati è consentito limitatamente al Dirigente Scolastico, Collaboratori del DS, DSGA e ai soggetti facenti parte dell’unità organizzativa “segreteria”.

2.1.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento di tali dati si fonda sull’esecuzione del contratto di lavoro e/o collaborazione stipulato con la Pubblica Amministrazione.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto contrattuale.

I dati dovrebbero essere trattati per tutta la durata del rapporto di lavoro e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e giuslavoristica ai fini della prescrizione dei relativi diritti.

2.1.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello MEDIO, in quanto l'eventuale violazione o trattamento illecito o indisponibilità potrebbe avere conseguenze non trascurabili per gli interessati sia in termini di riservatezza che di disponibilità ed integrità legate all'impossibilità o alla limitazione per l'erogazione di servizi contrattualizzati con gli stessi interessati.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **MEDIO**.

2.2 Gestione dei dati relativi agli alunni e alle loro famiglie

2.2.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati degli alunni e delle loro famiglie di natura personale, sensibile e giudiziaria con lo scopo di dare corretta esecuzione alla funzione istituzionale svolta dall'Istituzione Scolastica.

L'Istituto Scolastico gestisce tali dati al fine di consentire agli alunni e alle loro famiglie o esercenti la potestà l'esercizio di tutti i diritti di legge connessi all'espletamento della funzione istituzionale educativa e didattica svolta dall'Istituto Scolastico. Pertanto il trattamento di tali dati avviene per finalità specifiche, esplicite e legittime e legislativamente e contrattualmente previste.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata del periodo di iscrizione dell'alunno alla scuola nonché limitatamente all'esecuzione degli obblighi di legge anche successivamente alla fine della frequenza dell'Istituto.

L'accesso a tali dati è consentito limitatamente al Dirigente Scolastico, collaboratori del DS, docenti, DSGA e soggetti facenti parte dell'unità organizzativa "segreteria"

2.2.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento si fonda sugli obblighi di legge connessi all'espletamento della funzione istituzionale.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto istituzionale.

I dati dovrebbero essere trattati per tutta la durata del periodo di iscrizione dell'alunno alla scuola nonché limitatamente all'esecuzione degli obblighi di legge anche successivamente alla fine della frequenza dell'Istituto.

2.2.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello ALTO, in quanto l'eventuale violazione o trattamento illecito o indisponibilità avrebbe la conseguenza di rilevare aspetti intimi della sfera personale di un individuo e/o dei suoi coniugi. Il rischio si potrebbe definire di alto livello poiché in questo caso trattasi di dati non solo di natura comune ma anche di natura sensibile e giudiziaria. Pertanto l'eventuale loro violazione potrebbe comportare danni di rilevante entità in capo agli alunni e anche alle loro famiglie e coniugi, riducendo drasticamente la sfera di libertà personale degli stessi.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **MEDIO**.

2.3 Gestione dati fornitori

2.3.1 Descrizione processo di trattamento

Il trattamento in esame riguarda la gestione dei dati aziendali dei fornitori e personali (identificativi) dei loro rappresentanti legali e referenti ai fini della gestione delle procedure di acquisto di beni e servizi.

L'Istituto Scolastico è pertanto in possesso dei dati identificativi aziendali e personali dei fornitori ai fini della sottoscrizione e gestione del contratto e del rapporto di fornitura anche con riferimento alla verifica e controllo iniziale e periodico dei requisiti di legge per la stipula di contratti con la PA. Pertanto il trattamento di tali dati avviene su base di legge e di contratto per finalità specifiche, esplicite e legittime.

I dati personali sono gestiti su base cartacea e informatizzata e dovrebbero essere trattati per tutta la durata della fornitura e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e tributaria ai fini della prescrizione dei relativi diritti.

L'accesso a tali dati è consentito limitatamente al Dirigente Scolastico, collaboratori del DS, DSGA e soggetti facenti parte dell'unità organizzativa "segreteria".

2.3.2 Necessità e proporzionalità dei trattamenti

La base legale che legittima il trattamento si fonda sull'esecuzione del contratto di fornitura stipulato tra le parti.

I dati raccolti sono adeguati, rilevanti e limitati a quanto è necessario in relazione alle finalità per cui sono stati trattati. I dati sono accurati e costantemente mantenuti aggiornati nell'ambito della gestione del rapporto contrattuale.

I dati dovrebbero essere trattati per tutta la durata della fornitura e successivamente all'eventuale risoluzione del contratto per il tempo previsto dalla normativa fiscale e tributaria ai fini della prescrizione dei relativi diritti.

2.3.3 Valutazione dei rischi per i diritti e le libertà degli interessati (rischio intrinseco)

Nel caso di violazione o illecito trattamento di questa tipologia di dati, l'impatto sugli interessati avrebbe un livello **BASSO** in quanto trattasi di dati di natura comune e coincidenti per la maggior parte con dati di natura pubblica (dati presenti su visure camerali...); pertanto l'eventuale loro violazione non arrecherebbe danni di rilevante entità alle aziende coinvolte.

Considerata anche la non elevata probabilità di accadimento (tenuto conto dei dati storici) e delle misure di sicurezza adottate il rischio intrinseco connesso al processo di trattamento in oggetto è stato nel complesso valutato **BASSO**.

3 INDIVIDUAZIONE DELLE MISURE PER AFFRONTARE I RISCHI

3.1 *Misure fisiche*

Allo stato attuale le misure fisiche adottate sono riconducibili per la gran parte dei trattamenti individuati all'utilizzo di archivi cartacei accessibili ai soli soggetti autorizzati.

Ai fini della *compliance* al GDPR si rende necessaria l'implementazione di una disciplina degli accessi agli archivi, delle forme di protezione da accessi non consentiti e dei tempi di utilizzabilità e conservazione dei dati.

3.2 *Misure informatiche*

Sotto il profilo dell'infrastruttura informatica invece, la stessa risulta sotto il profilo progettuale dotata di sistemi di sicurezza adeguati al trattamento dei dati contenuti.

Ai fini della *compliance* al GDPR si rende necessaria l'implementazione di una serie di *good practices* ai fini della *privacy* e della sicurezza dei dati gestiti.

La politica di accesso alla rete e le comunicazioni da e per la struttura deve essere regolata mediante un accesso condizionato al fine di ridurre il rischio di furti e data breach.

La conservazione dei dati deve essere sia sulle Postazioni di lavoro informatizzate che sui server (operativi e di Backup) protetta al fine di ridurre il rischio di furti e *data breach*.

Deve essere adottata una politica di mantenimento dei dati (*policy backup*) atta a conservare i dati necessari e sottoposti ad obbligatorietà, tutti i dati non necessari devono essere distrutti; tutte le attività di monitoraggio devono essere inserite in apposito registro (*registro dei log*).

Tale gestione impone il rilascio di informativa apposita al personale che deve essere informato dell'eventualità che lo svolgimento di tali attività in abbinamento ai dati di controllo e accesso alle varie applicazioni potrebbe costituire una forma di profilazione e/o controllo a distanza dell'attività dei dipendenti sottoposta alle regole e limitazioni di cui all'art. 4 dello Statuto dei Lavoratori.

Si dovrà tenere un registro delle attività di assistenza tecnica remota e assegnare ad ogni soggetto abilitato al collegamento credenziali specifiche secondo una politica adatta al livello di sicurezza interessato; tutti gli accessi dall'esterno della rete locale dovranno avvenire attraverso l'uso di connessioni protette e criptate e le credenziali devono essere attribuite dall'amministrazione di sistema secondo procedura comunicata alla direzione.

3.3 *Altre misure specifiche GDPR*

Per affrontare i rischi rilevati vengono identificate inoltre le seguenti ulteriori misure in considerazione degli specifici adempimenti introdotti per effetto dell'entrata in vigore del GDPR:

- Provvedere alla **nomina del personale impegnato nel processo ed autorizzato al trattamento** dei dati personali, formalizzando le istruzioni a cui attenersi per il trattamento ei dati personali nell'espletamento delle proprie mansioni;

- Provvedere ad impartire **formazione di base** in maniera documentata e dimostrabile al **personale coinvolto nel processo** sulle corrette modalità di trattamento dei dati personali, con riferimenti a casistiche potenzialmente a rischio;
- **Adozione del registro dei trattamenti, delle procedure di Data breach, del regolamento di utilizzo degli strumenti informatici e del Manuale Privacy.**

Non risulta inoltre essere necessario ricorrere ad una P.I.A. in quanto il GDPR prevede come obbligatoria tale documentazione *“in tutti i casi in cui un trattamento di dati può presentare un rischio elevato per i diritti e le libertà delle persone”*. Alla luce della tipologia dei dati sopra evidenziati e delle ulteriori condizioni individuate dal Regolamento non risulta necessaria la redazione di tale documento.

4 DATA PROTECTION OFFICER

Alla luce delle risultanze del presente Documento di valutazione dei rischi e della tipologia di dati trattati e del rischio connessi al trattamento di tali dati, l’Istituzione scolastica ritiene che sia necessaria la nomina del Data Protection Officer.

Infatti, ai sensi dell’art. 37 del GDPR il DPO, anche detto Responsabile della Protezione dei Dati (RPD), deve essere designato quando:

- a. il trattamento è effettuato da un’autorità pubblica o da un organismo pubblico – eccetto le autorità giurisdizionali;
- b. le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
- c. le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all’articolo 9 o di dati relativi a condanne penali e a reati di cui all’articolo 10.

I trattamenti posti in essere da questa Istituzione Scolastica rientrano nei casi previsti dal GDPR anche alla luce delle linee guida in materia sia del Gruppo di Lavoro Articolo 29 che del Garante per la protezione dei dati personali.

5 AGGIORNAMENTI DEL DOCUMENTO

Il presente Documento di valutazione dei rischi verrà periodicamente aggiornato ogni volta in cui l’organizzazione dell’Istituzione scolastica dovesse subire delle modifiche importanti e radicali nonché ogni volta in cui verranno poste in essere attività che andranno ad incidere in maniera decisiva e importante sulla tipologia dei dati trattati.

In ogni caso annualmente si effettuerà un’attività di controllo delle informazioni contenute nel presente Documento anche al fine di verificare la necessità di modificare eventuali misure di sicurezza adottate.

Il Dirigente
Prof.ssa Rosa De Leo