SCUOLA DELLE ARTI E DELLA FORMAZIONE PROFESSIONALE “RODOLFO VANTINI”

Modello Organizzativo sulla Protezione dei Dati ai sensi del Reg. UE 2016/679

Documento di Sintesi Protezione Dati

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
00		Prima Emissione	CdA

INDICE

Termini e definizioni

TRATTAMENTO	qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione
DATO PERSONALE	qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;
LIMITAZIONE AL TRATTAMENTO	il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro
TITOLARE DEL TRATTAMENTO	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri
RESPONSABILE DEL TRATTAMENTO	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento
DESTINATARIO	la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento
TERZO	la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile
CONSENSO DELL'INTERESSATO	qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento

VIOLAZIONE DEI DATI PERSONALI	la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati
RAPPRESENTANTE	la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento
AUTORITA' DI CONTROLLO	autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51
AUTORITA' DI CONTROLLO INTERESSATA	Autorità di controllo interessata al trattamento in quanto: a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo; b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure c) un reclamo è stato proposto a tale autorità di controllo
GRUPPO IMPRENDITORIALE	Un gruppo costituito da un'impresa controllante r dalle imprese da queste controllate
TRATTAMENTO TRANSFRONTALIERO	Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento enll'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.
DATA PROTECTION OFFICER (DPO-RESPONSABILE DELLA PROTEZIONE DEI DATI)	Soggetto designato dal Titolare o dal Responsabile del trattamento nelle ipotesi di cui all'art. 37 GDPR. Tra i suoi compiti rientrano: • Fornire consulenza in materia privacy; • Sorvegliare l'osservanza del GDPR, delle altre disposizioni relative alla privacy e delle politiche del Titolare o del Responsabile del trattamento sulla protezione dei dati; • Fornire parere sulla valutazione d'impatto sulla privacy; • Cooperare con l'Autorità di Controllo; • Fungere da punto di contatto con l'Autorità di Controllo per questioni connesse al trattamento

1. PREMESSA

Il presente documento, corredato di tutti i suoi allegati, è il Documento di Sintesi sulla Protezione dei Dati ai sensi del Reg. UE n. 2016/679, adottato dalla società Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini".

La Scuola, consapevole dell'importanza che riveste la tutela dei dati personali, intende conformare la propria struttura ai nuovi principi del Regolamento UE n. 2016/679 (c.d. GDPR). Al riguardo, i dati personali saranno trattati in conformità ai principi di:

a) liceità, correttezza e trasparenza

b) limitazione delle finalità, per cui i data saranno raccolti per finalità determinate, esplicite e legittime e trattati in modo conforme rispetto alle predette finalità;

c) minimizzazione dei dati: i dati devono essere adeguati, pertinenti e limitati a quanto accessorio rispetto alle finalità per cui sono trattati;

d) esattezza: i dati devono essere esatti e opportunamente aggiornati in caso di modificazioni;

e) limitazione della conservazione: i dati personali non saranno conservati in un modo che consente l'identificazione degli interessati per un tempo superiore rispetto al perseguimento delle finalità, fatte salve le deroghe nelle ipotesi indicate espressamente dal legislatore nazionale e comunitario;

f) integrità e sicurezza, poiché i dati saranno protetti attraverso misure tecniche ed organizzative adeguate al fine di impedire il trattamento non autorizzato, la perdita, la distruzione e il danno accidentale ai dati.

2. IL CONTESTO NORMATIVO DI RIFERIMENTO

2.1 Il Regolamento Europeo 679/2016 (General Data Protection Regulation)

L'eterogeneità della tutela della privacy nei diversi Paesi dell'Unione ha spinto il Legislatore Europeo a rielaborare la materia, al fine di armonizzare la tutela della privacy e di garantire livelli elevati di tutela dei dati personali all'interno di tutto il territorio dell'UE.

Per questi motivi è stato emanato il Regolamento UE n. 2016/679-General Data Protection Regulation (c.d. GDPR). Il GDPR abroga la Direttiva 95/46/CE del 1995 (Direttiva "Madre"), ma non abroga la successiva Direttiva 2002/58/CE (e-privacy) c, ad oggi in fase di revisione, la quale dovrebbe essere sostituita da uno specifico Regolamento (Regulation on Privacy and Electronic Comunications) volta ad allineare la normativa e-privacy con le nuove regole del GDPR.

Il Regolamento non va invece ad abrogare le normative dei singoli Stati membri, che saranno chiamati a disapplicare le disposizioni interne in contrasto con la disciplina comunitaria e ad armonizzarne i contenuti.

Oltre a ciò, poiché il GDPR prende in esame le sole sanzioni amministrative, gli Stati membri sono tenuti a determinare le specifiche responsabilità civili e penali derivanti dalla violazione delle norme privacy, in conformità con i principi generali degli ordinamenti interni.

Sono fatte salve altresì le disposizioni interne in materia di diritto del lavoro e di diritto amministrativo: i suddetti ambiti, che spesso si intersecano con la tutela della privacy, sono rimangono di competenza esclusiva dei singoli Stati membri.

Di seguito, in tabella, vengono riportati gli elementi principali del Regolamento UE n. 2016/679.

	REGOLAMENTO UE 2016/679
SOGGETTI	Artt. 4, 28 e 29 GDPR Titolare del trattamento Co – titolari del trattamento Rappresentante Responsabile del trattamento Persone autorizzate al trattamento
DPO	Artt. 37, 38 e 39 GDPR Introduce la figura del Responsabile Protezione dei Dati (Data Protection Officer) con compiti eterogenei alcuni di natura ispettiva, altri consulenziali e altri esterni come il rapporto con interessati e con Autorità di controllo.
ANALISI DEI RISCHI E SICUREZZA DEL TRATTAMENTO	Art. 32 GDPR Nel valutare l'adeguatezza delle misure di sicurezza il titolare e il Responsabile devono effettuare un'analisi dei rischi derivanti dai trattamenti che

	intendono effettuare o effettuano.
PRIVACY BY DESIGN E BY DEFAULT	Definite nell'art. 25 paragrafi 1 e 2 del GDPR La tutela dei dati personali deve essere calata all'interno dei processi e dell'organizzazione aziendale e deve essere presupposto da tenere in considerazione sia dalla fase di progettazione dei prodotti e servizi.
VALUTAZIONE D'IMPATTO DULLA PROTEZIONE DEI DATI (PRIVACY IMPACT ASSESSMENT)	Art. 35 GDPR Qualora un trattamento presenti un rischio elevato per i diritti e libertà delle persone il Titolare (unitamente a DPO se nominato) è tenuto ad effettuare una valutazione d'impatto privacy (se possibile in via preventiva)
DATA BREACH	Art. 33 GDPR Entro 72 ore dalla scoperta, tutti i Titolari e Responsabili del trattamento devono notificare l'avvenuta violazione dei dati personali all'autorità di controllo e se ricorrono determinate condizioni agli interessati
REGISTRO DEI TRATTAMENTI	Art. 30 Titolari e Responsabili dovranno tenere un registro delle attività di trattamento. Il registro non è obbligatorio per le imprese od organizzazioni con meno di 250 dipendenti, salvo deroghe.
TEMPO DI CONSERVAZIONE DEI DATI (RETENTION DATI)	Art. 6 par. 1 lett. e) del GDPR e Art. 30 lett. f) Titolari e Responsabili dovranno definire internamente e comunicare ai terzi i tempi di conservazione dei dati (retention)
DIRITTI DELL'INTERESSATO	Artt. 15, 16, 17, 18, 20 e 21 del GDPR Ribadisce le prerogative concesse agli interessati e introduce nuovi diritti quali la portabilità del dato e il diritto all'obblio.
COMPETENZA DELL'AUTORITA' CAPOFILA (ONE STOP SHOP)	Art. 56 del GDPR Introduce la nuova figura dell'Autorità Capofila (cd Lead Authority) per i trattamenti transfrontalieri.
SANZIONI AMMINISTRATIVE PECUNIARIE	Artt. 83, 84 del GDP Si modifica l'entità delle sanzioni pecuniarie.
CERTIFICAZIONE DEI TRATTAMENTI	Artt. 42, 43 del GDPR

	Il GDPR promuove l'istituzione di meccanismi di certificazione della protezione dei dati allo scopo di dimostrare la conformità al Regolamento.

Con particolare riferimento alle sanzioni amministrative previste, l'art. 83 prevede le seguenti sanzioni pecuniarie:

- fino a 10 000 000 Euro, o per le imprese, fino al 2 % del fatturato globale totale annuo dell'esercizio precedente, se superiore;

- fino a 20 000 000 Euro, o per le imprese, fino al 4 % del fatturato globale totale annuo dell'esercizio precedente, se superiore;

- l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 Euro, o per le imprese, fino al 4 % del fatturato globale totale annuo dell'esercizio precedente, se superiore.

Le sanzioni più elevate si applicano nel caso di:

- Violazioni dei principi del trattamento (esempio condizioni per il consenso);
- Violazione dei diritti degli interessati;
- Inosservanza delle norme per il trasferimento internazionale dei dati;
- Violazioni di obblighi previsti dalle legislazioni degli stati membri;
- Inosservanza di ordini e disposizioni delle Autorità di Controllo.

2.3 Le Autorità Garanti e il contesto Europeo

Ogni stato membro dispone una Autorità di Controllo indipendenti (Garanti Privacy) che sono incaricate di sorvegliare l'applicazione del Regolamento (da art.51 a art.55 GDPR).

L'art. 56 del GDPR prevede una rilevante novità in ordine all'Autorità di Controllo, poiché introduce la nuova figura dell'Autorità Capofila (cd Lead Authority). L'Autorità di Controllo dello Stabilimento principale o unico del Titolare o Responsabile del trattamento è competente ad agire quale Autorità di Controllo Capofila per i trattamenti transfrontalieri. Ciò ad eccezione delle ipotesi di cui al paragrafo 2, per cui ogni Autorità di Controllo resta competente se l'oggetto della violazione riguarda esclusivamente uno stabilimento nel suo Stato membro o riguarda interessati unicamente nel suo Stato, dandone tempestiva informazione all'Autorità Capofila.

Al fine di contribuire all'applicazione coerente del presente regolamento in tutta l'UE, le Autorità di controllo cooperano tra loro e mediante il meccanismo di coerenza definito nel Regolamento stesso (da art. 60 a art. 67 GDPR).
Il comitato europeo per la protezione dati (EDPB) è istituito quale organismo dell'unione ed è dotato di personalità giuridica i compiti sono definiti dal Regolamento (art.68 a art. 76 GDPR).

Il Working Party 29 (Gruppo di Lavoro) istituito dall'art. 29 della direttiva 1995/46; è un organo consultivo indipendente composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal GEPD (Garante europeo della protezione dei dati), nonché da un rappresentante della Commissione. Nel corso della sua attività il WP 29 ha elaborato delle Linee Guida utili

per la comprensione ed uniforme applicazione della normativa privacy nel territorio dell'Unione. Con riferimento al GDPR, si ricordano:

- Linee Giuda WP 243 sul DPO;
- Linee Giuda WP 248 sulla Valutazione Impatto sulla Protezione Dati;
- Linee Guida WP 259 sul consenso;

Linee Guida WP 260 sulla trasparenza e le misure da adottarsi dal Titolare per fornire le informazioni e le comunicazioni previste dal GDPR.

A partire dal 25 maggio 2018 opererà in luogo del WP29 l'EDPB (European Data Protection Board) come previsto da Regolamento.

3. IL MODELLO ORGANIZZATIVO PROTEZIONE DEI DATI

3.1 Obiettivi perseguiti

Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini", si pone l'obiettivo di conformare la propria organizzazione alla nuova normativa europea in materia di Privacy (GDPR). Ciò al fine di assicurare la tutela dei diritti degli interessati che, a vario titolo, conferiranno i loro dati alla Società

In particolare, intende garantire:

- un'informativa chiara, corretta e facilmente accessibile per gli interessati relativamente alle modalità di trattamento dei dati personali da parte di Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini";

- un esercizio semplice e immediato dei diritti degli interessati in materia di privacy;

- che il trattamento dei dati sia giustificato da un legittimo interesse, ovvero dal consenso o da altre basi giuridiche in conformità con quanto previsto dalla legge europea;

- la sicurezza nel trattamento dei dati, attraverso la predisposizione di misure adeguate rispetto al rischio;

- la conservazione dei dati per un periodo non superiore rispetto al conseguimento delle finalità del trattamento;

- la gestione dei dati pertinente e limitata a quanto strettamente necessario per l'esercizio di ogni trattamento;

- il rispetto, da parte dei soggetti che gestiscono i dati degli interessati per conto di Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini", della normativa privacy.

3.2 Ambito di applicazione

Il Modello Organizzativo Protezione dei Dati si applica alla società Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini"

La Scuola si impegna a diffondere, nella propria organizzazione ed all'esterno, i contenuti del Modello Organizzativo di Protezione Dati ed i successivi aggiornamenti in modo completo, accurato e continuo.

3.3 Struttura del Modello Organizzativo Protezione dei Dati

Il Modello Organizzativo Protezione Dati integra i seguenti documenti:

- **Documento di Sintesi Protezione Dati**

  Documento riassuntivo dell'attività svolta in ordine all'adeguamento privacy al nuovo contesto europeo, con evidenza dell'approccio metodologico utilizzato per l'analisi dei rischi privacy e delle misure di sicurezza (controlli).

- **Registro dei trattamenti**

  Documento (da mantenersi anche in formato elettronico) riportante i trattamenti effettuati dal Titolare o Responsabile e corredati dall'indicazione della descrizione del trattamento (area, archivi/banche dati, descrizione), degli attori (Titolare, Responsabili, Privacy Officer e Persone Autorizzate al trattamento), delle finalità del trattamento (finalità, liceità, base giuridica), dei destinatari, degli interessati e delle misure adottate ai sensi dell'art. 32 del Regolamento in relazione ai rischi per i diritti e le libertà delle persone fisiche.

  Il Registro dei trattamenti è necessario per documentare dinanzi all'Autorità di controllo la conformità dell'organizzazione alle norme del Regolamento Privacy UE (Considerando 82). Il Registro non deve essere tenuto da Titolari o Responsabili che abbiano meno di 250 dipendenti, a meno che:

  - Il trattamento presenti rischi specifici per diritti e libertà e non sia occasionale o
  - il trattamento includa categorie particolari di dati;
  - Il trattamento includa dati giudiziari.

- **Rapporto PIA (Privacy impact Assessment)**

  Nel Rapporto PIA è riportata la valutazione d'impatto sulla protezione dei dati, che prende in esame nel dettaglio i dati trattati, i rischi per i diritti e le libertà delle persone (impatto privacy) e le misure da porre in atto per prevenire e risolvere le eventuali criticità rilevate. Si procede alla PIA allorquando si presenta un trattamento che può presentare un rischio elevato e in tutte le casistiche definite dal Regolamento e dalle Linee guida del WP29.

- **Procedure Protezione Dati**

  Ai fini dell'adeguamento al GDPR, sono ri-definite ovvero create nuove procedure aziendali relativamente a:
  - **Data Breach:** per rendere possibile la comunicazione della violazione dei dati all'Autorità di Controllo entro 72 ore dalla scoperta;
  - **Esercizio dei diritti degli interessati:** per consentire agli interessati l'esercizio effettivo dei diritti di cui all'art. 7 del Codice Privacy e degli artt. 15, 16, 17, 18, 20 e 21 del GDPR;
  - **Retention dei dati:** per conservare i dati nel periodo necessario allo svolgimento delle finalità previste.

- **Allegato - Organizzazione, Ruoli e Responsabilità in materia di Protezione Dati**

  E' il grafico della struttura interna, riportante l'indicazione del Titolare del trattamento e di tutte le figure incaricate che agiscono con profili e ruoli diversi in ambito di Protezione dei Dati e loro utilizzo; nonché dei Responsabili del trattamento che effettuano trattamenti di dati personali per conto del Titolare. Da esso discendono i documenti volti a nominare i Responsabili, il Privacy Officer nonché le persone autorizzate al trattamento, etc. corredati dalla definizione delle responsabilità e dei compiti ad essi spettanti nonché delle istruzioni loro impartite dal Titolare.

- **Allegato - Informative e clausole contrattuali**

  Conformemente al disposto dell'art. 13 del GDPR, le informative allegate sono atti predisposti a rendere le opportune informazioni in materia di protezione dei dati ai vari interessati al trattamento (personale dipendente, utenti del sito, clienti…). Le clausole, inserite nei contratti, comprovano la conoscenza e il rispetto della normativa da parte dei contraenti.

3.4 Approvazione, modifica e attuazione

Il Modello Organizzativo Protezione Dati è approvato e adottato con delibera del Consiglio di Amministrazione.

Si procede ad aggiornare o integrare il Modello, in seguito a:

- aggiornamenti normativi;
- significativi cambiamenti nell'organizzazione o nei processi;
- avvio di nuovi trattamenti;
- introduzione di nuove tecnologie o software (privacy by design)

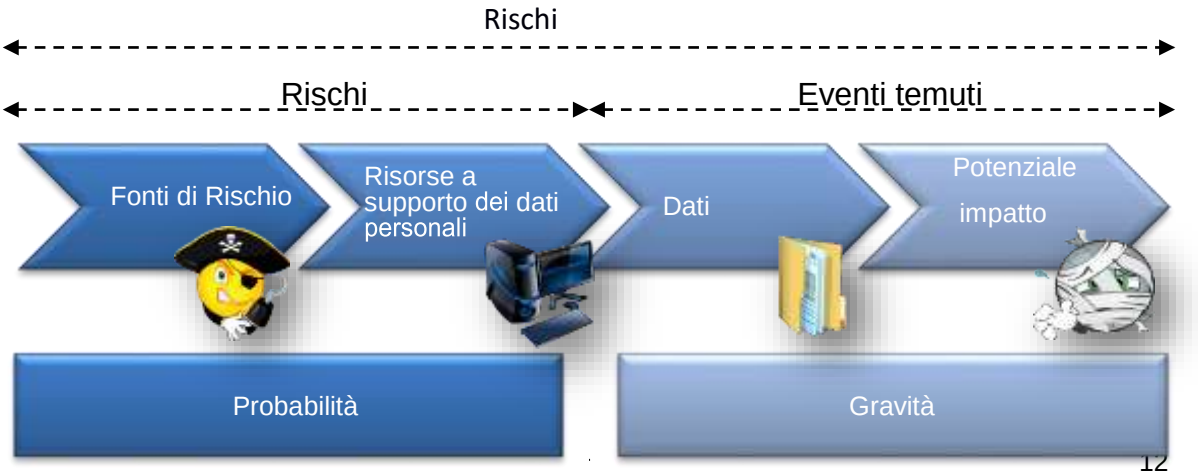
3.4 Metodologia di analisi dei rischi e valutazioni di impatto sulla protezione dei dati

L'analisi dei rischi per i diritti e le libertà delle persone fisiche o impatto sulla protezione dei dati è condotto secondo i criteri indicati dal WP 29 nel documento Linee Guida 248 - sulla Valutazione Impatto sulla Protezione Dati. Nello specifico si adotta la metodologia pubblicata dall' l'Autorità Garante dei dati personali Francese - **CNIL** (Commission Nationale Informatique & Libertes).

Lo **CNIL** ha provveduto a identificare i seguenti parametri di valutazione del livello di rischio:

- *gravità (o impatto)*: la gravità rappresenta l'entità del rischio. Essa è principalmente stimata in termini di portata degli impatti potenziali sulle persone interessate, tenendo conto dei controlli esistenti, pianificati o aggiuntivi.
- *probabilità (o potenzialità di verificazione del rischio)*: la probabilità rappresenta la possibilità che un rischio si verifichi. Questa viene principalmente stimata in termini di livello di vulnerabilità delle risorse di supporto interessate e di capacità delle fonti di rischio di sfruttarle, tenendo conto dei controlli esistenti, pianificati o aggiuntivi.

Il seguente schema riassume tutti i concetti sopra elencati:



fonte CNIL - Methodology

Fonti di Rischi	Descrizione
Fonti umane interne	Dipendenti, responsabili IT, tirocinanti e manager
Fonti umane esterne	Destinatari di dati personali, terzi autorizzati, fornitori di servizi, hacker, visitatori, ex dipendenti, attivisti, concorrenti, clienti, addetti alla manutenzione, autori di reati, sindacati, giornalisti, organizzazioni non governative, organizzazioni criminali, organizzazioni sotto il controllo di uno Stato estero, organizzazioni terroristiche, attività industriali vicine
Fonti non umane	Codice maligno di origine sconosciuta (virus, worm ecc.), acqua (tubi, vie navigabili ecc.), materiali infiammabili, corrosivi o esplosivi, calamità naturali, epidemie, animali

Eventi Temuti	Descrizione
Accesso non autorizzato a dati personali	I dati vengono utilizzati per finalità diverse da quelle previste e/o in modo scorretto I dati sono diffusi più del necessario e al di fuori del controllo degli interessati
Modifiche indesiderate a dati personali	I dati vengono modificati in dati validi o non validi, che non saranno utilizzati correttamente, il trattamento potrebbe causare errori, malfunzionamenti, o non fornire più il servizio previsto I dati vengono modificati in altri dati validi, così che le operazioni di trattamento sono state o possono essere utilizzate in modo improprio
Scomparsa di dati personali	I dati non sono disponibili per elaborazioni di dati personali, e questo genera errori, malfunzionamenti o fornisce un servizio diverso da quello previsto Mancano i dati per i trattamenti di dati personali, che non possono più fornire il servizio previsto

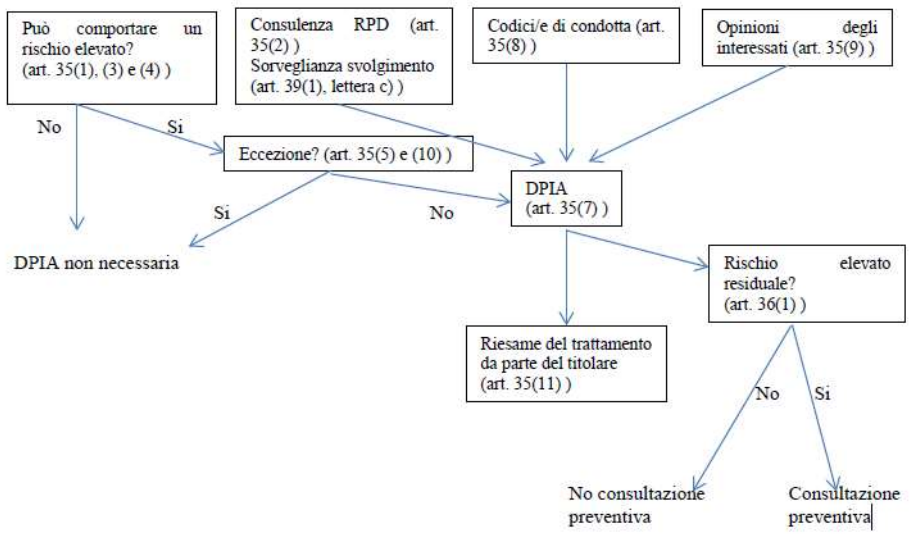
Minacce	Descrizione

Utilizzo improprio delle risorse di supporto	le risorse di supporto sono utilizzate all'esterno o addirittura deviate dal contesto di utilizzo previsto senza essere alterate o danneggiate
Limiti operativi delle risorse di supporto o loro danneggiamento	i limiti operativi delle risorse di supporto vengono superati, le risorse di supporto sono sovraccaricate, sfruttate eccessivamente o utilizzate in condizioni che non ne consentono il corretto funzionamento le risorse di supporto sono parzialmente o completamente danneggiate
Perdita delle risorse di supporto	le risorse di supporto vanno perse, vengono rubate, vendute o alienate, pertanto non consentono più l'esercizio dei diritti di proprietà.

L'analisi viene condotta preliminarmente per tutti i trattamenti di dati personali al fine di determinarne il livello di rischio.

In fase di valutazione del rischio viene compilato un questionario preliminare che consente di determinare se il trattamento necessita di un approfondimento PIA oppure no (presupporti e casistiche definite dal Regolamento e dalle Linee guida WP29).

La figura seguente illustra i principi fondamentali concernenti la PIA in base al RGPD:



Fonte Linee guida WP29 - 248

3.4. Controlli e Misure

Allo scopo di costruire un sistema che garantisca il rispetto dei principi della protezione dati previsti dal Regolamento vengono implementati i controlli sul trattamento dei rischi.

I controlli o misure che vengono descritti sinteticamente nel registro dei trattamenti e poi ripresi e approfonditi, se necessario, nel rapporto PIA sono:

- **Misure legali obbligatorie**
- **Misure organizzative**
- **Misure tecniche**
- **Misure fisiche**

Misure legali obbligatorie

Consentono di verificare che il trattamento sia conforme ai requisiti legali espressi nel GDPR e sono da intendersi obbligatorie per tutti trattamenti. Le misure sono riepilogate in tabella a seguito. Le Misure legali sono da considerarsi obbligatorie e producono i loro effetti sui Dati.

Misure legali (obbligatorie)	Descrizione
Finalità	scopo specificato, esplicito e legittimo
Minimizzazione	limitazione della quantità di dati personali allo stretto necessario
Periodo di conservazione	periodo necessario per conseguire gli obiettivi
Informazione	rispetto del diritto degli interessati all'informazione
Consenso	ottenere il consenso degli interessati o esistenza di altra base giuridica che giustifichi il trattamento dei dai
Diritto di opposizione	rispetto dei diritti degli interessati
Diritto di accesso	rispetto dei diritti degli interessati
Diritto di rettifica e cancellazione	rispetto dei diritti degli interessati
Diritto alla portabilità	rispetto dei diritti degli interessati
Trasferimenti al di fuori dell'Unione europea	rispetto delgi obblighi previsti per il trasferimento di dati fuori da UE
Formalità	definizione ed espletamento delle formalità prima della trasformazione

Misure organizzative

Consistono nella verifica dell'organizzazione, politica e gestione dei rischi. Alcuni di essi sono trasversali, cioè riferibili a tutti i trattamenti considerati, altre specifiche. Le misure organizzative producono i loro effetti a livello transorganizzativo , ovvero sugli impatti e sulle fonti dei rischi.

Misure organizzative (trattamento dei rischi)	Descrizione
Organizzazione	Transorganizzativo
Politiche (gestione delle regole)	Transorganizzativo
Gestione dei rischi	Transorganizzativo
Gestione dei progetti	Transorganizzativo
Gestione degli incidenti e della violazione dei dati	Impatti
Gestione del personale	Fonti
Relazione con i terzi	Fonti
Manutenzione	Fonti

Supervisione (audits, dashboard…)	Transorganizzativo
Marcatura dei documenti	Fonti
Archiviazione	Transorganizzativo

Misure tecniche

Consistono nella verifica degli aspetti di governance IT e di sicurezza informatica. Le misure tecniche possono essere trasversali o specifiche rispetto ai trattamenti e producono i loro effetti sui dati, sugli impatti e sulle fonti dei rischi e sulle risorse di supporto.

Misure sicurezza logica (trattamento dei rischi)	Descrizione
Anonimizzazione	Dati
Crittografia	Fonti
Controlli integrità	Impatti
Backup	Impatti
Partizionamento dati	Fonti
Controllo degli accessi logici	Fonti
Tracciabilità	Fonti
Operazioni	Risorse di supporto
Monitoraggio (impostazione , controlli in tempo reale, etc.)	Risorse di supporto
Gestione delle postazioni di lavoro	Risorse di supporto
Antivirus, spyware, etc.	Fonti
Protezione dei canali informatici (reti)	Risorse di supporto

Misure fisiche

Consistono nella verifica di sicurezza fisica e di security. Le misure tecniche possono essere trasversali o specifiche rispetto ai trattamenti e producono i loro effetti principalmente sulle fonti dei rischi e sulle risorse di supporto.

Misure sicurezza fisica (trattamento dei rischi)	Effetto principale
Distanziamento delle fonti di rischio (prodotti pericolosi, aree pericolose, etc.)	Fonti
Controllo degli accessi fisici	Fonti
Sicurezza dell'hardware	Risorse di supporto
Sicurezza dei documenti cartacei	Risorse di supporto
Sicurezza dei canali cartacei	Risorse di supporto

Protezione fonti di rischio non umane (incendio, etc.)	Fonti

4. DPO (DATA PROTECTION OFFICER-RESPONSABILE PROTEZIONE DATI)

4.1 Identificazione del DPO

Ai sensi dell'art. 37 del GDPR, il Responsabile della Protezione dei Dati (DPO o, in lingua inglese, DPO-Data Protection Officer) è designato dal Titolare e dal Responsabile del Trattamento e deve essere obbligatoriamente nominato ogni volta che si verifichino le seguenti condizioni:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni 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.

Dal momento che il GDPR riporta espressioni dal significato ampio, il WP29 ha specificato che:

1. Le nozioni di "autorità pubblica" o "organismo pubblico" devono essere conformi al diritto nazionale;
2. Per attività principali si possono intendere le operazioni essenziali al raggiungimento degli obiettivi da parte del Titolare o Responsabile del Trattamento, ovvero quando il trattamento dei dati costituisce una componente inscindibile dalle attività svolte;
3. La sussistenza di un trattamento su "larga scala" va individuata ricorrendo ad alcuni fattori, tra cui il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento;
4. Monitoraggio "regolare": avviene in modo continuo ovvero su intervalli definiti per un arco di tempo definito; è ricorrente o ripetuto a intervalli costanti; avviene in modo costante o a intervalli periodici;
5. Monitoraggio "sistematico": avviene per sistema; è predeterminato, organizzato o metodico; ha luogo nell'ambito di un progetto complessivo di raccolta di dati; è svolto nell'ambito di una strategia.

Il DPO viene designato sulla base delle sue competenze professionali, specie con riferimento alla conoscenza specialistica e normativa in materia privacy. Il livello di conoscenza va commisurato ai trattamenti di dati effettuati e alla sensibilità, complessità e quantità dei dati oggetto del trattamento.

Il GDPR non specifica le qualità professionali da prendere in considerazione per la nomina del DPO, ma sicuramente sono pertinenti al riguardo la conoscenza delle prassi nazionali ed europee relative alla protezione dei dati e un'accurata padronanza della disciplina del GDPR. E' utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento; inoltre, il DPO deve

avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.

Per quanto attiene la Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini", si è ritenuto opportuno procedere alla nomina di un Data Protecion Officer. Ciò in considerazione del fatto che la Scuola, giuridicamente qualificabile come associazione di due Comuni, quale attività principale si occupa dell'istruzione e della formazione di alunni in maggioranza minorenni, di cui a volte si profila la necessità di considerare dati relativi alla salute (a titolo di esempio, si consideri la condizione di un alunno disabile, per cui si richiede un programma di formazione specializzato).

Il trattamento quotidiano di dati relativi a soggetti vulnerabili, quali alunni minorenni, e l'impatto che le loro condizioni di salute possono avere sulla formazione offerta dalla scuola, rendono necessaria un'attenzione particolare in ordine al trattamento dei dati personali. In nessun caso i diritti e le libertà degli studenti minorenni, persone "vulnerabili" in quanto ancora lontani da una condizione di maturità, devono essere messi in pericolo. La figura del DPO permette di introdurre una figura esperta in ordine al trattamento dei dati, che sappia interfacciarsi con la Scuola in modo proficuo, avendo chiara sia la normativa privacy in ogni sua più recente applicazione, sia le esigenze organizzative scolastiche sia le misure informatiche di volta in volta richieste per la protezione dei dati.

4.2 Compiti del DPO

Il Data Protection Officer è tenuto a considerare i rischi attinenti il trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento. IL DPO, specificamente, deve almeno:

a) informare e fornire consulenza al Titolare del trattamento o al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;

b) sorvegliare l'osservanza del GDPR, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del Titolare del trattamento o del Responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;

c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento;

d) cooperare con Autorità di Controllo;

e) fungere da punto di contatto per l'Autorità di Controllo per questioni connesse al trattamento, tra cui la consultazione preventiva ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

5. COMUNICAZIONE, INFORMAZIONE E FORMAZIONE

Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini" intende porre in essere tutte le misure che si renderanno necessarie per rendere edotti gli interessati dei diritti loro spettanti ai sensi della normativa comunitaria; delle modalità di trattamento dei loro dati personali; della liceità del trattamento dovuto al consenso o ad altra base giuridica; della finalità del trattamento e del tempo massimo di conservazione dei dati ovvero i criteri utilizzati per determinare tale periodo. A tal riguardo, si rinvia alle informative allegate.

A tal fine la Società provvede a istituire un'apposita casella di posta elettronica il cui indirizzo è: privacy@vantini.it che in aggiunta a mezzi di comunicazione tradizionali, consente ai destinatari di denunciare eventuali comportamenti non conformi alle disposizioni normative e di esercitare i propri diritti.

Scuola delle Arti e della Formazione Professionale "Rodolfo Vantini" si occupa di informare il proprio personale dipendente, i Responsabili del trattamento nonché tutti coloro che a vario titolo tratteranno i

dati per conto della Società, delle modalità di trattamento dei dati personali, delle finalità perseguite e dei sistemi utilizzati per garantire il rispetto dei diritti e delle libertà fondamentali degli interessati. Ciò in conformità a quanto previsto dall'art. 29 del GDPR, in ordine al quale *"Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento… non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri"* e dall'art. 32 par. IV del GDPR, per cui *"Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri."*

La formazione va finalizzata all'illustrazione dei rischi generali e specifici del trattamento, le misure organizzative, tecniche e informatiche adottate, nonché le rispettive responsabilità e le sanzioni.