Conservatorio “San Pier Martire”
Piazza San Felice, 6; 50125, Firenze (FI)
P. IVA 04152730489
Tel.: 055/222457 - Fax: 055/2337723
Email: scuolapiermartire@libero.it

DATA PROTECTION IMPACT ASSESSMENT

D.P.I.A.

Valutazione d'Impatto sulla Protezione dei Dati

Redatto ai sensi e per gli effetti Regolamento UE 2016/679 (GDPR)

Indice

Introduzione

A distanza di diciannove anni dall'entrata in vigore – 8 maggio 1997 – della prima legge italiana in materia di privacy, lo scorso 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale Europea il Regolamento UE n. 2016/679 (da ora in vanti, nominato come GDPR), il quale entrerà in vigore il prossimo 25 maggio.
Tale GDPR si inserisce all'interno di quello che, insieme alla Direttiva 2016/680, è stato definito il "Pacchetto europeo protezione dati".

Gli Stati membri ad ogni modo, sebbene il GDPR, in quanto tale, non abbia bisogno di recepimento, hanno due anni per adeguare le proprie normative interne nonché, le aziende, per essere sensibilizzate alle novità introdotte.
Ciò, anche in considerazione del fatto che il GDPR attribuisce alla Commissione europea il potere di adottare atti delegati e di esecuzione, al fine di rendere operativa la disciplina, ma lascia ai legislatori nazionali la facoltà di introdurre, a seconda delle circostanze, norme nazionali ad hoc.

Le novità introdotte con il GDPR riguarderanno, dal punto di vista delle aziende (i c.d. "titolari" del trattamento dei dati personali) tutte quelle che – salvo qualche eccezione, una in particolare di cui si dirà tra breve, relativamente alle aziende medio e piccole – avendo uno stabilimento all'interno dell'UE, trattano dati personali, indipendentemente dal fatto che il trattamento sia effettuato nell'UE stessa.
Dal punto di vista, invece, delle persone fisiche – i c.d. "interessati" al trattamento dei propri dati – la nuova normativa si applicherà a tutti i soggetti presenti nell'UE anche quando, sebbene l'azienda titolare del trattamento non abbia uno stabilimento in territorio UE, il trattamento stesso riguardi l'offerta di beni o la prestazione di servizi ai soggetti interessati o il monitoraggio del loro comportamento, nella misura in cui tale comportamento abbia luogo all'interno dell'UE.

Tra le prime novità di maggior rilievo, merita sicuramente attenzione particolare una nuova figura – e professionalità – che va ad affiancarsi alla nomenclatura già conosciuta nel nostro Codice Privacy, ovvero al "titolare", al "responsabile" e all' "incaricato" del trattamento dei dati.
Tale nuova figura è quella del c.d. Data Protection Officer (“DPO”, che nel presente documento verrà nominato come Responsabile della Protezione dei Dati (“RDP”).
Il RDP dovrà essere obbligatoriamente presente all'interno di tutte le aziende pubbliche nonché in tutte quelle ove i trattamenti presentino specifici rischi, come ad esempio le aziende nelle quali sia richiesto un monitoraggio regolare e sistematico degli "interessati", su larga scala, e quelle che trattano i c.d. "dati sensibili".
Le società facenti parte di uno stesso gruppo, a livello nazionale o transfrontaliero, potranno nominare un unico RDP, a condizione che lo stesso sia facilmente raggiungibile da ciascuna società del gruppo stesso.
Il RDP, inoltre, potrà essere un dipendente della società Titolare del Trattamento o, in alternativa, assolvere i propri compiti in base ad un contratto di servizi. Ad ogni modo, ogni azienda dovrà rendere noti i dati del proprio RDP – il quale dovrà essere contattabile da tutti i soggetti "interessati" – nonché comunicarli al locale "Garante per la protezione dei dati personali".

Altra novità di rilievo, è l'introduzione dell'obbligo, per ogni azienda Titolare del Trattamento dei dati, di tenere un "registro delle attività di trattamento", svolte sotto la propria responsabilità, nonché quello di effettuare una "valutazione di impatto sulla protezione dei dati".
Quest'ultimo adempimento, in particolare, è richiesto ad esempio in relazione ai trattamenti automatizzati, ivi compresa la profilazione, o con riguardo ai trattamenti su larga scala di categorie particolari di dati (sensibili), nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico. Sarà ad ogni modo il Garante Privacy (per quanto riguarda l'Italia), a redigere e rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della "valutazione di impatto sulla protezione dei dati".

Per chiudere sul punto, si rileva come (ed ecco l'eccezione cui si è fatto riferimento in apertura) il comma 5 dell'art. 30 del GDPR esoneri dagli adempimenti appena accennati le piccole e medie imprese, quelle dunque con meno di 250 dipendenti, a meno che, però, "…il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati (sensibili)…o i dati personali relativi a condanne penali…" (si vedrà come sarà interpretato ed applicato tale articolo, nella prassi).

Ancora, andando a concludere, il GDPR:

- riconosce espressamente il "diritto all'oblio", ovvero la possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non più necessari per le finalità per le quali sono stati raccolti, nel caso di revoca del consenso o quando si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al GDPR;
- stabilisce il diritto alla "portabilità dei dati", in virtù del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un Titolare del Trattamento e ha il diritto di trasmettere tali dati a un altro Titolare del Trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto;
- sancisce il principio di "accountability", per cui il titolare dovrà dimostrare l'adozione di politiche privacy e misure adeguate in conformità al GDPR;
- introduce il principio della "privacy by design" (dal quale discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento) nonché quello della "privacy by default" (che ricalca il principio di necessità di cui all'attuale disciplina, stabilendo che i dati vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini).

Infine, per quanto concerne il "sistema sanzionatorio", il GDPR ha aumentato l'ammontare delle sanzioni amministrative pecuniarie, che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo, lasciando peraltro ciascuno Stato membro libero di adottare norme relative ad altre sanzioni.

Normativa di Riferimento

- Reg. UE 2016/679 (GDPR): "*relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*"
- Linee guida WP 248 rev.01, modificate e adottate da ultimo il 4 ottobre 2017: *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679"*

Finalità del Documento

Il presente Documento di Valutazione d'Impatto sulla Protezione dei Dati – da ora in avanti nominata come DPIA – è stato redatto ai sensi dell'Art. 35 del GDPR, paragrafo 1, secondo il quale:

> *Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.*

Il DPIA assume dunque la connotazione di documento programmatico, inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione, in quanto sostengono i Titolari del Trattamento non soltanto nel rispettare i requisiti del GDPR, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento stesso (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità al GDPR.

Metodi di Valutazione e Redazione DPIA

Il presente DPIA è stato redatto sulla base delle disposizioni normative del GDPR, nonché seguendo le indicazioni fornite nelle Linee guida WP 248 rev.01, modificate e adottate da ultimo il 4 ottobre 2017: *"Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679"*.

La valutazione, attraverso cui è stata effettuata la raccolta delle informazioni necessarie alla redazione del DPIA, è stata invece eseguita in sede di sopralluogo presso l'azienda oggetto del trattamento dei dati, alla presenza del Titolare e dei Responsabili del Trattamento, nonché di un consulente esterno in possesso delle conoscenze in materia di protezione dei dati personali: la raccolta delle informazioni riguardanti il trattamento, è stata svolta mediante utilizzo del software PIA, creato dall'Autorità Francese per la Protezione dei Dati (CNIL), fornito dal suddetto consulente esterno.

Gruppo di Lavoro

Il presente DPIA, come specificato poc'anzi, è stato predisposto dal seguente gruppo di lavoro:

Nome, Cognome	Ruolo aziendale	Ruolo ai fini della privacy
Agnese Carpitelli	Responsabile amministrativa del "Conservatorio San Pier Martire"	Incaricata interno al Trattamento dei dati presso l'Istituto
Alessio Gini	Consulente Esterno	———

Al termine dei lavori il Titolare/Responsabile del Trattamento, valutato il livello di conoscenza specialistica e delle competenze richieste dall'art. 37, par. 5, del GDPR, per la nomina a RPD, e non si trova in situazioni di conflitto di interesse con la posizione da ricoprire e i compiti e le funzioni da espletare, predisposto la nomina del consulente presente in sede di sopralluogo valutativo quale RPD dell'azienda.

Copia del presente documento, compresi gli allegati, è disponibile presso la sede legale dell'azienda, conservato dai Titolare/Responsabile del Trattamento: quest'ultimo, insieme al RDP, ne cureranno i futuri aggiornamenti.

Identificazione dell'Azienda

Il "Conservatorio San Pier Martire" - da ora in avanti nominato sono come "Istituto" - sito in Piazza San Felice n° 6 a Firenze (FI), si configura come scuola privata paritaria volta all'istruzione elementare primaria: essa, essendo inserita nel sistema nazionale di istruzione, svolge un servizio pubblico, la cui regolare frequentazione costituisce assolvimento dell'obbligo di istruzione, al pari della scuola pubblica propriamente detta.

Difatti, il riconoscimento della parità garantisce:

- l'equiparazione dei diritti e dei doveri degli studenti;
- le medesime modalità di svolgimento degli esami di Stato;
- l'abilitazione a rilasciare titoli di studio aventi lo stesso valore legale delle scuole statali.

Tale riconoscimento risulta vincolante al fatto che l'Istituto si attenga ai programmi e codici di condotta, disposizioni e direttive, rispettivamente elaborati ed emanate dal Ministero dell'Istruzione dell'Università e della Ricerca (da ora in avanti, menzionato come MIUR).

Dati Aziendali

Denominazione	Conservatorio “San Pier Martire”
C.F. e P. IVA	04152730489
Sede Legale	Piazza San Felice, 6; 50125, Firenze (FI)
Telefono	055/222457
Fax	055/2337723
E-mail	scuolapiermartire@libero.it

Organigramma ai fini della Privacy

Nome, Cognome	Ruolo aziendale	Ruolo ai fini della privacy	Firma
Avv. Francesco Casini	Legale Rappresentante del “Conservatorio San Pier Martire”	Titolare del Trattamento	
Giuseppina Angotti	Coordinatrice didattica del “Conservatorio San Pier Martire”	Delegata Responsabile interno del Trattamento locale dei dati presso l’Istituto	
Agnese Carpitelli	Responsabile amministrativa del “Conservatorio San Pier Martire”	Incaricata interno del Trattamento dei dati presso l’Istituto	
Maria Gambioli	Insegnante del “Conservatorio San Pier Martire”	Incaricata interno del Trattamento dei dati presso l’Istituto	
Silvia Giuliani	Insegnante del “Conservatorio San Pier Martire”	Incaricata interno del Trattamento dei dati presso l’Istituto	
Karia Mainardi	Insegnante del “Conservatorio San Pier Martire”	Incaricata interno del Trattamento dei dati presso l’Istituto	
Gloria Perrone	Insegnante del “Conservatorio San Pier Martire”	Incaricata interno del Trattamento dei dati presso l’Istituto	

Nome, Cognome	Ruolo aziendale	Ruolo ai fini della privacy	Firma
Elisabetta Rosso	Insegnante del "Conservatorio San Pier Martire"	Incaricata interno del Trattamento dei dati presso l'Istituto	
Costanza Bertelli	Insegnante del "Conservatorio San Pier Martire"	Incaricata interno del Trattamento dei dati presso l'Istituto	
Angela Cerrini	Insegnante del "Conservatorio San Pier Martire"	Incaricata interno del Trattamento dei dati presso l'Istituto	
Pasqualina Assunta Lariccia	Insegnante del "Conservatorio San Pier Martire"	Incaricata interno del Trattamento dei dati presso l'Istituto	
Michela Terrazzani	Insegnante del "Conservatorio San Pier Martire"	Incaricata interno del Trattamento dei dati presso l'Istituto	
Dott.Alessio Gini	Consulente Esterno	Responsabile Protezione dei Dati (RDP)	

Sia il RDP, che gli Incaricati al Trattamento dei dati personali, vengono investiti di tale ruolo mediante apposita lettera di incarico da parte del Titolare del Trattamento. Copia di tali nomine, sono allegate al presente documento.

Dati di Contatto RDP

Nome e Cognome	Dott. Alessio Gini
C.F.	GNILSS87M30G843Q
Sede Legale	Via Ugo Foscolo, 17; 56025, Pontedera (PI)
Telefono	333/4661393
E-mail	gini.alessio@gmail.com
PEC	gini.alessio@pec.it

Identificazione del Trattamento

Il "Conservatorio San Pier Martire" viene a svolgere la raccolta, il trattamento, l'archiviazione e, quando richiesto, la trasmissione di una variegata tipologia di dati.
Di seguito vengono riportate schede esemplificative di tutti le informazioni gestite all'interno dell'istituto, ciascuna delle quali corredate da esplicazione di specifica finalità, necessità e legittimità di trattamento:

Scheda n°1

Trattamento:
Iscrizione Studenti all'Anno Scolastico di riferimento

Interessati al trattamento:
Genitori degli studenti

Scopo del trattamento:
Corretta iscrizione dello studente all'anno scolastico di riferimento

Dati trattati:

Identificazione dei genitori: nome, cognome, indirizzo postale, numeri di telefono, e-mail

Caratteristiche personali dei genitori: data e luogo di nascita, sesso, nazionalità, cod. fisc.

Identificazione dello studente: nome, cognome, indirizzo postale

Caratteristiche personali dello studente: data e luogo di nascita, sesso, nazionalità, dati di natura clinico - sanitari (allergie, intolleranze alimentari, dismetabolismi), posizione personale in relazione all'esercizio del diritto di avvalersi o meno dell'insegnamento della religione cattolica

Caratteristiche personali dello studente **possibilmente richieste**: dati di natura clinico - sanitari (condizioni patologiche per lo status di salute psico - fisico del bambino, posizione personale in relazione all'asservimento a vaccinazioni obbligatorie)

Responsabile interno all'istituto della raccolta, del trattamento e della archiviazione dei dati:

Sig.ra Giuseppina Angotti

Scheda n°2

Trattamento:

Emissioni Compensi

Interessati al trattamento:

Dipendenti e personale operativo

Scopo del trattamento:

Gestione del rapporto di lavoro con i dipendenti e il personale operativo

Dati trattati:

Identificazione:	nome, cognome, indirizzo postale, numeri di telefono, e-mail
Caratteristiche personali:	data e luogo di nascita, età, sesso, nazionalità, cod. fisc., stato civile, dati bancari (per il pagamento diretto dei compensi), istituto giuridico, eventuali disposizioni civili/giuridiche pendenti

Responsabile interno all'istituto della raccolta, del trattamento e della archiviazione dei dati:

Sig.ra Giuseppina Angotti

Responsabile esterno a cui i dati personali vengono comunicati dal suddetto personale, per elaborazione buste paghe:

AGIDAE;
Via Bellini, 10; 00198 Roma (RM)

Scheda n°2 bis

Trattamento:

Emissione attestati formativi

Interessati al trattamento:

Dipendenti e personale operativo

Scopo del trattamento:

Corretta emissione di documentazione attestante la partecipazione del personale ai percorsi informativi e formativi organizzati dal Datore di Lavoro.

Dati trattati:

Identificazione: nome, cognome

Caratteristiche personali: data e luogo di nascita, età, sesso, nazionalità, cod. fisc.

Responsabile interno all'istituto della raccolta, del trattamento e della archiviazione dei dati:

Sig.ra Giuseppina Angotti

Scheda n°3

Trattamento:

Acquisti e gestione fornitori

Interessati al trattamento:

Fornitori e Servizi di Assistenza
(Manutentori, Fornitori materiale scolastico, Manutentori attrezzature informatiche)

Scopo del trattamento:

Emissione ricevute di corrispettivo

Dati trattati:

Identificazione: ragione sociale, sede legale, partita IVA e/o Codice Fiscale

Responsabile interno all'istituto della raccolta, del trattamento e della archiviazione dei dati:

Sig.ra Giuseppina Angotti

Scheda n°4

Trattamento:

Stipula contratti di affitto

Interessati al trattamento:

Locatario

Scopo del trattamento:

Corretta stipula di contratti di affitto di immobili

Dati trattati:

Identificazione:	nome, cognome, numeri di telefono, e-mail
Caratteristiche personali:	data e luogo di nascita, età, sesso, nazionalità, cod. fisc., stato civile, istituto giuridico

Responsabile interno all'istituto della raccolta dei dati:

Sig.ra Giuseppina Angotti

Responsabile esterno a cui i dati personali vengono comunicati dal suddetto personale, per elaborazione contratti di affitto:

Architetto Giuseppe Pancino
Via di Peretola, 143; 50145 Firenze (FI)

Scheda n°1

Modalità di raccolta, trattamento dei dati e archiviazione dei dati

I dati vengono forniti all'Istituto direttamente dagli interessati, al momento dell'iscrizione del bambino all'anno scolastico, mediante compilazione di apposito modulo "domanda di iscrizione".

I dati, una volta raccolti, vengono poi inseriti all'interno della piattaforma online delle Segreterie Comunali, al fine di verificare la bontà e la veridicità dei dati forniti e, conseguentemente, completare la procedura di iscrizione dello studente.

Verificata la effettiva iscrizione dell'alunno sulla piattaforma online delle Segreterie Comunali, i dati personali degli studenti vengo forniti sia al personale docente, sia al personale operante nel refettorio dell'Istituto (Addetti alla cucina e Addetti allo sporzionamento)

I dati vengono conservati per una durata stabilita dal MIUR, secondo apposito tabellario ("massimario di scarto"). Copia di tale tabellario, dovrà essere allegata al presente documento.

In azienda i dati sono conservati sia in forma cartacea che elettronica.

Finalità, Necessità e Legittimità dei dati

La raccolta, il trattamento e la detenzione dei dati trattati nel presente documento, si basano su principi di ovvia legittimità da parte dell'Istituto, giacché indispensabili non solo per la corretta iscrizione dello studente all'anno scolastico, ma anche per la conoscenza dei bambini che accedono al servizio di istruzione, nonché del proprio nucleo familiare, al fine di ridurre al minimo eventuali situazioni di disagio nei confronti di quest'ultimi.

La stessa raccolta, trattamento, detenzione e trasmissione dei dati dei propri iscritti e del proprio nucleo familiare, viene legittimata dalle specifiche disposizioni del MIUR, nonché da circolari emanate dal Provveditorato allo Studio e dal Piano Triennale di Offerta Formativa (PTOF).

Lo stesso modulo "domanda di iscrizione", consegnato ai genitori, contiene un'informativa redatta in maniera chiara, semplice e comprensibile, mediante la quale gli stessi legittimano il trattamento dei dati propri e dei figli e al loro inserimento sui portali istituzionali.

Scheda n°2

Modalità di raccolta e trattamento dei dati

I dati vengono forniti all'Istituto, direttamente dagli interessati al momento della loro assunzione, mediante apposito modulo di richiesta inserimento dati personali.

I dati vengono conservati per tutta la durata del rapporto lavorativo e sino alla scadenza prevista dalla normativa fiscale e del lavoro.

In azienda i dati sono conservati sia in forma cartacea che elettronica.

Finalità, Necessità e Legittimità dei dati

La raccolta, il trattamento e la detenzione dei dati trattati nel presente documento, si basano su principi di ovvia legittimità da parte dell'Istituto, giacché indispensabili per la stipula di contratti di lavoro, corretta emissione delle buste paga e rendicontazione compensi da parte di soggetto terzo, identificato alla relativa Scheda n° 2.

Lo stesso modulo di richiesta inserimento dati personali, consegnata al personale operativo, contiene un'informativa redatta in maniera chiara, semplice e comprensibile, mediante la quale i lavoratori legittimano il trattamento dei propri dati e la loro successiva trasmissione al soggetto terzo responsabile della emissione della documentazione sopra indicata.
Il numero dei dati personali elaborati è il minimo per poter emettere la busta paga.
Il lavoratore è tenuto ad informare il Titolare e il Responsabile del Trattamento nel momento in cui i propri dati debbano essere rettificati.

Scheda n°2 bis

Modalità di raccolta e trattamento dei dati

I dati vengono forniti all'Istituto, direttamente dagli interessati, mediante apposito registri formativi.

I dati vengono conservati per tutta la durata del rapporto lavorativo.

In azienda i dati sono conservati sia in forma cartacea (registri formativi) che elettronica (attestati in formato digitale).

Finalità, Necessità e Legittimità dei dati

La raccolta, il trattamento e la detenzione dei dati trattati nel presente documento, si basano su principi di ovvia legittimità da parte dell'Istituto, giacché indispensabili per la corretta emissione di documentazione attestante la partecipazione degli interessati ai percorsi informativi e formativi nonché di aggiornamento periodico obbligatori, stilati dal Datore di Lavoro dell'Istituto.

Lo stesso registro formativo, consegnato al personale operativo al momento dell'effettuazione dei percorsi informativi e formativi nonché di aggiornamento periodico obbligatori, contiene un'informativa redatta in maniera chiara, semplice e comprensibile, mediante la quale i lavoratori legittimano il trattamento dei propri dati e la loro successiva elaborazione per il rilascio della documentazione sopra indicata.
Il numero dei dati personali elaborati è il minimo per poter emettere gli attestati formativi.
Il lavoratore è tenuto ad informare il Titolare e il Responsabile del Trattamento nel momento in cui i propri dati debbano essere rettificati.

Scheda n°3

Modalità di raccolta e trattamento dei dati

I dati vengono forniti all'Istituto, direttamente dai fornitori al momento che si instaura il rapporto commerciale.

I dati non vengono trattati, ma solo conservati per tutta la durata del rapporto commerciale e sino alla scadenza prevista dalla normativa fiscale.

In azienda, i dati sono conservati in forma cartacea.

Finalità, Necessità e Legittimità dei dati

La raccolta e la detenzione dei dati trattati nel presente documento, si basano su principi di ovvia legittimità da parte dell'Istituto, giacché indispensabili per la emissione di ricevute compensi da parte del personale amministrativo dell'Istituto.

Il numero dei dati elaborati è il minimo per mettere in condizione il personale amministrativo interno di elaborare ed emettere ricevute compensi.
Il fornitore è tenuto ad informare il Titolare e il Responsabile del Trattamento nel momento in cui i propri dati debbano essere rettificati.

Scheda n°4

Modalità di raccolta e trattamento dei dati

I dati vengono forniti all'Istituto, direttamente dagli interessati, al momento della stipula del contratto di affitto degli immobili intestati all'Istituto.

I dati vengono solamente raccolti dall'Istituto; il trattamento e l'archiviazione dei dati invece viene svolta, per tutta la durata del rapporto di locazione, da soggetto terzo identificato alla relativa Scheda n° 4.

In azienda i dati vengono raccolti in sola forma cartacea.

Finalità, Necessità e Legittimità dei dati

La raccolta, il trattamento e la detenzione dei dati trattati nel presente documento, si basano su principi di ovvia legittimità da parte dell'Istituto, giacché indispensabili per la stipula di contratti di affitto da parte di soggetto terzo, identificato alla relativa Scheda n° 4.

Lo stesso contratto di affitto, consegnata al locatore, contiene un'informativa redatta in maniera chiara, semplice e comprensibile, mediante la quale i quest'ultimo legittima il trattamento dei propri dati e la loro successiva trasmissione da parte di soggetto terzo responsabile della emissione della documentazione sopra indicata.
Il numero dei dati personali elaborati è il minimo per poter stipulare contratti di locazione.
L'interessato è tenuto ad informare il Titolare e il Responsabile del Trattamento nel momento in cui i propri dati debbano essere rettificati.

Diritti degli Interessati

Il GDPR, al capo III, esamina le modalità per l'esercizio dei diritti dell'interessato al trattamento, ossia della persona fisica a cui si riferiscono i dati personali.

Inoltre, in base a quanto definito dal Considerando n° 39 della suddetta normativa comunitaria:

- "*Dovrebbero essere trasparenti, per le persone fisiche, le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati*";
- "*Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro*";
- "*È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento*";
- "*Le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali*":
- "*I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento*".

A conferma di quanto enunciato finora, si riporta di seguito una tabella esplicativa delle modalità di esercizio che dovranno essere messe in atto nell'azienda "Studio Deri", al fine di permettere il rispetto dei diritti degli interessati al trattamento dei propri dati, così come sancito dal GDPR:

Diritti dell'interessato	Modalità di richiesta da parte dell'interessato	Modalità di esercizio	Presenza di procedura operativa per il personale incaricato
Informazione sul trattamento dei propri dati	———	Informativa sulla legittimità, necessità e proporzionalità dei dati richiesti in apposito contratto/mandato di incarico di trattamento, consegnato e controfirmato dai clienti all'atto della sua stipula	X
Accesso ai dati	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Fornitura all'interessato delle informazioni richieste in forma scritta, anche attraverso strumenti elettronici, entro 30 giorni dal recepimento della richiesta di accesso	X
Rettifica dei dati	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Comunicazione in forma scritta, anche attraverso strumenti elettronici, della modifiche e/o integrazioni apportate, senza ingiustificato ritardo	X
Cancellazione dei dati ("*Diritto all'oblio*")	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Comunicazione in forma scritta, anche attraverso strumenti elettronici, della cancellazione dei dati richiesti, senza ingiustificato ritardo	X

Diritti dell'interessato	Modalità di richiesta da parte dell'interessato	Modalità di esercizio	Presenza di procedura operativa per il personale incaricato
Limitazione del trattamento*	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Comunicazione in forma scritta, anche attraverso strumenti elettronici, della limitazione dei dati richiesti, senza ingiustificato ritardo	X
Portabilità dei dati**	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Consegna delle copie originali dei dati richiesti, le quali risultano accompagnate da apposita comunicazione in forma scritta, anche attraverso strumenti elettronici, della avvenuta consegna del materiale richiesto	X
Opposizione al trattamento***	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Comunicazione in forma scritta, anche attraverso strumenti elettronici, dell'arresto alle metodiche di trattamento dei dati dell'interessato	X
Protezione dei dati in caso di trasferimento in Paese Extra UE	Richiesta in forma scritta, anche attraverso strumenti elettronici, al fine del successivo inserimento della stessa nel relativo registro di protocollo	Invio al futuro destinatario e responsabile del trattamento dei dati, mediante appositi mezzi muniti di tracciabilità che assicurino il più alto grado di protezione dei dati.	_____

**N.B.: Con il Regolamento UE 2016/679, l'interessato, ha, infatti, il diritto di ottenere dal titolare un trattamento limitato dei propri dati quando contesta l'esattezza dei dati personali; quando il trattamento è illecito e se l'interessato si è opposto al trattamento, ai sensi dell'articolo 21, paragrafo 1, del Regolamento UE 2016/679, in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento o dei diritti dell'interessato. Inoltre, il diritto di limitazione può essere invocato nel caso in cui il titolare del trattamento non abbia più necessità di conservare i dati ai fini del trattamento, ma questi possono essere necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Quindi, se il trattamento è limitato, i dati personali dell'interessato sono trattati, esclusa la conservazione, solo con il suo consenso. La limitazione può essere revocata e, in tal caso, il titolare del trattamento deve informarne il soggetto interessato.*

***N.B.: Il diritto alla portabilità dei dati consente all'interessato di ricevere i dati personali che lo riguardano forniti a un titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico, in modo che possa trasmetterli a un altro titolare del trattamento senza impedimenti da parte del titolare a cui li ha forniti. L'esercizio del diritto alla portabilità non deve ledere i diritti e le libertà altrui. Sono portabili i dati personali che si riferiscono all'interessato. Sono, quindi, esclusi i dati anonimi. Per essere portabili i dati devono essere trattati attraverso strumenti automatizzati. Sono quindi esclusi gli archivi e registri cartacei. Sono, inoltre, portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato. I dati devono essere stati forniti consapevolmente e in modo attivo dall'interessato (quali ad esempio, i dati di registrazione inseriti compilando un modulo online, ossia nome utente, età, indirizzo email, ecc.).*

****N.B.: L'articolo 21 del Regolamento UE 2016/679, ha disciplinato il diritto all'opposizione del trattamento, il quale per definizione consente all'interessato di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano. Qualora i dati personali siano trattati a fini di ricerca scientifica o storica, l'interessato ha il diritto di opporsi al trattamento dei dati personali che lo riguardano, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico (l'articolo 21, paragrafo 6).*

Locali, strumenti e standard utilizzati per il trattamento e archiviazione dei dati

Il trattamento dei dati raccolti, viene svolto all'interno di diversi locali, in base all tipologia dei dati degli interessati:

- **Locale segreteria amministrativa:** *tutti i dati riportati nelle varie nelle schede nella sezione "Identificazione del Trattamento";*
- **Locale segreteria scolastica:** *dati riportati nella scheda n°1 nella sezione "Identificazione del Trattamento";*
- **Refettorio:** *specifici dati riportati nella scheda n°1 nella sezione "Identificazione del Trattamento" (allergie, intolleranze alimentari, dismetabolismi);*
- **Aule:** *dati riportati nella scheda n°1 nella sezione "Identificazione del Trattamento";*

Anche la conservazione dei dati raccolti viene svolta nei medesimi locali sopra riportati, con la sola esclusione del **refettorio**.

Le attività di trattamento ed archiviazione dei dati raccolti, avvengono sia mediante l'utilizzo di postazioni informatiche, sia mediante archivio cartaceo.

L'archiviazione in formato cartaceo viene svolta esclusivamente nel **Locale segreteria amministrativa** e nel **Locale segreteria scolastica**. Il *trattamento* mediante supporti informatici invece, avviene come di seguito indicato:

Supporti informatici utilizzati per il Trattamento

1. N° 2 PC, muniti di sistema operativo Microsoft Windows, nel **Locale segreteria amministrativa**;
2. Tablet muniti di registro elettronico, nelle **Aule didattiche.**

Supporti informatici utilizzati per la Conservazione

1. N° 2 PC, muniti di sistema operativo Microsoft Windows, nel **Locale segreteria amministrativa**;

La raccolta, trattamento e conservazione dei dati viene esercitata in maniera molto accurata da parte sia del Responsabile del Trattamento degli stessi, sia del suo Incaricato, i quali provvedono:

- alla verifica dei dati inseriti dagli interessati, così da poter contattare questi ultimi in caso di errata compilazione e/o assente fornitura dei dati richiesti;
- all'archiviazione della documentazione raccolta, scansionandola e catalogandola, per anno scolastico, in singole cartelle personali per ogni fornitore e personale operativo;

- all'aggiornamento dei dati archiviati, mediante campagna informativa periodica con i fornitori e il personale operativo e/o ogniqualvolta questi ultimi ne diano tempestiva comunicazione alla segreteria didattica.

Archivio cartaceo

In azienda sono presenti vari archivi cartacei, rappresentati da cartolari, fascicoli e raccoglitori riposti in appositi arredi da interni.

Le modalità di conservazione dei dati dei vari interessati, si basa principalmente su procedure operative elaborate internamente all'Istituto, sulla base dei principi di praticità di catalogazione, nonché di celerità di reperimento della varia documentazione.

Al momento della presente valutazione, il MIUR non ha infatti concesso la fornitura di alcuna linea guida in fatto di trattamento e archiviazione del GDPR nel campo scolastico, ma si è limitato alla emanazione di una nota ministeriale (nota 0000563 del 22 maggio 2018), avente l'unico obiettivo di fornire le prime indicazioni per la nomina obbligatoria del Responsabile della protezione dei dati personali negli istituti di istruzione.
Per questo motivo, non è possibile definire uno standard né particolari certificazioni riconosciute ai fini del trattamento e protezione dei dati, ma solamente adeguare tali fasi al solo GDPR, interpretato nel caso concreto del settore delle istituzioni scolastiche, nonché a regolamenti di "buona prassi di lavorazione" elaborati internamente nei singoli istituti.

Valutazione dei Rischi

Il GDPR ha introdotto un un approccio basato sulla valutazione del rischio (*risk based*), attraverso la quale si determina la misura di responsabilità del Titolare o del Responsabile del Trattamento, tenendo conto della natura, della portata, del contesto e delle finalità del trattamento, nonché della probabilità e della gravità dei rischi per i diritti e le libertà degli utenti.

Il Considerando 75 del suddetto Regolamento, viene da dare specifico riferimento al concetto di rischio:

"*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare:*

- *se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo;*
- *se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano;*
- *se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza;*
- *in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali;*
- *se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*".

Il presente documento, si prefigge dunque l'obiettivo di un'analisi dei vari rischi che possono essere presenti nella trattamento dei dati personali all'interno dell'azienda "Studio Deri", ma anche di valutare le misure tecniche od organizzative che il titolare ritiene di dover adottare per ridurre l'eventuale rischio.

Si delineano dunque i possibili rischi che possono verificarsi nel corso di un trattamento di dati personali all'interno dell'Istituto, andando altresì ad individuare la loro ipotizzabile gravità in caso di accadimento:

Accesso illegittimo ai dati degli interessati (A.I)

Impatto sui soggetti interessati	Principali minacce	Fonti di rischio	Gravità di danno ipotizzabile	Probabilità di accadimento evento
Pedofilia, Estorsione verso i genitori, Sequestro di persona (genitore), Sequestro di persona minorile (studente), Atti persecutori, Stalking	Persone estranee, Pirati informatici, Personale interno (fuga di dati occasionali o involontari)	Fonti umane esterne, Malware, Phishing, Fonti umane interne	Limitata	Limitata

"Errore Umano" durante raccolta dati (E.U.)

Impatto sui soggetti interessati	Principali minacce	Fonti di rischio	Gravità di danno ipotizzabile	Probabilità di accadimento evento
Rallentamento nella celere erogazione dei servizi offerti dall'Istituto	Personale interno	Fonti umane interne	Limitata	Limitata

Piano d'Azione: Misure esistenti, pianificate e correttive da implementare

Una volta evidenziati i rischi presenti nel corso del trattamento di dati personali all'interno dell'Istituto, si è provveduto ad individuare le principali misure, già esistenti e pianificate dal Titolare del trattamento, volte alla gestione degli scenari appena descritti:

Misura esistente/pianificata	Spiegazione
Criptografia dei dati	I dati trattati vengono archiviati a cura del Responsabile segreteria didattica, su diretto incarico da parte del Titolare del Trattamento. L'archiviazione, si articola in due modalità, per ciascuna delle quali vengono applicate due differenti tipologie di crittografia: ❖ **Archiviazione su PC**: i dati vengono salvati nella memoria interna della postazione informatica sotto forma di file, al quale viene attribuita specifica denominazione, conosciuta solamente dal Responsabile segreteria amministrativa (incaricata dell'inserimento nell'archivio informatico). I singoli file vengono poi inseriti in cartelle e sottocartelle, i cui livelli di archiviazione vengono autonomamente scelti dal Responsabile segreteria amministrativa (incaricata dell'inserimento nell'archivio informatico). Gli stessi archivi vengono poi duplicati all'interno di hard disk esterno. ❖ **Archivio cartaceo**: i dati vengono raccolti in raccoglitori, cartelline, faldoni, creati appositamente per ogni singolo studente, inserendo attestazioni di merito e profitto, certificati medici, richieste ufficiali presentate dai genitori, ecc. Ad ogni singolo raccoglitore, viene attribuita specifica denominazione, conosciuta solamente dal responsabile segreteria didattica (incaricata dell'inserimento nell'archivio cartaceo). Quest'ultimo infine, viene incaricato dal Titolare del Trattamento di scegliere e applicare, in completa autonomia, la miglior strategia di disposizione dei singoli raccoglitori all'interno dell'archivio.
Controllo degli accessi ai locali interessanti l'archiviazione cartacea dei dati	Il Titolare del Trattamento ha predisposto la consegna delle chiavi di accesso al locale segreteria amministrativa, al fine di limitare l'accesso di personale non autorizzato in assenza fisica di quest'ultimo.
Controllo degli accessi alle postazioni informatiche di trattamento e/o archiviazione dei dati	Il Titolare del Trattamento ha predisposto l'autorizzazione del responsabile segreteria amministrativa ad accedere personalmente alle postazioni informatiche presenti, lasciando allo stesso pieno potere decisionale di gestione dei PC, modalità di accesso comprese Difatti, il Responsabile segreteria amministrativa provvede alla creazione di password con 8 caratteri di carattere variabile, prive di riferimento alcuno a dati inerenti gli utilizzatori (come date di nascita, nomi di parenti, ecc.).

Misura esistente/pianificata	Spiegazione
Sicurezza dei documenti cartacei	La efficace sorveglianza della documentazione cartacea viene lasciata al solo responsabile della segreteria amministrativa, su diretto incarico da parte del Titolare del Trattamento: l'archiviazione delle informazioni personali degli interessati infatti, avviene all'interno del locale dove il Responsabile segreteria amministrativa è sempre presente in orario di apertura dell'Istituto. Il Titolare del Trattamento, ha altresì predisposto che la consegna della chiave di accesso al locale contenenti gli archivi cartacei, avvenisse per il solo responsabile della segreteria amministrativa, incaricato di vegliare sulla corretta integrità dei dati presenti in archivio. In caso di sua assenza temporanea, il Responsabile segreteria amministrativa provvederà a chiudere a chiave il locale segreteria didattica, al fine di impedire eventuali e indesiderate intrusioni e possibili fughe di informazioni.
Minimizzare la quantità di dati personali richiesti	I dati personali richiesti si attengono a quelli strettamente necessari al fine di iscrivere correttamente lo studente all'anno scolastico, nonché di conoscere approfonditamente il bambino e tutto ciò che è necessario sapere, al fine di scongiurare problematiche all'interessato, durante lo svolgimento del servizio di istruzione.
Vulnerabilità delle postazioni informatiche	Il sistema operativo delle postazioni informatiche presenti in azienda (Microsoft Windows) son stati impostati in modo tale che questi si aggiornino sistematicamente e automaticamente.
Lotta contro i malware	La protezione delle postazioni informatiche contro hackeraggi e attacchi informatici, viene scongiurata con l'utilizzo di software antivirus, malware e phishing, nonché di firewall accuratamente impostati da tecnici esterni specializzati. I software antintrusione sono tutti originali e di stampo professionale, forniti da tecnici esterni specializzati, i quali forniscono altresì regolare licenza di utilizzo, con validità annuale. A seguito di consultazione con il responsabile della protezione del trattamento dei dati, è stato escluso l'utilizzo di programmi freeware (liberamente scaricabili da internet, non a pagamento e privi di licenza di utilizzo), in quanto è risaputa la loro vulnerabilità rispetto ai programmi auguralmente in uso
Gestione postazioni	La sicurezza delle postazioni informatiche, viene garantita dalle buone prassi di lavorazione messe in pratica dal responsabile segreteria amministrativa, su diretto incarico da parte del Titolare del Trattamento. Per le modalità di gestione degli accessi alle singole postazioni si rimanda al punto precedente "Controllo degli accessi". Si specifica inoltre, che non è presente lavoro in rete.
Manutenzione	La manutenzione fisica delle attrezzature viene lasciata a personale esterno qualificato, contattato direttamente dall'Istituto nel momento del bisogno

Misura esistente/pianificata	Spiegazione
Sicurezza della rete	La sicurezza della rete viene favorita mediante utilizzo di software antivirus, malware e phishing, nonché di firewall accuratamente impostati da tecnici esterni specializzati.
Contratti di trattamento	L'Istituto gestisce internamente il trattamento dei dati personali interessanti studenti e relativo nucleo familiare. Lascia comunque la gestione di alcune tipologie di dati a soggetti terzi esterni. Per la specificazione di tale evidenza, si rimanda alla specifica sezione *"Identificazione del Trattamento"*.
Sicurezza dell'hardware	Come specificato in precedenza, la sicurezza degli hardware e delle postazioni informatiche viene favorita da specifico e apposito servizio di assistenza erogato da ditta specializzata.
Tracciabilità	Al fine di favorire la tracciabilità e la rintracciabilità dei dati, l'Istituto dispone di apposto registro di protocollo, nel quale vengono catalogate, con numero progressivo, tutte le informazioi in entrata e in uscita.
Archiviazione	L'Istituto ha predisposto un sistema di backup dei dati presenti nella memoria interna delle varie postazioni informatiche mediante hard disk esterni portatili.
Backup	Per quanto riguarda il backup dei dati presenti nella memoria delle varie postazioni informatiche utilizzate, si rimanda al punto soprastante "*Archiviazione*".
Gestione dei rischi sulla privacy	La gestione dei rischi avviene in modo bidirezionale, in quanto svolta: ❖ su base pressoché quotidiana, dal personale interno; ❖ su base periodica, in presenza del Responsabile della Protezione dei Dati, il quale provvederà a svolgere attività di audit interno, al fine di verificare la bontà, la corretta applicazione e l'efficacia delle metodiche atte alla gestione dei dati degli interessati. La periodicità con cui verrà svolta attività di audit interno, verrà concordata tra la dirigenza dell'Istituto e il Responsabile della Protezione dei Dati, ponendo come limite una frequenza non inferiore alla trimestralità.
Supervisione	Al pari della gestione dei rischi, anche la supervisione delle procedure operative interne in fatto di trattamento e gestione dei dati personali degli interessati avviene in modo bidirezionale, in quanto svolta: ❖ su base pressoché quotidiana, dal personale interno; ❖ su base periodica, in presenza del Responsabile della Protezione dei Dati, il quale provvederà a svolgere attività di audit interno, al fine di verificare la bontà, la corretta applicazione e l'efficacia delle metodiche atte alla gestione dei dati degli interessati. La periodicità con cui verrà svolta attività di audit interno, verrà concordata tra la dirigenza dell'Istituto e il Responsabile della Protezione dei Dati, ponendo come limite una frequenza non inferiore alla trimestralità.

Misura esistente/pianificata	Spiegazione
Politiche e procedure interne	Al fine di favorire il più alto grado di sicurezza possibile in fatto di raccolta, trattamento e conservazione dei dati personali degli interessati, l'Istituto ha deciso di basare la propria politica gestionale interna, in maniera trasparente, sulla elaborazione e messa in atto di apposite "buone prassi operative", nello specifico: ❖ mettere a disposizione del proprio personale, una apposita guida utile alla sensibilizzazione delle sostanziali modifiche introdotte dal Reg. UE 2016/679 in fatto di trattamento dei dati della privacy; ❖ programmare ed effettuare incontri formativi con il personale operante in azienda sul tema della gestione dei dati della privacy e di tutte le fonti di pericolo, rischio e possibili conseguenze inerenti la perdita, fuga, distruzione, qualsivoglia problematica intercorsa nel trattamento dei dati della privacy; ❖ fornire ai propri clienti apposite informative inerenti le finalità del trattamento dei propri dati, le figure incaricate del trattamento e della protezione di tali informazioni, le modalità con cui vengono svolte le varie fasi del processo di trattamento, nonché la possibilità di esercizio dei propri diritti (accesso, cancellazione, obiezione, restrizione, portabilità, ecc.); ❖ elaborazione di specifiche procedere utili alle corrette modalità di raccolta, trattamento e archiviazione dei dati dei vari interessati.

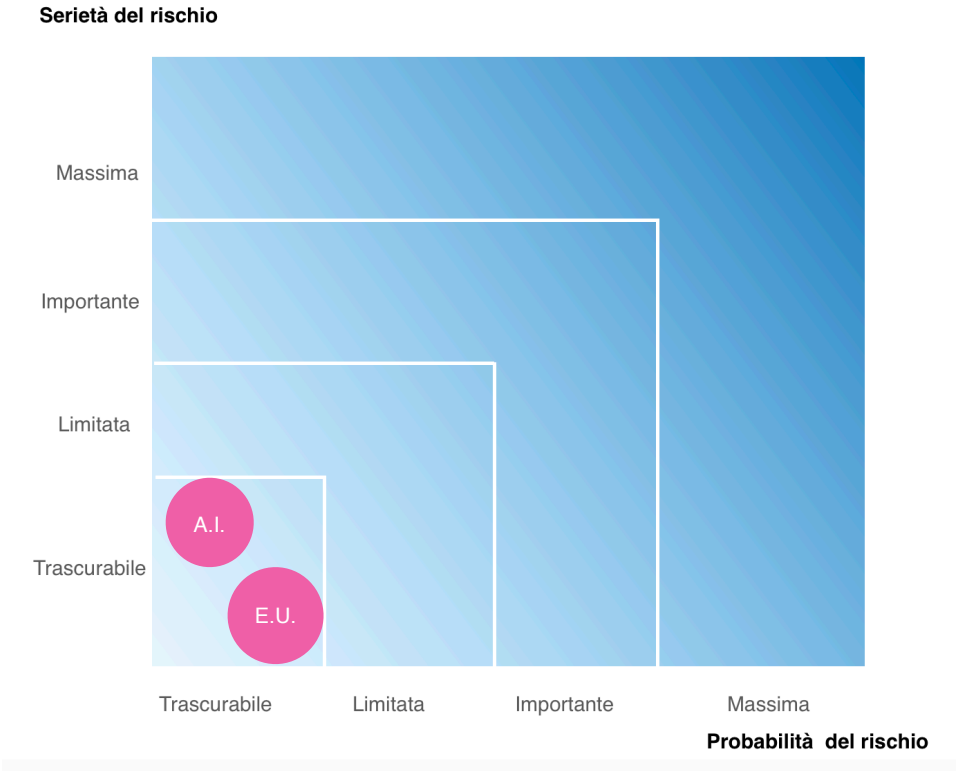
Al termine della presente Valutazione dei Rischi, non si individuano ulteriori misure correttive da implementare nelle metodiche di raccolta, trattamento e conservazione dei dati personali.

Sarà comunque cura del Titolare/Responsabile del Trattamento, nonché del Responsabile della Protezione dei Dati, verificare la corretta applicazione delle accortezze esistenti, al fine di valutarne una futura revisione o implementazione.

Piano d'Azione: stima finale del rischio

Una volta individuate sia le misure in essere e già messe in atto al fine di garantire il più alto grado di sicurezza e protezione dei dati trattati all'interno dell'Istituto", si riporta di seguito il piano d'azione effettivo utile alla riduzione dei rischi prima elencati, corredato dalla finale mappatura del rischio:

Rischio	Misure esistenti/pianificate	Misure correttive da implementare
Accesso illegittimo ai dati degli interessati	Criptografia dei dati, Controllo degli accessi ai locali archiviazione, Controllo degli accessi alle postazioni informatiche, Sicurezza dei documenti cartacei, Vulnerabilità delle postazioni informatiche, Lotta contro i malware, Gestione postazioni, Sicurezza della rete, Gestione dei rischi sulla privacy, Supervisione, Politiche	Nessuna ulteriore misura ad implementare
"Errore Umano" durante raccolta dati	Supervisione, Politiche	Nessuna ulteriore misura ad implementare



Rischio valutato con le sole misure esistenti o pianificate