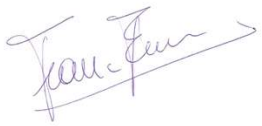
I.C. DELLA VAL NERVIA
Prot. 0002107 del 23/03/2023
I-4 (Uscita)

Documento di valutazione impatto sulla protezione dei dati personali D.P.I.A.

Redatto in base alle indicazioni del Garante Privacy

DATA DI DECORRENZA	COGNOME DIRIGENTE SCOL.	FIRMA D.S.	FIRMA D.P.O.
			

DOCUMENTO DI VALUTAZIONE IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Si redige il seguente documento di valutazione impatto sulla sicurezza dei dati personali che vengono trattati in Istituto, in cui sono individuati

- elenco dei trattamenti (Registro dei Trattamenti)
- misure di sicurezza
- struttura organizzativa per la sicurezza dei dati personali
- misure fisiche e logiche poste a tutela del trattamento dei dati

TITOLARE DEL TRATTAMENTO (Timbro lineare)

Denominazione:	
Sede del trattamento:	
Codice fiscale o Partita Iva:	
Recapito telefonico :	
Indirizzo e-mail :	
Indirizzo PEC :	

RESPONSABILE DELLA PROTEZIONE DEI DATI (DPO-RPD se richiesto)

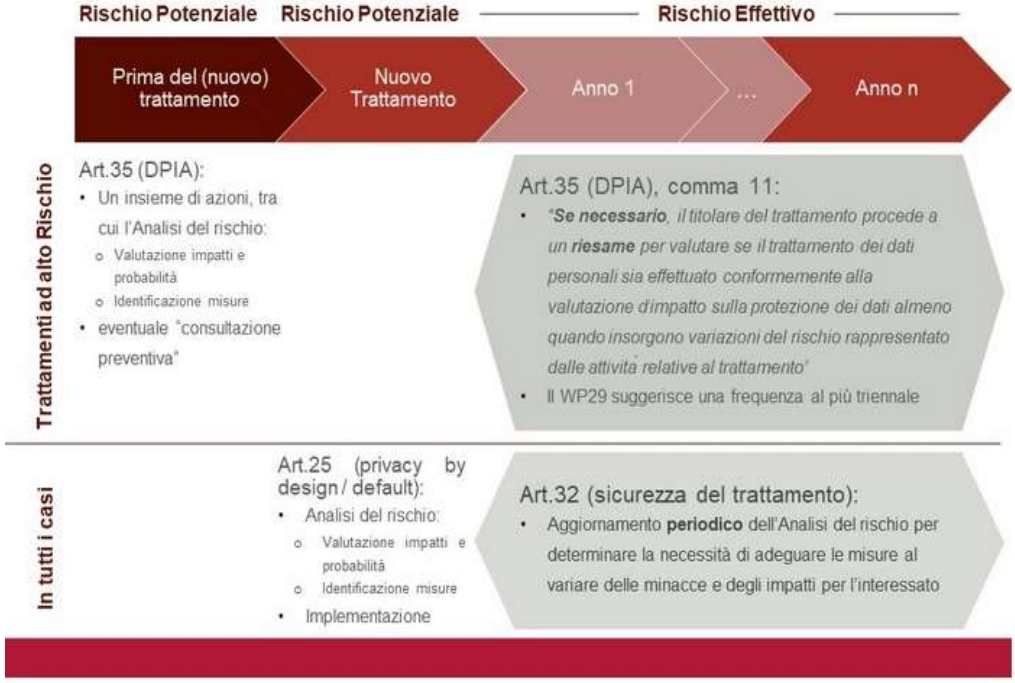
COGNOME E NOME:	**FRANCO ENRICO**
INDIRIZZO	VIALE XXV APRILE 172 – 10133 TORINO
Codice fiscale o Partita Iva:	C.F. FRNNRC60M25L219D – P.I. 09301030012
Recapito telefonico :	340.6083531
Indirizzo e-mail :	EFRANCO@FERS-TO.IT
Indirizzo PEC :	EFRANCO@PEC.IT

ELENCO DEI TRATTAMENTI DI DATI PERSONALI (Registro dei trattamenti)

Le operazioni di trattamento effettuate nell'ambito dell'Istituto consistono essenzialmente:

- acquisizione e reperimento dei dati direttamente dalla persona interessata, presso terzi ovvero indirettamente;
- registrazione dei dati, cioè il loro inserimento in supporti informatici o cartacei;
- l'elaborazione;
- la modificazione dei dati registrati, in relazione a variazioni o nuove acquisizioni;
- la conservazione dei dati per tutto il tempo necessario agli scopi per i quali sono stati raccolti o successivamente trattati;
- la cancellazione o la distruzione dei dati, quando sono terminati gli scopi per cui sono stati inizialmente raccolti oppure trascorso il tempo stabilito per quel trattamento.

Attualmente, l'Istituto è titolare dei trattamenti di dati personali riportati nel REGISTRO DEI TRATTAMENTI ed effettua "Trattamenti non occasionali di dati relativi a soggetti vulnerabili" dovendo gestire i dati relativi ai minori



In caso di nuovi trattamenti bisogna procedere con la valutazione preventiva dei flussi e dei punti critici nel trattamento e riportare il nuovo trattamento nel REGISTRO DEI TRATTAMENTI

Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente.

In caso di trattamento di dati personali di particolare rilevanza è almeno semestrale ed i dati vengono digitalmente crittografati.

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Nella tabella allegata al presente documento vengono riportate le strutture presso cui vengono effettuati i trattamenti:

RESPONSABILI DEL TRATTAMENTO E D.P.O./R.P.D. (Se nominati)

Il titolare del trattamento, individua i responsabili del trattamento i quali avranno il compito di controllare sul corretto comportamento del personale dell'Istituto e di affiancare il titolare del trattamento o sostituirlo in caso di temporanea assenza.
A ciascun responsabile, incluso il DPO/RPD, nominato in base alle proprie competenze in materia di gestione dei dati, viene consegnata una specifica lettera di incarico individuale o nomina, nella quale sono fornite precise istruzioni sulle modalità di effettuazione del trattamento e sulle misure di sicurezza da osservare.

INCARICATI o ADDETTI AL TRATTAMENTO

I responsabili del trattamento, hanno individuato gli incaricati / addetti al trattamento a ciascuno dei quali viene consegnata una specifica lettera di incarico individuale, nella quale sono fornite precise istruzioni sulle modalità di effettuazione del trattamento e sulle misure di sicurezza da osservare.

SISTEMA DI AUTENTICAZIONE INFORMATICA

La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ***ogni sei mesi****.*

In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ***ogni tre mesi.***

In caso di ***videosorveglianza*** *i dati raccolti dovranno essere mantenuti per un tempo massimo di* ***48 ore*** *salvo differenti prescrizioni e non dovranno riprendere attività svolte dai lavoratori se non a fronte di una specifica autorizzazione e comunicazione agli enti preposti.*

ATTUALMENTE NON SONO PRESENTI SISTEMI DI VIDEOSORVEGLIANZA

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

I rischi ai quali possono essere soggetti i dati trattati dal personale dell'Istituto nell'ambito dell'esercizio della propria normale attività, possono essere: la distruzione o la perdita, anche accidentale; l'accesso non autorizzato; il trattamento non consentito; il trattamento non conforme alle finalità per le quali è avvenuta la raccolta dei dati personali.

si prende in considerazione la lista dei seguenti eventi:

Categoria A : comportamenti degli operatori:

sottrazione di credenziali di autenticazione
carenza di consapevolezza, disattenzione o incuria
comportamenti sleali o fraudolenti
errore materiale

Categoria B : eventi relativi agli strumenti:

azione di virus informatici o di programmi in grado di recare danno (Malware)
spamming o tecniche di sabotaggio elettronico
malfunzionamento, indisponibilità o degrado degli strumenti di elaborazione
accessi esterni non autorizzati
intercettazione di informazioni in rete

Categoria C : eventi relativi al contesto fisico-ambientale:

ingressi non autorizzati a locali/aree ad accesso ristretto
sottrazione di strumenti contenenti dati
eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi,allagamenti, condizioni ambientali, ecc.), nonché dolosi, accidentali o dovuti ad incuria guasto a sistemi complementari (impianto elettrico, climatizzazione, ecc.), errori umani nella gestione della sicurezza fisica

MISURE IN ESSERE E DA ADOTTARE

Per evitare o ridurre al minimo tutti questi rischi l'Istituto si è dotato di una serie di misure di sicurezza adeguate, di carattere organizzativo, fisico e logico, che riguardano le varie operazioni di trattamento che vengono effettuate ed in particolare la custodia dei dati personali ed il controllo della loro integrità.

L'allegato documento di analisi dei rischi *raccoglie i rischi individuati e le relative misure adeguate che vengono adottate ed eventuali tempi di attuazione e verifica.*

CRITERI E MODALITÀ DI RIPRISTINO DELLA DISPONIBILITÀ DEI DATI

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e **non superiori a sette giorni**.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con **frequenza almeno settimanale e procedure di ripristino ed emergenza in grado di fronteggiare possibili eventi critici di varia natura**.

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

Il presente paragrafo riporta il piano di formazione e le modalità di attuazione:

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Formazione base per neoassunti	INCARICATI/ADDETTI	ENTRO 60 GG DA ASSUNZIONE
Formazione base per nuovi incaricati	INCARICATI/ADDETTI	ENTRO 60 GG DAL NUOVO INCARICO
Formazione base per nuovi responsabili	RESPONSABILI	ENTRO 60 GG DAL NUOVO INCARICO
Informazione del personale	INCARICATI/ADDETTI	MAIL CON TESTO ALLEGATO

PROCEDURE E SISTEMA DI AUDIT PERIODICO

Sono state implementate e rese operative alcune procedure per il rispetto della normativa che vengono allegate, in particolare per la gestione accessi in segreteria, per la progettazione di nuovi trattamenti, per la gestione dei CV e per la modifica e cancellazione dei dati.

Per dimostrare l'applicazione delle procedure e la verifica periodica dei trattamenti effettuati e delle misure in essere sono previsti periodici AUDIT (almeno annuali) effettuati dal DPO con la stesura di apposito verbale o nel caso di AUDIT sul sito WEB di una mail di segnalazione del risultato dell'Audit.

TRATTAMENTI AFFIDATI ALL'ESTERNO, ALL'ESTERO o SU LARGA SCALA

Non sono previsti trattamenti con comunicazione dei dati a paesi terzi all'estero UE o trattamenti biometrici o su LARGA SCALA.
Il trasferimento di dati personali verso l'esterno avviene previo nomina di responsabile al trattamento esterno dell'Ente o della ditta esterna che riceve i dati .

*Per le **piattaforme di workspace** ed i servizi ICT in uso, questi sono conformi al "GDPR" attraverso i relativi accordi di servizio, che costituiscono base giuridica del trattamento ai sensi dell'art. 28 del GDPR. In particolare, tali accordi di servizio prevedono ed autorizzano trasferimenti internazionali dei dati che avvengono sulla base delle garanzie indicate all'art. 46 del GDPR*

Google Workspace for Education riporta :

<<…… può essere utilizzato in conformità con il GDPR. Il nostro Emendamento sul trattamento dei dati è progettato per soddisfare i requisiti di adeguatezza e sicurezza del GDPR; inoltre, la Commissione europea ha creato delle clausole contrattuali tipo per consentire in particolare il trasferimento dei dati personali dall'Europa. I clienti possono aderire all'Emendamento sul trattamento dei dati e alle clausole contrattuali tipo. Nel caso in cui i dati personali vengano trasferiti fuori dall'UE in paesi terzi non coperti da decisioni di adeguatezza, ci impegniamo a fronte dei nostri contratti per il trattamento dei dati a mantenere un meccanismo che faciliti questi trasferimenti secondo quanto stabilito dal GDPR. >>