ISTITUTO COMPRENSIVO DI MOLTENO

Piazza Don Biffi, 1 23847 MOLTENO (LC)

MOP MODELLO OPERATIVO PRIVACY

REDATTO AI SENSI E PER GLI EFFETTI DEGLI ARTT. 24 COMMA 1,30 E 35 DEL REGOLAMENTO DELL'UNIONE EUROPEA 2016/679

CONTIENE:

- **REGISTRO DELLE ATTIVITA' DI TRATTAMENTO (Art. 30 G.D.P.R.)**

Data di elaborazione del documento

29/12/2025

MODELLO REV. 1-2025

STUDIO TECNICO LEGALE
CORBELLINI
Studio AG.I.COM. S.r.l.

Redatto a cura e negli uffici di :
STUDIO AG.I.COM. S.R.L. UNIPERSONALE
Via XXV Aprile, 12 - 20070 SAN ZENONE AL LAMBRO (MI)
Tel. 02 90601324 Fax 02 700527180
R.E.A. - C.F. - P.IVA 05078440962
E-mail info@agicomstudio.it www.agicomstudio.it

SEDI IN CUI VENGONO TRATTATI I DATI (LUOGHI)

Al Titolare del trattamento è affidato il compito di vigilare sui trattamenti di dati personali svolti nell'ambito di ogni luogo a disposizione del Titolare stesso, affinchè venga svolto ad opera del solo personale a ciò autorizzato.

Per l'ente in oggetto i luoghi in cui avviene i trattamenti principali sono collocati presso:

ISTITUTO COMPRENSIVO DI MOLTENO

Piazza Don Biffi, 1
23847 MOLTENO (LC)

Devono intendersi luoghi entro i quali avviene il trattamento dei dati anche i seguenti:

SCUOLA DELL'INFANZIA DI GARBAGNATE MONASTERO - Viale Brianza, 4, Garbagnate Monastero (LC)
SCUOLA PRIMARIA DI MOLTENO - Via Don Biffi, 3, Molteno (LC)
SCUOLA PRIMARIA DI GARBAGNATE MONASTERO - Viale Brianza, 2, Garbagnate Monastero (LC)
SCUOLA PRIMARIA DI ROGENO - Piazza Martiri della Libertà, 1, Rogeno (LC)
SCUOLA PRIMARIA DI SIRONE - Via Molteni, 27, Sirone (LC)
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

ORGANIGRAMMA DEL TRATTAMENTO DEI DATI (PERSONE)

All'interno dell'Istituto il trattamento dei dati personali avviene ad opera di questi soggetti:

TITOLARE DEL TRATTAMENTO DEI DATI

L'ENTE NELLA PERSONA DEL RAPPRESENTANTE LEGALE

MARCO MAGNI

AUTORIZZATI AL TRATTAMENTO

SOGGETTI INTERNI (DIPENDENTI E ASSIMILATI) CHE TRATTANO DATI IN NOME E PER CONTO DEL TITOLARE

ELENCO NOMINATIVO ALLE PAGINE CHE SEGUONO

RESPONSABILI DEL TRATTAMENTO

SOGGETTI ESTERNI CHE TRATTANO DATI IN NOME E PER CONTO DEL TITOLARE CON LORO ORGANIZZAZIONE AUTONOMA IN FORZA DI UN CONTRATTO

ELENCO NOMINATIVO ALLE PAGINE CHE SEGUONO

Il Titolare del trattamento ha individuato specialisti competenti che svolgono compiti di affiancamento tecnico-legale a garanzia dell'adozione di adeguate misure di sicurezza dei dati personali :

DATA PROTECTION OFFICER (D.P.O.)

LUCA CORBELLINI

INCARICATI TECNICI

(ordine alfabetico)

	COGNOME E NOME	SEDE / AZIENDA	RUOLO
1	COLOMBARI MILENA	SEDE	AMM. DI PIATTAFORMA INT.
2	CRISTINELLI ESTER	SEDE	AMM. DI PIATTAFORMA INT.
3	DE COL SARA	SEDE	AMM. DI PIATTAFORMA INT.
4	GRISONI SISTEMI DIDATTICI S.R.L.	Via Canturina, 83/B - 22100 Como (CO)	ADD. MANUTENZ. ESTERNO
5	LAURIO CLAUDIO	SEDE	ADD. MANUTENZ. INTERNO
6	SECCHI GIANCARLO	SEDE	AMM. DI PIATTAFORMA INT.
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Alla pagina che segue il contenuto dei profili di autorizzazione per ciascun ruolo previsto per gli incaricati tecnici.

ELENCO NOMINATIVO DEGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI

Ai fini del presente documento ed in ottemperanza a quanto previsto dal Regolamento UE 2016/679, con il termine "autorizzato" (o incaricato o designato) al trattamento dei dati personali, si intende il soggetto che esegue materialmente le operazioni di trattamento su tali dati con queste prerogative:

- Per tutto il tempo in cui svolgerà le predette mansioni nell'ambito di questo Titolare del trattamento;
- In modalità che potrà essere sia cartacea che digitale;
- Adottando, scrupolosamente, le misure di sicurezza espressamente riportate nel fascicolo recante "Istruzioni Operative", oggetto di formazione specifica somministrata a ciascun soggetto autorizzato.

AUTORIZZATO (ordine alfabetico)	**DESCRIZIONE SINTETICA DELLE AUTORIZZAZIONI**		
ALDEGHI RAFFAELLA	D.S.G.A.		
BARBACINI ANTONINA	DOCENTE	REFERENTE DI PLESSO	
BECCALLI LUIGIA	ASSISTENTE AMMIN.VO		
BONFANTI MARIA CARLA	DOCENTE	REFERENTE DI PLESSO	
BRAMBILLA MARA	ASSISTENTE AMMIN.VO		
CAGLIANI LUCIA	DOCENTE	ANIMATORE/TEAM DIGITALE	
CAPIAGHI LAURA	DOCENTE	REFERENTE DI PLESSO	CONTINUITA'
CASALINIOVO DEBORA	DOCENTE	REFERENTE DI PLESSO	INCLUSIONE
COLOMBARI MILENA	DOCENTE	ANIMATORE/TEAM DIGITALE	PUBBLICAZIONE SITO
CORTI LORENZA	DOCENTE	ANIMATORE/TEAM DIGITALE	
CRISTINELLI ESTER	DOCENTE	ANIMATORE/TEAM DIGITALE	INNOVAZIONE TECN.
DE COL SARA	DOCENTE	INNOVAZIONE TECN.	
FRIGERIO LUCIA	REFERENTE DI PLESSO	REFERENTE PER LA SICUREZZA	CONTINUITA'
FUMAGALLI ELISA	DOCENTE	REFERENTE DI PLESSO	ANIMATORE/TEAM DIGITALE
FUMAGALLI MARIA GRAZIA	DOCENTE	REFERENTE PER LA SICUREZZA	
GIACOMETTI SONIA	REFERENTE DI PLESSO	INVALSI	TUTOR NEO IMMESSI
IEZZI GIULIANA	DOCENTE	REFERENTE PER LA SICUREZZA	
LAURIO CLAUDIO	ASSISTENTE TECNICO		
LOMBARDO FLAVIA	DOCENTE	TUTOR NEO IMMESSI	
MAGGIONI CRISTINA	ORIENTAMENTO	BULLISMO/CYBER	REF SPORTELLO PSICO
MANZONI LUISA ROSA	DOCENTE	REFERENTE PER LA SICUREZZA	CONTINUITA'
MARTINATI VALERIA	DOCENTE	VALUTAZIONE	
MONTRASIO DAVIDE	DOCENTE	REFERENTE PER LA SICUREZZA	
MURANO FRANCESCO	ASSISTENTE AMMIN.VO	R.L.S. INTERNO	
NAVA GIOVANNA	DOCENTE	ANIMATORE/TEAM DIGITALE	
ORIANI MARIA PAOLA	DOCENTE	INCLUSIONE	
PANIZZA GIACOMO	DOCENTE	REFERENTE PER LA SICUREZZA	
PAPAGNA LUCIA	ASSISTENTE AMMIN.VO		
PEREGO FRANCA	DOCENTE	REFERENTE PER LA SICUREZZA	TUTOR NEO IMMESSI
RAMPELLO ALDO	DOCENTE	R.S.P.P. INTERNO	
RIGAMONTI ROSITA	DOCENTE	REFERENTE DI PLESSO	REFERENTE PER LA SICUREZZA
RODA ERNESTINA	VICARIO DEL D.S.	REFERENTE DI PLESSO	REFERENTE PER LA SICUREZZA
RUSCONI SILVIA	DOCENTE	CONTINUITA'	
SANGALLI ELENA	DOCENTE	REFERENTE PER LA SICUREZZA	
SANGALLI SILVIA	DOCENTE	REFERENTE DI PLESSO	REFERENTE PER LA SICUREZZA

(*) LA DEFINIZIONE DETTAGLIATA DI QUESTO RUOLO E' CONTENUTA NELLA LETTERA DI AUTORIZZAZIONE

ELENCO NOMINATIVO DEGLI AUTORIZZATI AL TRATTAMENTO DEI DATI PERSONALI (segue)

AUTORIZZATO (ordine alfabetico)	**DESCRIZIONE SINTETICA DELLE AUTORIZZAZIONI**		
SANGIORGIO SIMONETTA	DOCENTE	INVALSI	
SECCHI GIANCARLO	DOCENTE	INNOVAZIONE TECN.	
SIRONI ESTER	DOCENTE	ANIMATORE/TEAM DIGITALE	
STINGI SALVATORE	ASSISTENTE AMMIN.VO		
TAIANA MIRIAM	DOCENTE	TUTOR NEO IMMESSI	
TENTORIO PAOLA	DOCENTE	COLLABORATORE DEL D.S.	REFERENTE DI PLESSO
VALSECCHI ERIKA	DOCENTE	ANIMATORE/TEAM DIGITALE	
VALSECCHI FABIOLA	DOCENTE	ANIMATORE/TEAM DIGITALE	
VALSECCHI GIUSEPPINA	DOCENTE	ANIMATORE/TEAM DIGITALE	
VALSECCHI ORNELLA	DOCENTE	REFERENTE PER LA SICUREZZA	

(*) LA DEFINIZIONE DETTAGLIATA DI QUESTO RUOLO E' CONTENUTA NELLA LETTERA DI AUTORIZZAZIONE

Il personale autorizzato, sopra elencato, esegue trattamenti secondo questi profili:

	CATEGORIE DI INTERESSATI E FINALITA'
D.S.G.A.	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO E PER IL LORO COORDINAMENTO (A.T.A.) FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE
ASSISTENTE AMMINISTRATIVO	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE I TRATTAMENTI POSSONO ESSERE PARZIALI IN FUNZIONE DEL PIANO DI LAVORO COMUNICATO DAL D.S.G.A.
COLLABORATORE VICARIO DEL DIRIGENTE COLLABORATORE DEL DIRIGENTE REFERENTE DI PLESSO	ALLIEVI ISCRITTI E LICENZIATI/DIPLOMATI PER FINALITA' GESTIONALI ED AMMINISTRATIVE PERSONALE ASPIRANTE, IN SERVIZIO, TRASFERITO ED IN QUIESCENZA PER FINALITA' CONNESSE AL LORO TRATTAMENTO ECONOMICO E GIURIDICO E PER IL LORO COORDINAMENTO FORNITORI PER FINALITA' DI NATURA CONTABILE E PER LA LORO SELEZIONE SVOLGE COMPITI DI COMPLETA SOSTITUZIONE DEL DIRIGENTE SCOLASTICO IN SUA ASSENZA
FUNZIONE STRUMENTALE/REF. PER L'INCLUSIONE	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE INERENTI ANCHE A SOGGETTI CON DISABILITA' O ALTRO BISOGNO SPECIFICO ANCHE SE NON APPARTENENTI ALLE CLASSI ASSEGNATE
FUNZIONE STRUMENTALE/REF. PER L'ORIENTAMENTO FUNZIONE STRUMENTALE/REF. PER LA CONTINUITA' FUNZIONE STRUMENTALE/REF. INVALSI F.S./REF. P.C.T.O. E ALTERNANZA - TUTOR P.C.T.O. FUNZIONE STRUMENTALE/REF. PER L'INTERCULTURA	IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA, PER LA FINALITA' CONNESSA ALLA PROPRIA FUNZIONE E DEFINITA CHIARAMENTE IN SEDE DI DESIGNAZIONE, DATI INERENTI ANCHE A SOGGETTI NON APPARTENENTI ALLE PROPRIE CLASSI
MEMBRO DEL G.L.O.	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE INERENTI AI SOGGETTI CON DISABILITA' A FAVORE DEI QUALI E' STATO ISTITUITO IL G.L.O. DI CUI E' MEMBRO FORMALMENTE DESIGNATO DAL DIRIGENTE SCOLASTICO.
ANIMATORE DIGITALE FUNZIONE STRUMENTALE/REF. PER L'INNOVAZIONE	TRATTA DATI DI NATURA PREVALENTEMENTE COMUNE NELLA PROGETTAZIONE E REALIZZAZIONE DEI PROGETTI DI INNOVAZIONE DIGITALE CONTENUTI NEL PIANO NAZIONALE SCUOLA DIGITALE. IL TRATTAMENTO DATI DEVE INTENDERSI SOLO EVENTUALE E SPECIFICAMENTE RISERVATO ALLA FASE ESECUTIVA.

Segue dalla pagina precedente

RESPONSABILE ALLA PUBBLICAZIONE SUL SITO	IL SOGGETTO TRATTA I DATI AL FINE DI ATTUARE GLI OBBLIGHI DI PUBBLICITA' PREVISTI DALLA VIGENTE NORMATIVA NONCHE' LE PUBBLICAZIONI PER LE QUALI SI E' PREVENTIVAMENTE ACQUISITO ESPLICITO CONSENSO DEGLI INTERESSATI
MEMBRO DELLA COMMISSIONE FORMAZIONE CLASSI	ALLIEVI ISCRITTI AL PRIMO ANNO DEL CICLO DI STUDI PER I QUALI SIA NECESSARIO AVERE UN INQUADRAMENTO GENERALE IN ORDINE AL LORO ANDAMENTO SCOLASTICO ED AI LORO BISOGNI EDUCATIVI SPECIFICI AL FINE DI COSTITUIRE GRUPPI CLASSE UNIFORMI
MEMBRO DEL COMITATO DI VALUTAZIONE	DOCENTI NEOASSUNTI O IN PASSAGGIO DI RUOLO PER I QUALI SIA NECESSARIO RICONOSCERE L'ADEGUATEZZA DELLE COMPETENZE PROFESSIONALI IN SEGUITO AD UNA VALUTAZIONE DELLE ATTIVITA' FORMATIVE PREDISPOSTE, DELLE ESPERIENZE DI INSEGNAMENTO E PARTECIPAZIONE ALLA VITA DELLA SCUOLA
TIROCINANTE / STAGISTA	I TRATTAMENTI DATI AVVENGONO IN SEGUITO ALL'AFFIANCAMENTO DI PERSONALE SCOLASTICO AL FINE DI FORNIRE ALL'AUTORIZZATO LE ABILITA' INDISPENSABILI AD ORGANIZZARE / PROGETTARE / REALIZZARE IN MODO COMPETENTE LE ATTIVITA' TIPICHE DEL RUOLO AFFIANCATO. IL TRATTAMENTO DEI DATI AVVIENE SOTTO STRETTA SORVEGLIANZA DEL SOGGETTO AFFIANCATO. I DATI TRATTATI NON POSSONO ESSERE DIVULGATI.
R.S.P.P. INTERNO A.S.P.P. REFERENTE PER LA SICUREZZA R.L.S.	IL SOGGETTO AUTORIZZATO, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA DATI DI NATURA PARTICOLARE E POTENZIALMENTE ANCHE DATI INERENTI ALLO STATO DI SALUTE (AD ESEMPIO IN SEGUITO AD INFORTUNI O PER L'ADEGUAMENTO DEI PIANI DI EMERGENZA), VOLTI AL CORRETTO SVOLGIMENTO DELL'INCARICO DI R.S.P.P. COME PREVISTO DALL'ART. 33 DEL D.LGS 81/2008.
DOCENTE	IL DOCENTE ACCEDE A DATI DI NATURA IDENTIFICATIVA E DI ANDAMENTO SCOLASTICO DI TUTTI GLI ALLIEVI DELLE CLASSI ASSEGNATE, SIA STABILMENTE CHE PERIODICAMENTE (SUPPLENZE). ACCEDE INOLTRE, POTENZIALMENTE, A DATI DI NATURA PARTICOLARE (SALUTE) E GIUDIZIARIA, NEL CASO DI ALLIEVI CON BISOGNI EDUCATIVI SPECIALI, SEMPRE LIMITATAMENTE AI COMPONENTI DELLE CLASSI ASSEGNATE.
COLLABORATORE AUSILIARIO	IL COLLABORATORE SCOLASTICO, NELL'AMBITO DELLE PROPRIE MANSIONI DI ACCOGLIENZA E SORVEGLIANZA DEGLI ALLIEVI E DI LORO VIGILANZA ED ASSISTENZA NEI MODI E NEI TEMPI PREVISTI DAL CONTRATTO COLLETTIVO DI RIFERIMENTO, PUO' ACCEDERE AI LORO DATI IDENTIFICATIVI. ACCEDE AI DATI IDENTIFICATIVI DEL PERSONALE SCOLASTICO PER FINALITA' ORGANIZZATIVE IN AFFIANCAMENTO ALLA SEGRETERIA.
ASSISTENTE TECNICO	L'ASSISTENTE TECNICO, NELL'AMBITO DELLE PROPRIE MANSIONI DI SUPPORTO TECNICO DIRETTO ALLA ATTIVITA' DIDATTICA LABORATORIALE, PUO' TROVARSI AD ACCEDERE AI DATI IDENTIFICATIVI DEGLI ALLIEVI E DEL PERSONALE (ORARIO DI SERVIZIO DEI DOCENTI ETC.).

Segue dalla pagina precedente

PSICOLOGO / PSICOPEDAGOGISTA INTERNO	TRATTA I DATI RELATIVI A COLORO CHE RICHIEDONO L'ACCESSO ALLO SPORTELLO PSICOLOGICO ISTITUITO A SCUOLA AL FINE DI COSTRUIRE BUONE RELAZIONI ED UNA STABILE BASE DI CRESCITA SIA RIVOLTA AGLI ALLIEVI CHE AL PERSONALE CHE NE FACCIA RICHIESTA. SVOLGE ATTIVITA' DI CONSULENZA E SUPPORTO.
AUTORIZZATO CONSULTAZIONE IMMAGINI VIDEOSORV.	SONO INTERESSATI TUTTI I SOGGETTI CHE SI INTRODUCONO NEI LOCALI SCOLASTICI DURANTE GLI ORARI DI ATTIVAZIONE DELL'IMPIANTO, LA REGISTRAZIONE AVVIENE AL FINE DI SCONGIURARE FURTI, VANDALISMI ED ACCESSI IMPROPRI AI LOCALI
F.S./REF. PER IL BULLISMO / CYBERBULLISMO	IL DOCENTE, IN AGGIUNTA ALLE AUTORIZZAZIONI AL TRATTAMENTO INERENTI AL PROPRIO RUOLO ORDINARIO, TRATTA, PER LA FINALITA' CONNESSA ALLA PROPRIA FUNZIONE E DEFINITA CHIARAMENTE IN SEDE DI DESIGNAZIONE, DATI INERENTI ANCHE A SOGGETTI NON APPARTENENTI ALLE PROPRIE CLASSI
REFERENTE SPORTELLO PSICOLOGICO	IL REFERENTE SI OCCUPA DELLA GESTIONE DELL'AGENDA DELLO PSICOLOGO / PSICOPEDAGOGISTA, INTERFACCIANDOSI CON ESSO, CON GLI ALLIEVI E TALVOLTA CON LE LORO FAMIGLIE AL FINE DI ORGANIZZARE INCONTRI ED ATTIVITA'
ADDDETTO ALLA SOMMINISTRAZIONE DI FARMACI	L'ADDETTO CHE HA MANIFESTATO, SU BASE VOLONTARIA, LA PROPRIA DISPONIBILITA', ACCEDE A DATI DI NATURA IDENTIFICATIVA E PARTICOLARE (SALUTE), NEL CASO DI ALLIEVI CHE ABBIANO FATTO RICHIESTA DIRETTAMENTE O MEDIANTE I LORO GENITORI/TUTORI, DI SOMMINISTRAZIONE DI FARMACI IN ORARIO SCOLASTICO.

Tutti i soggetti autorizzati sopra elencati, hanno ricevuto una lettera di autorizzazione allo scopo di chiarire il perimetro di tali autorizzazioni.
Ogni autorizzato al trattamento riceve, oltre ad una formazione specifica organizzata a cadenza periodica, al fine di coprire anche i nuovi arrivati in corso di anno, anche un documento recante "Istruzioni operative" nel quale sono riportate le indicazioni specifiche a cui rifarsi durante le operazioni di trattamento dati.

ELENCO NOMINATIVO DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

L'Art. 28 del G.D.P.R. prevede che il Titolare possa nominare un Responsabile che effettui il trattamento per suo conto.
Ai fini del presente documento ed in ottemperanza a quanto previsto dal Regolamento UE 2016/679, con il termine "Responsabile del trattamento dei dati personali", intendiamo un soggetto esterno (questa tendenza ad escludere che il Responsabile possa essere un dipendente del Titolare è di gran lunga l'interpretazione più convincente) che si occupa di trattare i dati in nome e per conto del Titolare.
Appurato che il Responsabile è un esterno, la conseguenza è che il Titolare non può esercitare, su di esso, quei poteri di indirizzo e controllo tipici del rapporto di lavoro subordinato, ed è proprio con il "Contratto di nomina a Responsabile del trattamento" che ciò avviene in seguito all'instaurazione di questo nuovo rapporto contrattuale.
Il contratto di nomina a Responsabile del trattamento quasi sempre affianca un "contratto sottostante" con il quale il Titolare ha individuato il soggetto esterno per svolgere un incarico che comporterà il trattamento di dati (R.S.P.P., Medico Competente, D.P.O., Tesoreria, Registro elettronico etc.), obiettivo di questo atto è proprio quello di integrare tale contratto sottostante per tutte quelle questioni che non sono disciplinate all'interno di questo (data breach, audit etc.).

	Studio AG.I.COM. S.r.l.	Via XXV Aprile, 12
	C/A Dott. Luca Corbellini	20070 SAN ZENONE AL LAMBRO (MI)
1	**LA DESIGNAZIONE DI PERSONALE INCARICATO DAL FORNITORE A DATA PROTECTION OFFICER (D.P.O.) DELL'ISTITUTO SCOLASTICO**	

	Madisoft S.p.a.	Via G. Falcone, 5
	C/A Amministrazione	62010 POLLENZA (MC)
2	**LA FORNITURA DEL SERVIZIO DI GESTIONE DEL REGISTRO ELETTRONICO**	

	Madisoft S.p.a.	Via G. Falcone, 5
	C/A Amministrazione	62010 POLLENZA (MC)
3	**LA FORNITURA DEL SERVIZIO DI GESTIONE DIGITALE DEGLI UFFICI DI SEGRETERIA**	

	Google Ireland Limited	Gordon House, Barrow Street
	C/A Amministrazione	Dublin 4 Ireland
4	**LA FORNITURA DEL SERVIZIO DI PIATTAFORMA DIDATTICA DIGITALE**	

	Crédit Agricole Italia S.p.a.	Via Giuseppe Parini, 21
	C/A Amministrazione	23900 LECCO (LC)
5	**SERVIZIO DI CASSA**	

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

AMMINISTRATORE DI SISTEMA

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI DI TUTTE LE TIPOLOGIE (COMUNI, PARTICOLARI E GIUDIZIARI)	DATI DI ALLIEVI, PERSONALE E FORNITORI, TRATTATI ALL'UNICO FINE DI GESTIONE E MANUTENZIONE DEGLI IMPIANTI DI ELABORAZIONE ENTRO CUI SONO CUSTODITI O DI LORO COMPONENTI SIA HARDWARE CHE SOFTWARE LIMITATAMENTE ALL'AMBITO / PIATTAFORMA DI COMPETENZA.

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Adottare sistemi di registrazione degli accessi (log) degli amministratori ai sistemi di elaborazione ed agli archivi. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo (almeno sei mesi);

Sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, antivirus, filtri etc.);

Monitorare lo stato dei sistemi, con particolare attenzione alla loro sicurezza;

Effettuare in prima persona o sovraintendere agli interventi di manutenzione hardware ed a quelli software su sistemi operativi e applicativi;

Sovrintendere all'operato di eventuali tecnici esterni;

Fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'autorizzato l'accesso a PC, device e piattaforme, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;

Gestire le password di root o di amministratore di sistema;

Collaborare con il Titolare del trattamento, i Responsabili ed il Data Protection Officer;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

Adottare le misure di sicurezza previste dalla legge e dalle D.P.I.A. eseguite, all'infrastruttura informatica di competenza;

Redigere annualmente un resoconto in ordine alla rispondenza della infrastruttura informatica di competenza, ai requisiti di sicurezza previsti dalle normative vigenti;

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

ADDETTO ALLA GESTIONE/MANUTENZIONE DI SISTEMA INFORMATICO

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI DI TUTTE LE TIPOLOGIE (COMUNI, PARTICOLARI E GIUDIZIARI)	DATI DI ALLIEVI, PERSONALE E FORNITORI, TRATTATI ALL'UNICO FINE DI GESTIONE E MANUTENZIONE DEGLI IMPIANTI DI ELABORAZIONE ENTRO CUI SONO CUSTODITI O DI LORO COMPONENTI SIA HARDWARE CHE SOFTWARE LIMITATAMENTE ALL'AMBITO / PIATTAFORMA DI COMPETENZA.

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Effettuare interventi di manutenzione e recupero di dati, documenti e archivi;

Eseguire richieste di spostamento, ricollocazione, distruzione di dati o archivi;

Acquisire e conservare temporaneamente i dati di log di accesso ad internet, quelli relativi ad attacchi di maleware in generale quali virus e trojan nonché quelli relativi a tentativi di intrusione;

Configurare periferiche di stampa ed acquisizione dati;

Configurare sistemi di backup del dati;

Allocare temporaneamente gli archivi dati su propri sistemi o cloud per consentire la regolare esecuzione degli interventi manutentivi o di configurazione;

In caso di ritiro di P.C. o device in genere e loro traslocazione temporanea presso laboratori tecnici per l'impossibilità di eseguire l'intervento in loco, adottare misure di sicurezza adeguate ad impedire a terzi l'accesso ai dati;

Eseguire interventi di pulizia dei sistemi da virus e di ottimizzazione delle prestazioni dei singoli device;

Installare software di gestione remota dei dati da attivare solamente previo informazione ed espresso consenso del soggetto a cui il PC / device è in uso;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

-

Il personale tecnico autorizzato esegue questa tipologia di trattamenti:

AMMINISTRATORE DI PIATTAFORMA DIGITALE

BASE DATI E LORO TIPOLOGIA	CATEGORIE DI INTERESSATI E FINALITA'
DATI PERSONALI COMUNI	DATI DI ALLIEVI E PERSONALE, TRATTATI AL FINE DELLA CREAZIONE DELLE UTENZE DI ACCESSO ALL'AMBITO / PIATTAFORMA DI COMPETENZA E DELLA SUA AMMINISTRAZIONE.

L'incarico di amministrazione viene svolto sulle principali piattaforme in uso all'interno dell'Istituto scolastico (segreteria digitale, registro elettronico, piattaforma didattica integrata etc.).

Quando interno all'Istituto Scolastico agisce in qualità di "AUTORIZZATO ALL'ACCESSO AL SISTEMA INFORMATICO" mentre, quando esterno, viene designato quale "RESPONSABILE DEL TRATTAMENTO" ai sensi dell'Art. 28 del G.D.P.R..

Di seguito i compiti assegnati:

Assicurare la custodia delle credenziali amministrative per la gestione dei sistemi di autenticazione e autorizzazione in uso e di prossima attivazione;

Creare e gestire gli utenti assegnando a ciascuno solamente i poteri di accesso che gli sono propri, ossia la possibilità di accesso ai soli dati riferiti alle classi di pertinenza;

Creare, se necessario, gruppi di utenti in base alle loro risorse utilizzabili;

Prestare assistenza nell'attivazione e configurazione di servizi legati alla piattaforma, nell'ottica della dematerializzazione e digitalizzazione dei documenti;

Informare senza ritardo il Titolare del trattamento di tutte le questioni che possano far temere il prodursi di un data breach e fornire assistenza allo stesso in ordine alla sua eventuale notifica al Garante ed agli interessati;

-

-

-

-

-

-

Terminiamo questa parte introduttiva di presentazione anagrafica delle sedi in cui avviene il trattamento e dell' organigramma dello stesso, per passare, alle pagine che seguono, ad analizzare nello specifico le attività di trattamento svolte.

INDICE

I. SCOPO DEL DOCUMENTO

Il Modello Organizzativo Privacy è uno strumento strategico che consente al Titolare del trattamento di gestire in modo responsabile e documentato tutti gli adempimenti previsti dal GDPR, dimostrare la conformità delle attività di trattamento dei dati personali, garantire la continuità nel tempo del percorso di adeguamento, anche in caso di cambiamenti organizzativi e dialogare efficacemente con le autorità di controllo, offrendo un quadro chiaro e strutturato delle misure adottate.

Parte essenziale del modello organizzativo è il **Registro delle attività di trattamento** allegato al presente documento e costituito da una tabella complessa che permette la precisa rendicontazione dei trattamenti svolti nonché la valutazione dei rischi connessi a tali trattamenti e la individuazione delle relative contromisure.
Esso viene aggiornato ogni anno per garantire una perfetta aderenza del contenuto dello stesso alle modificate esigenze di sicurezza nonché, al variare nel tempo, del profilo dei rischi incombenti sui dati.

All'interno del documento vengono definiti i criteri per:

I. La protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ai medesimi locali;
II. I criteri e le procedure per assicurare l'integrità dei dati;
III. I criteri e le procedure per la sicurezza della trasmissione dei dati, ivi compresi quelli per le redazioni di accesso per via telematica;
IV. L'elaborazione di un piano di formazione per rendere edotti gli autorizzati al trattamento dei rischi individuati e dei modi per prevenire i danni.

Il presente documento è redatto e firmato in calce dal Titolare del trattamento e dal Responsabile della Protezione dei Dati (R.P.D. – D.P.O.).

II. AMBITO DI APPLICAZIONE DEL DOCUMENTO

Il presente modello è applicato ai trattamenti di dati che avvengono all'interno delle strutture di competenza del titolare, ovunque esse si trovino sul territorio europeo.
Si forniscono inoltre idonee informazioni riguardanti:

a) l'elenco dei trattamenti di dati personali mediante:

- Individuazione tipologia di dati trattati
- Descrizione aree, locali e strumenti con cui si esegue il trattamento
- Elaborazione mappa dei trattamenti effettuati

b) la distribuzione dei compiti e delle responsabilità e la previsione di interventi formativi degli autorizzati individuati dal presente;

c) l'analisi dei rischi che incombono sui dati;

d) le misure adottate e da adottare per garantire l'integrità e la disponibilità dei dati;

e) i criteri e le modalità di ripristino dei dati, in seguito a distruzione o danneggiamento;

f) i criteri da adottare per garantire l'adozione delle misure di sicurezza dei dati

g) le procedure per seguire il controllo dello stato di sicurezza

Le procedure contenute nel presente documento devono essere conosciute ed applicate da tutti gli uffici ed i reparti su cui è strutturato l'ente titolare del trattamento.

III. FONTI DEL DIRITTO

Il Modello Operativo Privacy (M.O.P.) e le disposizioni che esso contiene sono conformi a quanto previsto dagli articoli 24 comma 1, 30 e 35 del Regolamento dell'Unione Europea 2016/679.

IV. SOGGETTI DEL TRATTAMENTO DEI DATI

La normativa vigente ha definito talune figure fondamentali a cui attribuisce ruoli chiave nei vari passaggi su cui è strutturato il trattamento dei dati.

Queste figure sono:

IL TITOLARE DEL TRATTAMENTO DEI DATI PERSONALI

La persona giuridica o l'Istituzione statale è, "*ope legis*", per mezzo del suo rappresentante legale, TITOLARE DEL TRATTAMENTO.
Quale Titolare del trattamento gli è consentito individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurino che vengano adottate le misure di sicurezza previste dalla legge per il trattamento dei dati come le misure tese a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto dal Titolare stesso

IL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI

In relazione all'attività del Titolare del trattamento, è prevista come facoltativa, la nomina del Responsabile del trattamento, con compiti specifici in relazione alle funzioni svolte. Il Titolare del trattamento se vuole, affida al Responsabile del trattamento l'onere di individuare, nominare ed indicare per iscritto uno o più autorizzati al trattamento appartenenti alla propria organizzazione.

Il Titolare (ed il Responsabile del trattamento dei dati se designato) hanno il compito di:

- Redigere ed aggiornare ad ogni variazione l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco dei trattamenti effettuati;
- Attribuire ad ogni Utente (USER) o autorizzato un Codice identificativo personale (USER ID) per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile;
- Autorizzare i singoli autorizzati al trattamento e della manutenzione, qualora utilizzino elaboratori accessibili in rete e nel caso di trattamento di dati sensibili e giudiziari; per gli stessi dati, qualora il trattamento sia effettuato tramite elaboratori accessibili in rete disponibile al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare;
- Verificare, con cadenza almeno semestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali;
- Garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'ente siano applicate all'interno ed eventualmente al di fuori dello stesso, qualora cedute a soggetti terzi, quali Responsabili del trattamento, tutte o parte delle attività di trattamento;

Il Titolare del trattamento dei dati deve informare il Responsabile del trattamento dei dati delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, e dall'accordo contrattuale o di altra natura che egli ha concluso con questo.

La nomina del Responsabile del trattamento può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso, ed eventualmente affidata ad altro soggetto.

AUTORIZZATI AL TRATTAMENTO DEI DATI

Al Titolare del trattamento (ed al Responsabile del trattamento se nominato e per quanto attiene alla propria struttura) è affidato il compito di individuare uno o più autorizzati del trattamento dei dati. Tale designazione è funzionale (ma non strettamente obbligatorio) che avvenga per iscritto e che dal documento di autorizzazione siano facilmente desumibili i compiti che gli sono affidati.
Gli autorizzati al trattamento devono ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.
Agli autorizzati deve essere assegnata una parola chiave e un codice identificativo personale, salvo che non siano in uso altri sistemi di identificazione individuale.
La nomina degli autorizzati al trattamento deve essere controfirmata dall'interessato per presa visione e copia della stessa deve essere conservata a cura del Titolare/Responsabile del trattamento per la sicurezza dei dati in luogo sicuro.
Agli autorizzati al trattamento il Titolare/Responsabile del trattamento per la sicurezza dei dati deve consegnare una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli autorizzati è a tempo indeterminato e decade per revoca, per dimissioni o con il venir meno dei compiti che giustificavano il trattamento dei dati personali.

V. REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DI DATI PERSONALI DELL'ISTITUTO SCOLASTICO

Il registro delle attività di trattamento è la parte principale di questo documento e fornisce una rappresentazione dell'organizzazione sotto il profilo delle attività di trattamento dei dati personali.
Esso ha lo scopo di dare consapevolezza e condivisione interna del processo di gestione del dato.

Il suo contenuto è prescritto dall'art. 30 del GDPR, queste le informazioni da includere:

- dati di contatto del titolare del trattamento e, dove applicabile, del contitolare del trattamento e del Responsabile della protezione dei dati;
- finalità del trattamento, le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative.

Al fine di descrivere le misure di sicurezza tecniche ed organizzative attuate dall'Istituto a tutela dei dati, occorre eseguire una valutazione preliminare dei rischi incombenti su questi. Infatti, il GDPR predilige l'approccio c.d. "risk-based", cioè basato sul concetto di "rischio" circa il verificarsi di un evento che possa determinare una violazione dei dati.

Il Considerando 75 definisce il rischio in questo modo: "*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".

Un rischio è quindi uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla probabilità di accadimento (P) ed alle conseguenze ragionevolmente attese dal verificarsi di tale evento (G).

Dalla combinazione di queste grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

$$R = P \times G$$

R = livello di rischio
P = probabilità di accadimento
G = conseguenze (gravità dei danni attesi)

Alla probabilità di accadimento dell'evento (P) è associato un indice numerico rappresentato nella seguente tabella:

Legenda dei valori di probabilità (P)

QUASI SICURO (5)	La struttura è destinata a incorrere in incidenti di questa natura nell'immediato.
PROBABILE (4)	E' possibile che incidenti di questa natura si verifichino a breve.
POSSIBILE (3)	E' possibile sperimentare incidenti di questa natura.
IMPROBABILE (2)	incidenti di questo tipo sono rari, ma c'è una reale possibilità che si possano
RARO (1)	Sebbene siano concepibili, probabilmente non si verificheranno mai incidenti di

Alle conseguenze (G) è associato un indice numerico rappresentato nella seguente tabella:

Legenda dei valori di gravità (G)

ESTREMO (5)	Completo fallimento di gestione della privacy, perdita o cancellazione dei dati, trattamento illecito, irrisolvibile.
SIGNIFICATIVO (4)	Grave perdita di capacità di gestione della privacy, perdita o cancellazione dei dati altamente dannosa ed estremamente
MODERATO (3)	Impatto operativo sostanziale sui diritti degli interessati, molto costoso.
LIEVE (2)	Impatto operativo limitato sui diritti degli interessati, alcuni costi.
INSIGNIFICANTE (1)	Minimo su qualsiasi impatto dei diritti degli interessati. Costi trascurabili.

La matrice che scaturisce dalla combinazione di probabilità e conseguenze è rappresentata in figura seguente:

	VALORE DI GRAVITA' DEL DANNO (G)					
PROBABILITA' DI ACCADIMENTO DELL'EVENTO PREVISTO (P)	R	ESTREMO (5)	SIGNIFICATIVO (4)	MODERATO (3)	LIEVE (2)	INSIGNIFICANTE (1)
	QUASI SICURO (5)	25 ALTISSIMO (AA)	20 ALTO (A)	15 MEDIO-ALTO (MA)	10 MEDIO-BASSO (MB)	5 BASSO (B)
	PROBABILE (4)	20 ALTO (A)	16 MEDIO-ALTO (MA)	12 MEDIO (M)	8 MEDIO-BASSO (MB)	4 BASSO (B)
	POSSIBILE (3)	15 MEDIO-ALTO (MA)	12 MEDIO (M)	9 MEDIO-BASSO (MB)	6 MEDIO-BASSO (MB)	3 BASSO (B)
	IMPROBABILE (2)	10 MEDIO-BASSO (MB)	8 MEDIO-BASSO (MB)	6 MEDIO-BASSO (MB)	4 BASSO	2 BASSO (B)
	RARO (1)	5 BASSO (B)	4 BASSO (B)	3 BASSO (B)	2 BASSO (B)	1 BASSO (B)

Si ricava così, per ogni attività di trattamento, un livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati) che convenzionalmente riteniamo possa assumere i seguenti valori:

Legenda del rischio (R = P x G)

ALTISSIMO (AA) 23-25	RISCHIO NON ACCETTABILE DA ELIMINARE CON PRIORITA' MASSIMA
ALTO (A) 19-22	RISCHIO NON ACCETTABILE DA ELIMINARE
MEDIO-ALTO (MA) 15-18	RISCHIO NON ACCETTABILE DA MITIGARE CON AZIONI CORRETTIVE
MEDIO (M) 11-14	RISCHIO NON ACCETTABILE DA MITIGARE CON AZIONI DI MIGLIORAMENTO
MEDIO-BASSO (MB) 6-10	RISCHIO ACCETTABILE
BASSO (B) 1-5	RISCHIO TRASCURABILE

Per ciascun trattamento censito infine, è necessario valutare se debba essere prodotta la DPIA, acronimo di "*Data Protection Impact Assessment*", ossia una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

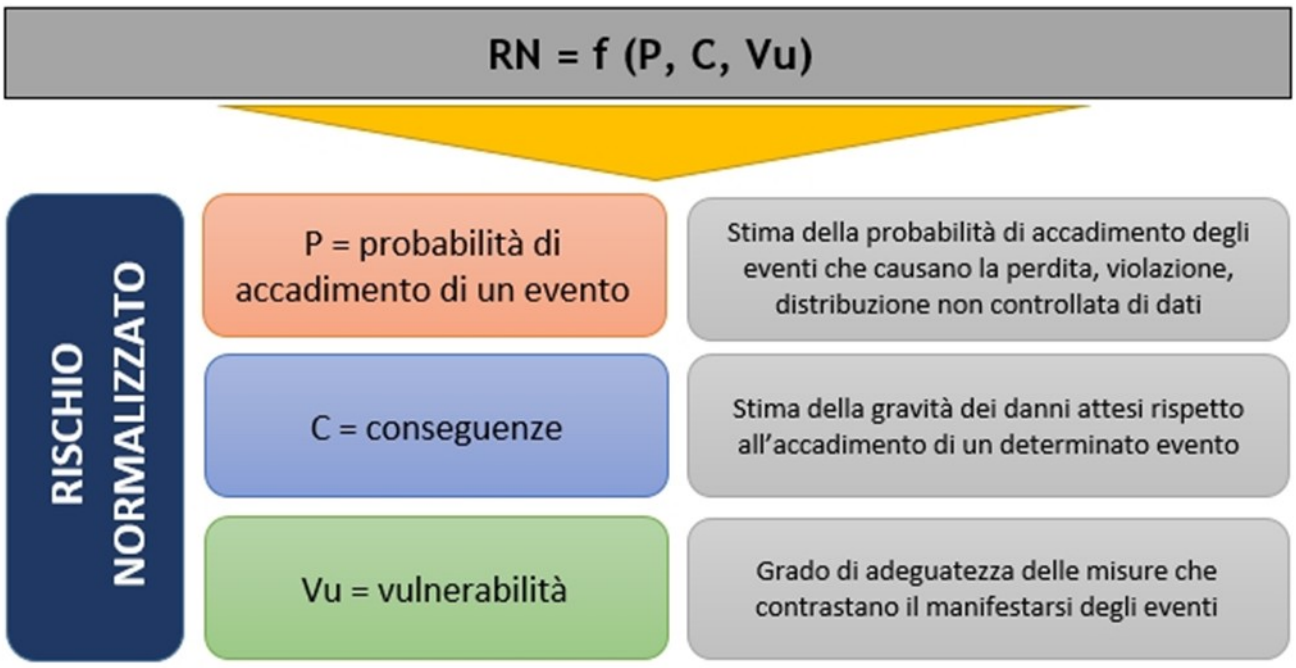
In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679), livello di rischio che si presume sussistere quando ci troviamo in una delle circostanze indicate nel Provvedimento del Garante n. 467 del 11 ottobre 2018 e che sono dettagliatamente indicate nel registro delle attività di trattamento dell'Istituto.

La DPIA, se necessaria, si basa su un'analisi dei rischi più dettagliata di quella di base descritta sopra, in cui si cerca di dare un peso ai possibili controlli applicabili, passando così da un indice di rischio "intrinseco" ad un indice di rischio "normalizzato" rispetto al contesto scolastico.

Il rischio (che definiamo "normalizzato") viene calcolato non più in funzione di 2 fattori, ma di 3:

$$RN = f(P, G, Vu)$$

P = probabilità
G = conseguenze generate dall'evento
Vu = vulnerabilità rispetto al grado di adeguatezza delle misure



Partendo dal valore di rischio (che chiamiamo convenzionalmente "Rischio Intrinseco") calcolato secondo la modalità prima descritta, per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla Vulnerabilità (Vu) è associato un indice numerico rappresentato nella seguente tabella:

Legenda dei valori di vulnerabilità (Vu)

INADEGUATE	1
PARZIALMENTE ADEGUATE	0,5
ADEGUATE	0,25

Quindi, per ogni rischio, vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori sopra indicati.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

		RISCHIO INTRINSECO (Ri)					
	RN	ALTISSIMO	ALTO	MEDIO-ALTO	MEDIO	MEDIO-BASSO	BASSO
VULNERABILITA' (Vu)	INADEGUATE (1)	ALTO	RILEVANTE	RILEVANTE	RILEVANTE	BASSO	BASSO
	PARZIALMENTE ADEGUATE (0,5)	RILEVANTE	BASSO	BASSO	BASSO	MOLTO BASSO	MOLTO BASSO
	ADEGUATE (0,25)	BASSO	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO	MOLTO BASSO (1-5)

Legenda dei valori del rischio normalizzato (RN)

ALTO	Consultare preventivamente il Garante ed attendere la sua valutazione
RILEVANTE	Adottare importanti misure di contenimento del rischio e migliorare il numero e l'efficacia delle misure di sicurezza adottate
BASSO	Adottare misure di contenimento del rischio e migliorare l'efficacia delle misure di sicurezza adottate
MOLTO BASSO	E' possibile eseguire il trattamento

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante, in tutti gli altri casi, salvo che nel caso di rischio MOLTO BASSO, si attiva per adottare misure di sicurezza supplementari che possano consentire una ulteriore diminuzione del valore di rischio normalizzato.

La DPIA non è l'unica forma di valutazione dei rischi di secondo livello; infatti, nel Registro delle attività di trattamento sono riportate anche la LIA (Legitimate Interest Assessment o Bilanciamento del Legittimo Interesse) da compilarsi ogniqualvolta la base giuridica di un trattamento sia il legittimo interesse (art. 6 par.1 lett. f G.D.P.R.) al fine di dimostrare che il proprio interesse non prevalga sui diritti e le libertà fondamentali dell'interessato.

Introdotta dal Regolamento UE 2024/1689 (AI Act) la FRIA (Fundamental Rights Impact Assessment o Valutazione di Impatto sui Diritti Fondamentali), anch'essa contenuta nel Registro delle attività di trattamento allegato al presente documento, è uno strumento per valutare l'impatto che un sistema di Intelligenza Artificiale (IA) può avere sui diritti fondamentali delle persone.

Il Ministero dell'Istruzione, mediante il Regolamento dei dati sensibili e giudiziari (D.M. 305 del 07/12/2006), ha identificato in maniera precisa quali trattamenti dei dati sono consentiti all'interno di una istituzione scolastica. Per fare questo ha utilizzato il sistema delle **SCHEDE,** indicando, in ciascuna di esse, le tipologie di dati sensibili e giudiziari e di operazioni su di essi indispensabili per la gestione del sistema dell'Istruzione in un particolare comparto della stessa.
Preventivamente ha però individuato, all'Art. 2, dei limiti oggettivi entro i quali rimanere anche in caso di operazioni legittime su dati sensibili o giudiziari; infatti, tutti i dati sensibili e giudiziari individuati dal regolamento in oggetto possono essere trattati previo verifica della loro:

PERTINENZA
Cioè i dati personali raccolti devono essere riferibili perfettamente all'interessato ed alla finalità del trattamento, sia nella loro forma individuale che nella forma più complessa dei documenti che li contengono.

COMPLETEZZA
Cioè i dati personali devono essere raccolti nella loro interezza onde evitare errori di valutazione che possano derivare dalla loro non completezza.

INDISPENSABILITA'
Cioè assolutamente indispensabili per raggiungere lo scopo prefissato.

SCHEDA N° 1 SELEZIONE, RECLUTAMENTO, INSTAURAZIONE, GESTIONE E CESSAZIONE DEL RAPPORTO DI LAVORO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
STATO DI SALUTE	Stato giuridico, idoneità al servizio, assunzione categoria protette, protezione maternità, igiene e sicurezza dei luoghi di lavoro, onoreficenze, assicurazioni, trattamenti assistenziali e previdenziali, denunce infortuni, malattie professionali, fruizione permessi, assenze giustificate.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 62 - Rilascio documenti di riconoscimento Art. 67 - Attività di controllo ed ispettive Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 70 - Obiezione di coscienza Art. 72 - Rapporti con Enti di culto Art. 73 - Supporto al collocamento e avviamento al lavoro
ADESIONE A SINDACATI	Versamento quote di iscrizione, esercizio diritti sindacali.	
CONVINZIONI RELIGIOSE	Concessione permessi e festività religiose, reclutamento docenti di religione.	
CONVINZIONI FILOSOFICHE	Svolgimento sevizio di leva come obiettore di coscienza.	
DATI GIUDIZIARI	Valutazione requisiti di ammissione, adozione di provvedimenti amministrativo-contabili.	
VITA SESSUALE	Rettificazione attribuzione di sesso	

COMUNICAZIONI DI DATI CONSENTITE

SERVIZI SANITARI COMPETENTI PER VISITE FISCALI ED ACCERTAMENTO IDONEITA' ALL'IMPIEGO;
ORGANI PREPOSTI ALLA VIGILANZA IN MATERIA DI IGIENE E SICUREZZA LUOGHI DI LAVORO (D.Lgs. 626/1994 oggi D.Lgs 81/2008);
ENTI ASSISTENZIALI, PREVIDENZIALI ED ASSICURATIVI;
AMMINISTRAZIONI PROVINCIALI PER GLI ASSUNTI EX L. 68/1999;
ORGANIZZAZIONI SINDACALI PER GESTIONE PERMESSI E VERSAMENTO QUOTA DI ISCRIZIONE;
PUBBLICHE AMMINISTRAZIONI VERSO LE QUALI SONO ASSEGNATI I DIPENDENTI IN MOBILITA';
ORDINARIO DIOCESANO PER IDONEITA' ALL'INSEGNAMENTO DELLA RELIGIONE CATTOLICA;
ORGANI DI CONTROLLO (CORTE DEI CONTI e MEF);
AGENZIA DELLE ENTRATE;
PRESIDENZA DEL CONSIGLIO DEI MINISTRI PER LA RILEVAZIONE ANNUALE DEI PERMESSI PER CARICHE SINDACALI ETC.

SCHEDA N° 2 GESTIONE DEL CONTENZIOSO E PROCEDIMENTI DISCIPLINARI

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla difesa in giudizio del Ministero della Pubblica Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro, amministrativo, penale e civile.	Art. 112 - Instaurazione e gestione rapporti di lavoro da parte di soggetto pubblico. Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

COMUNICAZIONI DI DATI CONSENTITE

MINISTERO DEL LAVORO PER SVOLGIMENTO TENTATIVI OBBLIGATORI DI CONCILIAZIONE;
ORGANI ARBITRALI PER SVOLGIMENTO PROCEDURE ARBITRALI INDICATE NEI CCNL;
AVVOCATURA DELLO STATO PER DIFESA E CONSULENZA;
MAGISTRATURA E ORGANI DI POLIZIA GIUDIZIARIA;
LIBERI PROFESSIONISTI A FINI DI PATROCINIO E CONSULENZA, INCLUSI QUELLI DI CONTROPARTE.

SCHEDA N° 3 ORGANISMI COLLEGIALI E COMMISSIONI ISTITUZIONALI

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Attivazione degli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero dell'Istruzione e dell'ordinamento scolastico.	Art. 65 - pubblicità dell'attività di organi. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.

COMUNICAZIONI DI DATI CONSENTITE

NESSUNA, ATTIVITA' INTERNA ALL'ISTITUZIONE SCOLASTICA.

SCHEDA N° 4 ATTIVITA' PROPEDEUTICHE ALL'AVVIO DELL'ANNO SCOLASTICO

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli ALLIEVI di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.	
STATO DI SALUTE	Per assicurare l'erogazione del sostegno agli ALLIEVI diversamente abili e per la composizione delle classi	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti, o qualora l'Autorità Giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno o ALLIEVI che abbiano commesso reati.	

COMUNICAZIONI DI DATI CONSENTITE

ENTI LOCALI PER LA FORNITURA DI SERVIZI;
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALLIEVI E DI SUPPORTO;
AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP.

SCHEDA N° 5 ATTIVITA' EDUCATIVA, DIDATTICA E FORMATIVA, DI VALUTAZIONE

DATI SENSIBILI O GIUDIZIARI	TRATTAMENTI CONSENTITI	FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE
ORIGINI RAZZIALI ED ETNICHE	Per tutti quegli atti tesi a favorire l'integrazione degli ALLIEVI di nazionalità non italiana.	Art. 68 - Applicazione disciplina benefici economici ed altri emolumenti. Art. 73 - Supporto al collocamento e avviamento al lavoro Art. 86 - Tutela maternità, disincentivazione uso sostanze psicotrope, integrazione diversamente abili, volontariato. Art. 95 - dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico.
CONVINZIONI RELIGIOSE	Per garantire la libertà di credo religioso.	
STATO DI SALUTE	Per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli ALLIEVI diversamente abili, dell'insegnamento domiciliare ed ospedaliero, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate ed ai viaggi di istruzione.	
DATI GIUDIZIARI	Per assicurare il diritto allo studio a soggetti detenuti.	
CONVINZIONI POLITICHE	Per la costituzione ed il funzionamento delle Consulte e delle Associazioni di studenti e dei genitori.	
DATI SENSIBILI IN GENERALE	In generale per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.	

COMUNICAZIONI DI DATI CONSENTITE

ALTRE ISTITUZIONI SCOLASTICHE STATALI E NON PER TRASMISSIONE DOCUMENTAZIONE ATTINENTE LA CARRIERA;
ENTI LOCALI PER FORNITURA SERVIZI;
GESTORI PUBBLICI E PRIVATI DI SERVIZI DI ASSISTENZA AGLI ALLIEVI E DI SUPPORTO;
ISTITUTI DI ASSICURAZIONE PER DENUNCIA INFORTUNI E CONNESSA R.C.;
ALL'INAIL PER LA DENUNCIA INFORTUNI;
AUSL ED ENTI LOCALI PER FUNZIONAMENTO GRUPPI DI LAVORO HANDICAP;
AZIENDE, IMPRESE ED ALTRI SOGGETTI PUBBLICI O PRIVATI PER STAGES.

SCHEDA N° 6	SCUOLE NON STATALI	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
FASCICOLI PERSONALI DI DOCENTI E ALLIEVI	Per rendere effettiva l'attività di vigilanza e controllo eseguita dall'Amministrazione centrale o periferica nei confronti delle scuole non statali parificate.	Art. 67 - Attività di controllo ed ispettive

SCHEDA N° 7	RAPPORTI SCUOLA-FAMIGLIA, GESTIONE DEL CONTENZIOSO	
DATI SENSIBILI O GIUDIZIARI	**TRATTAMENTI CONSENTITI**	**FINALITA' DI RILEVANTE INTERESSE PUBBLICO PERSEGUITE**
TUTTI I DATI SENSIBILI E GIUDIZIARI LECITAMENTE TRATTATI	Tutte le attività relative alla instaurazione del contenzioso (reclami, ricorsi, esposti, provvedimenti disciplinari, ispezioni, citazioni, denunce etc.) con gli ALLIEVI e le famiglie e tutte le attività di difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado.	Art. 67 - Attività di controllo ed ispettive Art. 71 - Attività sanzionatoria e di tutela

VI. LE MISURE DI SICUREZZA GLOBALI

La Legge, dapprima con il Decreto Legislativo 196/2003 e poi con il Regolamento UE 2016/679 definisce con il termine "misure di sicurezza", una serie di prescrizioni tecniche indispensabili affinché il trattamento dei dati personali, eseguito mediante l'impiego di apparecchiature elettroniche, sia sicuro.
Mentre la grande maggioranza di dette misure è (almeno fino alla prossima entrata in vigore di una normativa europea che aggiorni anche queste voci) positivamente indicata nel c.d. "Disciplinare Tecnico – Allegato B" del Codice della Privacy del 2003, molte altre indicazioni sono più generali e appartengono ad un metodo di lavoro organizzato secondo ragionevolezza e buona fede. All'interno dell'ente è stato implementato il REGOLAMENTO PER L'USO DI INTERNET E DELLA POSTA ELETTRONICA, rivolto al personale dipendente e a tutti coloro che collaborano, pur in assenza di un rapporto di lavoro subordinato, nel momento in cui utilizzano le attrezzature informatiche scolastiche.
É innanzitutto un aiuto per l'uso consapevole e diligente delle risorse informatiche messe a disposizione (postazioni di lavoro, dispositivi portatili, posta elettronica) evitando comportamenti che possono innescare problemi o minacce alla sicurezza del sistema. Informa inoltre delle misure di tipo organizzativo e tecnologico adottate e dei controlli che potrebbero essere effettuati, sempre nel rispetto della libertà e della dignità dei lavoratori.

USO DI INTERNET DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Il corretto utilizzo di internet rappresenta uno dei punti cardini per la sicurezza dell'infrastruttura informatica entro la quale si effettua il trattamento dei dati.
Uno dei momenti più critici è quello del "download" (scaricamento) di software o dati al di fuori dai casi espressamente previsti e consentiti dal Titolare del trattamento.
L'Autorizzato al trattamento dei dati mediante utilizzo di apparecchiature informatiche, deve astenersi dal compiere "download" non autorizzati onde prevenire situazioni critiche riconducibili a due fattispecie da evitare:

<u>"DOWNLOAD" INVOLONTARIO DI SOFTWARE CHE POSSA ESPORRE LA RETE A RISCHIO DI INTRUSIONI O DI DANNO CAGIONATO DA SOFTWARE RICONDUCIBILE A QUANTO PREVISTO DALL'ART. 615 QUINQUIES DEL CODICE PENALE (VIRUS INFORMATICI)</u>

Il "download" incontrollato molto frequentemente mina le misure di sicurezza adottate a protezione della rete. Le conseguenze tipiche di tale comportamento sono: L'apertura di un varco sul dispositivo firewall che agevoli l'accesso indebito alla rete da parte di soggetti non autorizzati; Il danneggiamento dei dispositivi operato da virus informatici.

<u>"DOWNLOAD" DI DATI CHE POSSANO ESSERE CATALOGATI COME "PERSONALI" O "PARTICOLARI" IN MANIERA INCONSAPEVOLE DA PARTE DEL TITOLARE DEL TRATTAMENTO</u>

Il "download" incontrollato può riguardare non solo "malware" (cioè software che abbia mire dannose per la rete) bensì anche dati personali o addirittura particolari che si troveranno a risiedere su elaboratori elettronici in maniera non consapevole e quindi verranno trattati, con ogni probabilità, in maniera inadeguata.

USO DELLA POSTA ELETTRONICA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Al "download" di software o dati da internet è assimilabile la consultazione <u>non</u> remota della posta elettronica. La rete pertanto sarà configurata in modo da impedire ai soggetti del trattamento la configurazione di software di posta (Outlook, Eudora etc.) che comportino lo scaricamento dei dati sui propri elaboratori. Se la consultazione della posta elettronica privata è consentita, essa avverrà mediante accesso remoto alla casella mail tramite browser (Internet Explorer, Netscape Navigator etc.).

USO DEL FAX DA PARTE DEI SOGGETTI DEL TRATTAMENTO

Ancorché si tratti di una pratica oggetto di progressiva dismissione, i documenti in ingresso, contenenti dati personali, che dovessero pervenire via FAX, devono essere trattati con particolare cura, affinché non restino a disposizione di soggetti non autorizzati. L'Autorizzato della gestione dei FAX deve vigilare sulla corretta esecuzione della procedura di smistamento.

DISTRUZIONE DI DOCUMENTI DA PARTE DEI SOGGETTI DEL TRATTAMENTO

I documenti cartacei contenenti dati personali che, a qualsiasi titolo (dismissione di archivi, errori di scrittura, copie ridondanti etc.) debbano essere eliminati, saranno resi illeggibili dal soggetto Autorizzato mediante l'uso di un distruggidocumenti o di altro metodo parimenti idoneo.

GESTIONE DELLA POSTA CARTACEA DA PARTE DEI SOGGETTI DEL TRATTAMENTO

La posta cartacea viene raccolta dall'Autorizzato in servizio in quel momento presso la portineria / reception ed immediatamente smistata verso gli uffici.
All'atto dell'apertura tutti i documenti contenenti dati personali devono essere smistati senza ritardi a cura del personale del protocollo stesso.
Il Titolare del trattamento determina gli Autorizzati espressamente autorizzati, quali responsabili della tenuta del protocollo e della visione dei contenuti delle missive.
La posta elettronica viene "scaricata" da ciascun Autorizzato e, se stampata, segue lo stesso procedimento previsto per la posta cartacea.
Le lettere arrivate per posta che presentino all'esterno l'indicazione "RISERVATO" o altre formule atte a qualificarle come contenenti documenti di tipo particolare, non possono essere aperte dagli Autorizzati della gestione del protocollo ma devono immediatamente essere consegnati all'attenzione del Titolare del trattamento il quale provvederà alla loro custodia ed all'inoltro, o a quella del destinatario in persona.

Si rammenta che l'Art. 616 Codice Penale vieta la Violazione, sottrazione e soppressione di corrispondenza:

Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prenderne o di farne da altri prender cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero in tutto o in parte la distrugge o sopprime, è punito, se il fatto non è preveduto come reato da altra disposizione di legge, con la reclusione fino a un anno o con la multa da € 31,00 a € 516,00
[omissis]

VII. MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o di perdita, il Titolare del trattamento dei dati stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati. Tale periodicità, tuttavia, non può essere superiore alla settimana.
I criteri debbono essere stabiliti dal Titolare del trattamento in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

Procedura di esecuzione del Back-up
Il Titolare del trattamento si deve preoccupare dell'esecuzione della procedura di back-up (salvataggio degli archivi).
Il Responsabile della procedura di Back-Up deve essere formato affinché sia totalmente indipendente nell'eseguire i passi tecnici necessari per l'attuazione del salvataggio delle copie degli archivi informatici contenenti dati personali.
La procedura di Back-Up deve avvenire in maniera completamente automatizzata senza bisogno dell'intervento da parte dell'operatore al fine di escludere tutte le ipotesi di dimenticanza e imperizia dell'attuazione del procedimento, in tali casi al soggetto incaricato spetta solo il compito di verificare che il salvataggio abbia avuto buon fine.

Il Titolare del trattamento è responsabile della custodia e della conservazione di supporti utilizzati per il *back up* dei dati.
Essi devono essere custoditi in modo da scongiurare il più possibile le aggressioni da:

- Agenti chimici;
- Fonti di calore;
- Campi magnetici;
- Intrusione ed atti vandalici;

- Incendio;
- Allagamento;
- Furto.

L'accesso ai supporti utilizzati per il *back up* dei dati è limitato per ogni banca dati al Titolare del trattamento della sicurezza dei dati ed all'Autorizzato al trattamento di competenza.

Se il Titolare del trattamento decide che i supporti per le copie di *back up* delle banche di dati trattate non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto, annullando e rendendo illeggibili le informazioni in esso contenute.
È compito del Titolare del trattamento assicurarsi che in nessun caso vengano lasciate copie di *back up* delle banche di dati trattate, non più utilizzate, senza che ne venga cancellato il contenuto ed annullate e rese illeggibili le informazioni in esso registrate.
I dati memorizzati sui supporti di back-up, nonché sui dispositivi mobili di archiviazione, devono risiedere sugli stessi in forma non-intellegibile; perché questo avvenga è necessario prevedere l'installazione di software di crittografia dei dati che impediscano, in caso di furto o smarrimento accidentale di questi supporti, la lettura da parte di chicchessia non autorizzato.
Con periodicità almeno semestrale viene verificato il corretto funzionamento della procedura di back-up simulando un ripristino totale dei dati.
La modalità di back-up cosiddetta "in cloud" ossia che avvenga utilizzando una piattaforma remota accessibile mediante web, non modifica i tratti essenziali della procedura che dovrà essere sempre verificata in ordine alla puntuale esecuzione del trasferimento dei dati oggetto di *back up*.

VIII. ALTRE MISURE DI SICUREZZA

Le regole vigenti vietano a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Titolare di dati oggetto del trattamento;
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Titolare, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Titolare, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- Consegnare a persone non autorizzate dal Titolare, stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

Il Titolare deve definire le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati.
In linea di massima sono autorizzate all'accesso ai locali esclusivamente quelle persone autorizzate al trattamento alle quali, il Titolare, concede l'accesso ai luoghi fisici mediante la consegna di un badge o di una chiave, nonché l'accesso agli ambiti informatici mediante la consegna di idonei criteri di accesso.

Il Titolare deve informare con una comunicazione scritta l'Autorizzato, dell'ufficio dei compiti che gli sono stati affidati e deve provvedere a formarlo affinché le mansioni indicate nella lettera gli siano familiari.

ASSEGNAZIONE NOMI UTENTE
Il Titolare deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Autorizzato al trattamento di accedere ai sistemi di trattamento delle banche di dati.
Non sono ammessi nomi identificativi di gruppo, con la sola eccezione dei pochi identificativi assegnati per l'amministrazione di sistema, relativamente ai sistemi operativi che prevedono un unico livello di accesso.
In ogni caso, un codice identificativo assegnato ad un Autorizzato al trattamento deve essere annullato se l'Autorizzato al trattamento ha dato le dimissioni.

ASSEGNAZIONE DELLE PASSWORD
Il Titolare deve definire le modalità di assegnazione delle *password* e decidere che ogni utente Autorizzato al trattamento possa modificare autonomamente la propria *password* di accesso.

In questo caso la modifica richiede che venga data comunicazione al Custode della *password* e al Responsabile del trattamento (se diverso dal Custode delle *password*).
Le password saranno composte da almeno 8 caratteri e non dovranno contenere elementi immediatamente riconducibili ai proprietari delle stesse.

SICUREZZA DELLE TRASMISSIONI DATI
Al fine di garantire la sicurezza delle trasmissioni dei dati su rete pubblica, il Titolare stabilisce le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione su ogni sistema collegato in rete pubblica.
I criteri debbono essere definiti dal Titolare in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.

PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI
Il Documento è costantemente aggiornato ad opera del Titolare circa ogni variazione dell'elenco degli Autorizzati del trattamento autorizzati al trattamento dei dati personali.
In particolare, in caso di trattamento automatizzato di dati, per ogni Autorizzato al trattamento deve essere indicato lo USER ID assegnato.

In caso di dimissioni di un Autorizzato al trattamento o di revoca delle autorizzazioni al trattamento dei dati, il Titolare deve darne immediata comunicazione affinché si provveda a disattivare la possibilità di accesso al sistema per il soggetto in questione.
Al Titolare è affidato il compito di verificare, ogni anno, le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati, oltre al compito di redigere e di aggiornare ad ogni variazione i permessi di accesso per ogni Autorizzato al trattamento autorizzato.
In particolare, per ogni Autorizzato al trattamento e per ogni banca dati debbono essere indicati i privilegi assegnati tra seguenti:

I. Inserimento dei dati;
II. Lettura e stampa dei dati;
III. Modifica di dati;
IV. Cancellazione di dati.

IX. MANUTENZIONE DELLE APPARECCHIATURE

Al Titolare al trattamento dei dati è affidato il compito di verificare ogni anno la situazione delle apparecchiature installate con cui vengono trattati i dati, delle apparecchiature periferiche e, in particolare, dei dispositivi di collegamento con le reti pubbliche.

La verifica ha lo scopo di controllare l'affidabilità del sistema per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito, tenendo conto anche dell'evoluzione tecnologica.

Al Titolare è affidato il compito di verificare ogni anno la situazione dei Sistemi Operativi installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito,

tenendo conto in particolare di:

- Disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati;
- Segnalazioni di *Patch*, *Fix* o *System-Pack* per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

Nel caso in cui esistano rischi evidenti il Titolare deve prendere gli opportuni provvedimenti allo scopo di assicurarne il corretto trattamento dei dati in conformità alle norme in vigore.
Al Titolare è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità del *software* applicativo, per quanto riguarda:

- La sicurezza dei dati trattati;
- Il rischio di distruzione o di perdita;
- Il rischio di accesso non autorizzato o non consentito,

tenendo conto in particolare della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati.
Nel caso in cui esistano rischi evidenti il Titolare deve prendere gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

X. IL DATA BREACH

Una violazione dei dati personali (c.d. *data breach*) può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali ed immateriali alle persone fisiche coinvolte.
Alcuni esempi che possiamo fare di questi danni sono: la perdita del controllo dei dati personali che li riguardano o la limitazione dei loro diritti, casi di discriminazione, furto o usurpazione d'identità, perdite finanziarie connesse alla sottrazione delle credenziali dell'home banking, decifratura non autorizzata delle forme di pseudonimizzazione attuate, pregiudizio alla reputazione, perdita di riservatezza dei dati protetti da segreto professionale e d'ufficio o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.
Questo paragrafo si prefigge lo scopo di indicare, al Titolare del trattamento dei dati, le opportune modalità di gestione del *data breach*, nel rispetto della normativa in materia di trattamento dei dati personali, garantendo in particolare l'aderenza ai principi e alle disposizioni contenute nel Regolamento UE 679/2016 (Considerando n. 85,86,87,88 ed Artt. 33 e 34) e nella *Guidelines on personal data breach notification under Regulation 2016/679 – article 29 data protection working party*.

In questo parte del documento si sintetizzano le regole per garantire il rispetto dei principi esposti e la realizzabilità tecnica e la sostenibilità organizzativa, nella gestione del *data breach*, sotto i diversi aspetti relativi a:

- modalità di segnalazione al Titolare da parte di chi venga a conoscenza della violazione
- modalità e profili di segnalazione all'Autorità Garante
- valutazione dell'evento accaduto
- eventuale comunicazione agli interessati

Ogni operatore autorizzato a trattare i dati personali, qualora venga a conoscenza di un potenziale caso di *data breach,* avvisa tempestivamente il Titolare del trattamento.
Ai fini di una corretta classificazione dell'episodio, il Titolare utilizzerà lo schema di scenario di *data breach*, riportato alle pagine seguenti.

Sulla scorta delle determinazioni raggiunte, il Titolare predispone l'eventuale comunicazione all'Autorità Garante, a propria firma, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi).
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del Titolare.

Nel caso in cui dal *data breach* possa derivare un rischio elevato per i diritti e le libertà delle persone, anche queste devono essere informate senza ingiustificato ritardo, al fine di consentire loro di prendere provvedimenti per proteggersi da eventuali conseguenze negative della violazione.

Il Titolare del trattamento predispone l'eventuale comunicazione agli interessati da inviarsi nei tempi e nei modi che lo stesso, individuerà come più opportuna come specificato nell'art. 34 del G.D.P.R. e tenendo conto di eventuali indicazioni fornite dall'Autorità Garante.
La comunicazione deve comprendere almeno:

- nome e recapiti del Titolare;
- le probabili conseguenze della violazione dei dati;
- eventuali misure adottate dal Titolare per porre rimedio o attenuare l'infrazione.

L'adeguatezza di una comunicazione è determinata non solo dal contenuto del messaggio, ma anche dalle modalità di effettuazione. Le linee guida, sulla base dell'art. 34, ricordano che devono sempre essere privilegiate modalità di comunicazione diretta con i soggetti interessati (quali email, SMS etc.).

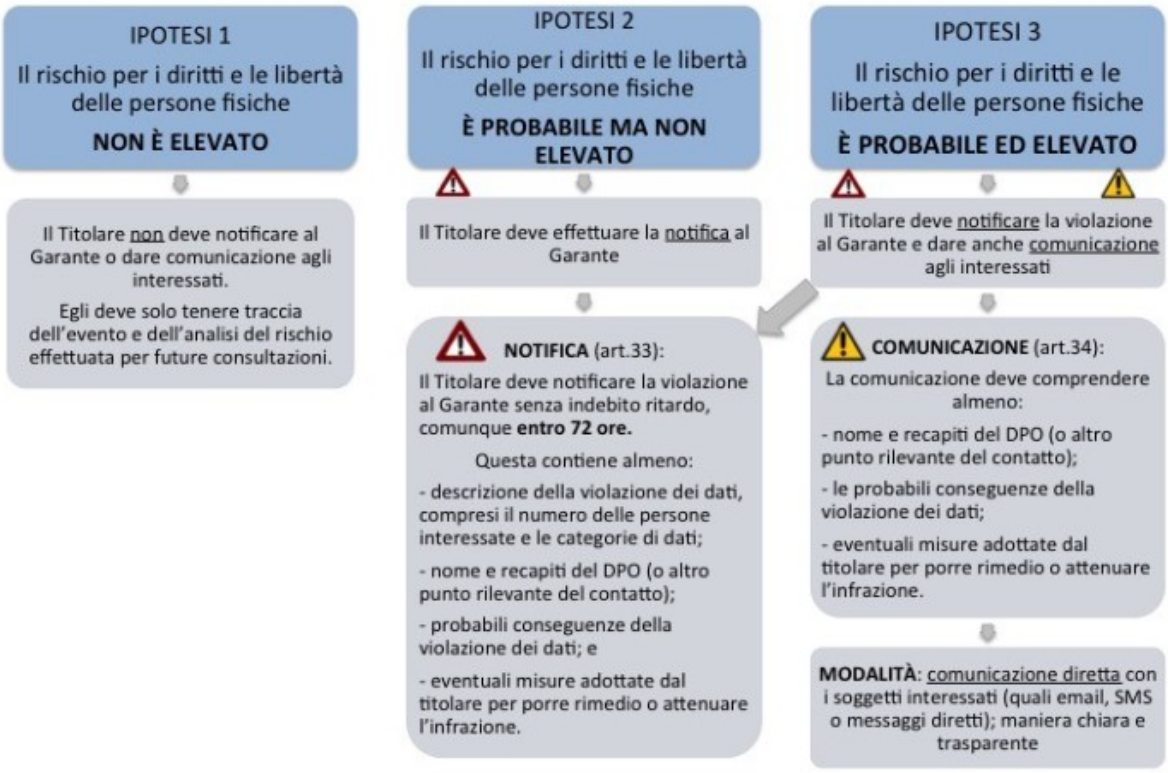
Si è detto, ai paragrafi precedenti, che ogniqualvolta il Titolare si trovi ad affidare il trattamento di dati ad un soggetto terzo/responsabile del trattamento, è tenuto a stipulare con tale soggetto uno specifico contratto che lo vincoli al rispetto delle istruzioni impartitegli dal Titolare in materia di protezione dati: è necessario che la presente procedura di segnalazione di *data breach* sia inclusa nel suddetto contratto; ciò al fine di obbligare il responsabile ad informare il Titolare del trattamento senza ingiustificato ritardo, di ogni potenziale evento di *data breach*.
Ad ogni responsabile del trattamento deve essere comunicato il contatto del Titolare al quale effettuare la predetta segnalazione.
La comunicazione deve avvenire senza ingiustificato ritardo, per "ingiustificato ritardo" si considera la notizia pervenuta al Titolare al più tardi entro 12 ore dalla presa di conoscenza iniziale da parte del responsabile.
Il Titolare effettua una valutazione dell'evento avvalendosi, nel caso, del gruppo privacy del soggetto esterno.
Ai fini di una corretta classificazione dell'episodio il Titolare utilizzerà lo schema di scenario di *data breach* di seguito riportato.
Pertanto, sulla scorta delle determinazioni raggiunte, il Titolare predispone l'eventuale comunicazione all'Autorità Garante, a sua firma, da inviare senza ingiustificato ritardo e, ove possibile, entro 72 ore, da determinarsi dal momento in cui ne è venuto a conoscenza, cioè quando abbia un ragionevole grado di certezza della verificazione di un incidente di sicurezza che riguardi dati personali.
Oltre il termine delle 72 ore, la notifica deve essere corredata delle ragioni del ritardo.
E' comunque fatta salva la possibilità di fornire successivamente all'Autorità Garante informazioni aggiuntive o dettagli rilevanti sulla violazione di cui il Titolare venga a conoscenza, a seguito della effettuazione di ulteriori indagini e attività di follow-up (c.d. notifica in fasi)
La scelta e le motivazioni che hanno portato a non notificare l'evento deve essere documentata a cura del referente privacy del soggetto obbligato.
Rimane salva la possibilità che sia il responsabile esterno del trattamento ad effettuare una notifica per conto del Titolare del trattamento, se il Titolare del trattamento ha rilasciato specifica autorizzazione al responsabile, all'interno del suddetto contratto. Tale notifica deve essere fatta in conformità con gli articoli 33 e 34 del G.D.P.R..
La responsabilità legale della notifica rimane in capo al Titolare del trattamento nella persona del Dirigente Scolastico.
Al fine di eseguire la valutazione dell'obbligatorietà o meno della notifica all'Autorità Garante dei data breach e di supportare i soggetti coinvolti nella procedura, vengono illustrati alcuni scenari di possibili violazioni di dati personali.

TIPO DI VIOLAZIONE (BREACH)	DEFINIZIONE	SOGLIA DI SEGNALAZIONE	ESEMPI (segnalazione SI)	CONTROESEMPI (segnalazione NO)
DISTRUZIONE	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo.	Dati non recuperabili o provenienti da procedure non ripetibili Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto non riparabile dell'hard disk contenente uno o più referti che, in violazione al regolamento, erano salvati localmente Incendio di archivio cartaceo Distruzione di documenti originali	Rottura di una chiavetta USB o di un hard disk che non contiene dati personali originali (in unica copia) Distruzione di un documento, ad esempio a causa di un guasto di sistema, durante la sua stesura nell'apposito applicativo
PERDITA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, non è più nella disponibilità del Titolare, ma potrebbe essere nella disponibilità di terzi (lecitamente o illecitamente). In caso di richiesta di dato da parte dell'interessato non sarebbe possibile produrlo, ed è possibile che terzi possano avere impropriamente accesso al dato.	Dati non recuperabili relativi a più utenti, o relativi a tipologie di dato la cui indisponibilità lede i diritti fondamentali dell'interessato o relativi a tipologie di dato la cui divulgazione conseguente alla perdita possa ledere i diritti fondamentali dell'interessato Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Smarrimento di chiavetta USB contenente dati originali Smarrimento di fascicolo cartaceo del personale o dell'utente	Smarrimento di un documento, ad esempio a causa di un guasto di sistema, appena avvenuta la stampa
MODIFICA	Un insieme di dati personali, a seguito di incidente o azione fraudolenta, è stato irreversibilmente modificato, senza possibilità di ripristinare lo stato originale. In caso di richiesta del dato da parte dell'interessato non sarebbe possibile produrlo con certezza che non sia stato alterato.	Modifiche sistematiche su più casi Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi	Guasto tecnico che altera parte dei contenuti di un sistema, compromettendo anche i backup Azione involontaria, o fraudolenta, di un utente che porta alla alterazione di dati in modo non tracciato e irreversibile	Guasto tecnico che altera parte dei contenuti di un sistema, rilevato e sanato tramite operazioni di recovery Azione involontaria di un utente che porta alla alterazione di dati tracciata e reversibile Modifica di un documento non ancora validato dal

				proprio autore.
DIVULGAZIONE NON AUTORIZZATA	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente), a seguito di incidente o azione fraudolenta, viene trasmesso a terze parti senza il consenso dell'interessato o in violazione del regolamento dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Malfunzionamento del sistema di differenziazione delle credenziali Consegna di un CD con dati di un utente ad altra struttura senza autorizzazione	Un dipendente sul proprio sistema seleziona l'utente Mario Rossi ma interviene sull'utente Luca Bianchi., inserisce i dati e li invia al gestionale. Infezione virale di un PC con un virus che dalla scheda tecnica non trasmette dati su internet Trasmissione non autorizzata di un documento non ancora validato dal proprio autore.
ACCESSO NON AUTORIZZATO	Un insieme di dati personali (e riconducibili all'individuo direttamente o indirettamente) sono stati resi disponibili per un intervallo di tempo a persone (anche Autorizzati dal Titolare) non titolati ad accedere al dato secondo principio di pertinenza e non eccedenza, o secondo i regolamenti dell'organizzazione	Rientrano tra i casi di segnalazione i soli dati appartenenti a documenti definitivi e già contrassegnati da un livello minimo di validazione.	Accesso alla rete aziendale da persone esterne all'organizzazione che sfruttano vulnerabilità di sistemi Accesso da parte di un utente a dati non di sua pertinenza a seguito di configurazione errata dei permessi di accesso ad un sistema.	Accesso da parte di un utente a dati di sua pertinenza, a cui segue un uso improprio degli stessi Accesso non autorizzata di un documento non ancora validato dal proprio autore.

INDISPONIBILITA' TEMPORANEA DEL DATO	Un insieme di dati personali, a seguito di incidente, azione fraudolenta o involontaria, è non disponibile per un periodo di tempo che lede i diritti dell'interessato.	Indisponibilità dei dati personali oltre i tempi definiti a livello aziendale	Infezione da ransomware che comporta la temporanea perdita di disponibilità dei dati e questi non possono essere ripristinati dal backup Cancellazione accidentale dei dati da parte di una persona non autorizzata Perdita della chiave di decrittografia di dati crittografati in modo sicuro irraggiungibilità di un sito di stoccaggio delle cartelle cliniche poste in montagna per isolamento neve	Indisponibilità dei dati personali a causa della manutenzione programmata del sistema in corso

Un *data breach*, quindi, non è solo un attacco informatico, ma può consistere anche in un accesso abusivo, un incidente (es. un incendio o una calamità naturale), nella semplice perdita di un dispositivo mobile di archiviazione (es. chiavetta USB, disco esterno), nella sottrazione di documenti con dati personali (es. furto di un notebook di un dipendente).
I casi di *data breach* per le casistiche già descritte si estendono dai dati digitali, ai documenti cartacei o su altri supporti analogici.
La comunicazione involontaria di documenti, o in generale di dati, che non abbiano vero senso compiuto/riconducibilità verso l'interessato non è considerato *data breach,* ma è considerato un normale errore procedurale.
Al fine di schematizzare ancora meglio lo schema del ragionamento prendiamo in prestito, dallo studio legale Delli Ponti, questo diagramma:



La segnalazione di un data breach all'Autorità Garante deve contenere alcune informazioni fondamentali.
Di seguito le riportiamo per esteso (verificare sul sito del Garante la presenza di modulistica ad hoc):

1. Titolare che effettua la comunicazione:
   a. Denominazione o ragione sociale:
   b. Sede del Titolare:
   c. Persona fisica addetta alla comunicazione:
   d. Funzione rivestita:
   e. Indirizzo email per eventuali comunicazioni:
   f. Recapito telefonico per eventuali comunicazioni:

2. Natura della comunicazione:
   a. Nuova comunicazione (inserire contatti per eventuali chiarimenti, se diversi da quelli sub 1.):
   b. Seguito di precedente comunicazione (inserire numero di riferimento):
   b.1. Inserimento ulteriori informazioni sulla precedente comunicazione:
   b.2. Ritiro precedente comunicazione (inserire le ragioni del ritiro):
3. Breve descrizione della violazione di dati personali:

4. Quando si è verificata la violazione di dati personali?
   a. Il …
   b. Tra il ….. e il …..
   c. In un tempo non ancora determinato
   d. È possibile che sia ancora in corso
5. Dove è avvenuta la violazione dei dati? (Specificare se smarrimento di dispositivi o supporti)

6. Modalità di esposizione al rischio:
   a. tipo di violazione:
   a.1. lettura (presumibilmente i dati non sono stati copiati)
   a.2. copia (i dati sono ancora presenti sui sistemi del Titolare)
   a.3. alterazione (i dati sono presenti sui sistemi ma sono stati alterati)
   a.4. cancellazione (i dati non sono più sui sistemi del Titolare e non li ha neppure l'autore della violazione)
   a.5. furto (i dati non sono più sui sistemi del Titolare e li ha l'autore della violazione)

a.6. altro [specificare]
b. dispositivo oggetto della violazione:
b.1. computer
b.2. dispositivo mobile
b.3. documento cartaceo
b.4. file o parte di un file
b.5. strumento di backup
b.6. rete
b.7. altro [specificare]

7. Sintetica descrizione dei sistemi di elaborazione o di memorizzazione dei dati coinvolti, con indicazione della loro ubicazione:

8. Quante persone sono state colpite dalla violazione di dati personali?
a. [numero esatto] persone
b. Circa [numero] persone
c. Un numero (ancora) sconosciuto di persone

9. Che tipo di dati sono coinvolti nella violazione?
a. Dati anagrafici
b. Numeri di telefono (fisso o mobile)
c. Indirizzi di posta elettronica
d. Dati di accesso e di identificazione (user name, password, customer ID, altro)
e. Dati di pagamento (numero di conto corrente, dettagli della carta di credito, altro)
f. Altri dati personali (sesso, data di nascita/età, …), dati sensibili e giudiziari
g. Ancora sconosciuto
h. Altro [specificare]

10. Livello di gravità della violazione di dati personali (secondo le valutazioni del Titolare):
a. Basso/trascurabile
b. Medio
c. Alto

11. Misure tecniche e organizzative applicate ai dati colpiti dalla violazione:

12. La violazione è stata comunicata anche a contraenti (o ad altre persone interessate)?
a. Sì, è stata comunicata il ….
b. No, perché [specificare]

13.Qual è il contenuto della comunicazione ai contraenti (o alle altre persone interessate)? [riportare il testo della notificazione]

14. Quale canale è utilizzato per la comunicazione ai contraenti (o alle altre persone interessate)?

15. Quali misure tecnologiche e organizzative sono state assunte per contenere la violazione dei dati e prevenire simili violazioni future?

16. La violazione coinvolge contraenti (o altre persone interessate) che si trovano in altri Paesi EU?
a. No
b. Si

17. La comunicazione è stata effettuata alle competenti autorità di altri Paesi EU?
a. No
b. Si, (specificare)

Come accade per tutti i sistemi basati sul concetto di “rischio” e di “valutazione del rischio”, la documentazione degli episodi che hanno determinato un danno (violazione dei dati – data breach) è fondamentale al fine di adottare precauzioni (tecniche o comportamentali) che possano scongiurare il verificarsi nuovamente di quell’episodio.

L'Art. 33 del G.D.P.R. pone l'attenzione su questa esigenza, il metodo migliore per adempiere a questa regola ma anche per poter comprovare, in caso di ispezione, tale adempimento consiste nella tenuta di un registro dei data breach (già previsto dal Garante con provvedimento 161 del 04 Aprile 2013) che contenga, per ciascun episodio, queste informazioni essenziali:

1. Dettagli relativi alla violazione (cause, luogo, tipologia di dati violati);
2. Effetti e conseguenze della violazione;
3. Piano di intervento predisposto dal Titolare;
4. Le motivazioni delle decisioni assunte a seguito del data breach nei casi in cui:
   a. Il Titolare ha deciso di non procedere alla notifica;
   b. Il Titolare ha ritardato nella procedura di notifica;
   c. Il Titolare ha deciso di non notificare il data breach agli interessati.

XI. LA TUTELA DEI DIRITTI DEGLI INTERESSATI (PROCEDURA)

Occorre definire le modalità e le responsabilità per l'adozione di misure adeguate a fornire all'interessato tutte le informazioni da egli richieste secondo quanto previsto dalla normativa, in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.

La procedura è applicabile a tutte le attività di trattamento dei dati personali svolte, con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi, ecc.), anche con il supporto di fornitori esterni.

Le richieste degli interessati possono pervenire unicamente tramite i canali previsti nell'informativa privacy fornita e possono riguardare:

- accesso ai dati;
- rettifica dei dati;
- cancellazione dei dati (diritto all'oblio);
- limitazione del trattamento;
- portabilità dei dati;
- esercizio del diritto di opposizione;
- esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato.

Il Titolare, in base al contenuto della richiesta, provvede di conseguenza ad adempiere alla richiesta, se basata su presupposti legittimi.
Eventuali altri casi, incluse richieste che facciano riferimento al Titolare, saranno gestiti caso per caso.
Prima di evadere la richiesta, il Titolare provvederà a verificare se la stessa è completa degli elementi essenziali per la identificazione dell'interessato e l'elaborazione di una risposta e, in caso contrario le acquisisce. In particolare si intendono "essenziali":

- nome e cognome;
- estremi di un documento in corso di validità;
- oggetto della richiesta;
- data di presentazione.

L'Unità Organizzativa o la Struttura competente per la risposta la prende in carico e la elabora. La risposta fornita all'interessato deve essere "intelligibile", concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.
La risposta all'interessato va data con lo stesso strumento utilizzato da quest'ultimo (es. email) salvo diversa indicazione dell'interessato stesso.
Il termine per la risposta all'interessato è, per tutti i diritti, di 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; è comunque necessario dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.
Qualora il Titolare verifichi la impossibilità o la non applicabilità di una risposta decide se applicare la deroga alla risposta. Tali casi sono:

- impossibilità di identificare l'interessato;
- carattere manifestamente infondato o eccessivo della richiesta inviata da parte dell'interessato, in particolare per via del carattere ripetitivo della stessa; oppure, come previsto dalla normativa, se:
- la richiesta ricade nel principio di tutela del diritto alla libertà d'espressione e di informazione, incluso il trattamento a scopi giornalistici o di espressione accademica, artistica o letteraria
- i dati personali sono trattati a fini di ricerca scientifica o storica
- i dati personali sono archiviati a fini meramente statistici
- i dati personali sono trattati per finalità di archiviazione nel pubblico interesse.

Nel caso in cui la richiesta debba essere respinta, la risposta dovrà contenere i motivi dell'inottemperanza e le indicazioni sulla possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.
Per ogni richiesta ricevuta viene compilato il "Registro delle richieste" nel quale sono riportati gli estremi della richiesta:

- numero progressivo;
- data della richiesta;
- data di ricezione della richiesta, se diversa dalla data della richiesta;
- canale di comunicazione (email, PEC, posta comune, posta raccomandata);
- nominativo dell'interessato;
- tipo di richiesta:

    o accesso ai dati;
    o rettifica dei dati;
    o cancellazione dei dati (diritto all'oblio);
    o limitazione di trattamento;
    o portabilità dei dati;
    o esercizio del diritto di opposizione;
    o esercizio del diritto di non essere sottoposto a una decisione basata sul trattamento automatizzato;
    o altro.

- Unità organizzative / strutture coinvolte nella gestione della richiesta;
- Completezza della richiesta (SI/NO);
- Fondatezza della richiesta (SI/NO);
- Complessità della richiesta (SI/NO);
- Gestione della prima risposta: data, canale di comunicazione, oggetto;
- Oneri economici per la gestione della richiesta (in ore / persona);
- Stato della richiesta (in corso/chiusa);
- Data di chiusura della gestione della richiesta;
- Note.

Qualora la richiesta riguardi l'accesso ai dati personali, una volta confermata la completezza e la fondatezza della richiesta stessa, il Titolare con il supporto della Struttura interessata, e dopo verifica che l'ottenimento della copia possa ledere i diritti e le libertà altrui, predispone una copia dei dati personali oggetto di trattamento.
Oltre quanto indicato in precedenza, nel caso specifico, si applicano le seguenti regole:

La riposta contiene la conferma che sia o meno in corso un trattamento di dati personali che riguardano l'interessato e, in tal caso, contiene i dati personali e le seguenti informazioni:

1. le finalità del trattamento;
2. le categorie di dati personali in questione;
3. i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
4. quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
5. l'esistenza del diritto dell'interessato di chiedere al Titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
6. il diritto di proporre reclamo a un'autorità di controllo;

7. qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
8. l'esistenza di un processo decisionale automatizzato, compresa la profilazione e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato;
9. qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, esistenza di garanzie adeguate relative al trasferimento.

Qualora la richiesta riguardi la rettifica dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali inesatti e/o dei dati personali incompleti, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di rettifica/integrazione, gli uffici interessati comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Le attività di rettifica/integrazione vanno completate senza ingiustificato ritardo.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali rettifiche effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.

Qualora la richiesta riguardi la cancellazione dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali da cancellare, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di cancellazione, le funzioni competenti comunicano al Titolare stesso il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, dopo aver verificato la fondatezza della richiesta predispone la risposta alla richiesta dell'interessato, in caso contrario, comunica il respingimento della richiesta.

Per valutare la fondatezza della richiesta stessa, il Titolare, verifica preliminarmente se sussiste uno dei motivi seguenti:

- i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- l'interessato revoca il consenso su cui si basa il trattamento e non sussiste altro fondamento giuridico per il trattamento;
- l'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto; - i dati personali sono trattati illecitamente;
- i dati personali devono essere cancellati per adempiere ad un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetta il Titolare del trattamento;
- i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione ai minori.

Per valutare il respingimento della richiesta stessa il Titolare verifica se il trattamento dei dati è necessario per uno dei motivi seguenti:

- per l'esercizio del diritto alla libertà di espressione e di informazione;
- per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il Titolare del trattamento;
- per motivi di interesse pubblico nel settore della sanità pubblica;
- a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, nella misura in cui la cancellazione rischia di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;
- per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali cancellazioni effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.
In particolare, se il Titolare del trattamento ha reso pubblici i dati personali oggetto della richiesta, esso è obbligata a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, per cui il Titolare stesso identifica le

misure per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato e per garantire la cancellazione di qualsiasi link, copia o riproduzione dei suoi dati personali.

Qualora la richiesta riguardi la limitazione del trattamento dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare, trasmette agli uffici interessati un elenco dei dati personali di cui limitare il trattamento, in forma scritta, preferibilmente a mezzo email, e concorda con esse le misure per contrassegnare il dato personale in attesa di determinazioni ulteriori. Terminate le operazioni di contrassegno e limitazione del trattamento, gli uffici interessati comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Se il Titolare del trattamento ha reso pubblici i dati personali oggetto della richiesta, essa è obbligata a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione, per cui identifica le misure per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato e per garantire la cancellazione di qualsiasi link, copia o riproduzione dei suoi dati personali.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.

Il Titolare, con il supporto degli uffici interessati, comunica a ciascuno dei destinatari cui sono stati trasmessi i dati personali le eventuali limitazioni del trattamento effettuate, salvo che ciò si riveli impossibile o implichi uno sforzo sproporzionato.
La risposta all'interessato contiene i nominativi di tali destinatari, qualora l'interessato lo richieda.

Se il trattamento è limitato, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'interessato o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria oppure per tutelare i diritti di un'altra persona fisica o giuridica o per motivi di interesse pubblico rilevante dell'Unione o di uno Stato membro.
Il Titolare, con il supporto degli uffici interessati, verifica che, per i dati per i quali siano in corso delle limitazioni di trattamento, siano attuati solo i trattamenti consentiti, fino a revoca delle limitazioni.

Il Titolare, con il supporto delle funzioni competenti, identifica i termini per la revoca della limitazione richiesta e ne informa l'interessato prima che detta limitazione sia revocata.

Qualora la richiesta riguardi la portabilità dei dati, confermata la completezza e la fondatezza della richiesta stessa, il Titolare trasmette agli uffici interessati un elenco dei dati personali di cui effettuare la portabilità, in forma scritta, preferibilmente a mezzo email.
Terminate le operazioni di portabilità, gli uffici interessati comunicano al Titolare stesso il completamento delle attività, in forma scritta, preferibilmente a mezzo email. Il diritto di ottenere la portabilità dei dati non deve ledere i diritti e le libertà altrui.
Secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.
Nel caso specifico, si applicano le seguenti regole.

Per valutare la fondatezza della richiesta stessa, il Titolare, verifica se sussistano entrambe le condizioni seguenti:

- il trattamento si basi sul consenso, anche in riferimento a dati sensibili, o su un contratto;
- il trattamento sia effettuato con mezzi automatizzati.

Inoltre, sono portabili i dati personali che:

- riguardano l'interessato, e
- sono stati forniti dall'interessato a un Titolare, intendendo sia i dati forniti consapevolmente e attivamente dall'interessato (ad esempio indirizzo postale, nome utente, età), sia i dati osservati forniti dall'interessato attraverso la fruizione di un servizio o l'utilizzo di un dispositivo (ad esempio cronologia delle ricerche effettuate dall'interessato e dati relativi al traffico).

L'interessato può continuare a fruire e beneficiare del servizio offerto dal Titolare anche dopo che sia compiuta un'operazione di portabilità. La portabilità non comporta la cancellazione automatica dei dati conservati nei sistemi del Titolare, e non incide sul periodo di conservazione previsto originariamente per i dati oggetto di trasmissione.
Il diritto alla portabilità non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il Titolare del trattamento.

I dati oggetto di portabilità sono riportati su un formato strutturato, di uso comune e leggibile da dispositivo automatico; ove possibile, tale formato dovrebbe essere interoperabile.

La richiesta dell'interessato può comprendere la trasmissione diretta dei dati personali da un Titolare del trattamento all'altro, se tecnicamente fattibile.
In tal caso, il Titolare, coinvolge le funzioni competenti per identificare le modalità per tale trasmissione diretta.
Qualora la richiesta riguardi l'esercizio del diritto di opposizione, confermata la completezza e la fondatezza della richiesta stessa, il Titolare, trasmette alle funzioni competenti un elenco dei dati personali di cui interrompere il trattamento, compresa la profilazione, in forma scritta, preferibilmente a mezzo email. Terminate le operazioni di interruzione del trattamento, le funzioni competenti comunicano al Titolare il completamento delle attività, in forma scritta, preferibilmente a mezzo email.
Secondo le modalità indicate, il Titolare, con il supporto delle funzioni competenti, predispone la risposta alla richiesta dell'interessato.

Oltre quanto indicato, nel caso specifico, si applicano le seguenti regole.
Nel contesto dell'utilizzo di servizi della società dell'informazione, l'interessato può esercitare il proprio diritto di opposizione con mezzi automatizzati che utilizzano specifiche tecniche.
Per valutare la fondatezza della richiesta stessa, il Titolare, verifica se la stessa riguarda dati personali che sono trattati per finalità di marketing diretto, compresa la profilazione nella misura in cui sia connessa a tale marketing diretto, caso in cui l'interessato ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano effettuato per tali finalità.
La richiesta è fondata anche qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, salvo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.
Per valutare il respingimento della richiesta stessa, il Titolare, verifica l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.
Qualora i dati personali siano trattati a fini di ricerca scientifica o storica o a fini statistici, la richiesta viene respinta se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico.

Il Titolare del trattamento attua misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, inclusi il diritto di ottenere l'intervento umano (non automatizzato) da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
Qualora la richiesta riguardi esercizio del diritto di non essere sottoposto a una decisione basata unicamente sul trattamento automatizzato, confermata la completezza e la fondatezza della richiesta stessa, secondo le modalità indicate, il Titolare, con il supporto degli uffici interessati, predispone la risposta alla richiesta dell'interessato.
Oltre quanto indicato nel caso specifico, si applicano le seguenti regole.

Per valutare il respingimento della richiesta stessa, il Titolare, verifica che la decisione sia stata presa al verificarsi di una delle seguenti condizioni:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un Titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il Titolare del trattamento);
- si basi sul consenso esplicito dell'interessato.

Comunque, tranne che nel secondo caso, il Titolare, verifica che siano in atto misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, almeno il diritto di ottenere l'intervento umano da parte del Titolare del trattamento, di esprimere la propria opinione e di contestare la decisione.
Qualora i dati personali oggetto della richiesta siano trattati da uno o più responsabili del trattamento, il Titolare del trattamento definisce contrattualmente con i responsabili del trattamento le modalità con le quali essi assicurano l’obbligo di assistere il Titolare del trattamento con misure tecniche e organizzative adeguate nel dare seguito alle richieste di esercizio dei diritti dell’interessato, di cui il Titolare del trattamento resta legalmente responsabile.

XII. FORMAZIONE DEGLI AUTORIZZATI

Al Titolare del trattamento dei dati è affidato il compito di verificare annualmente le necessità di formazione del personale autorizzato ad eseguire i compiti indicati nella lettera di autorizzazione.
Per ogni autorizzato al trattamento il Titolare della Protezione dei Dati definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione specifica ulteriore e la organizza:

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di autorizzati interessate
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO - Informazione sul contenuto e disposizioni del Regolamento UE 2016/679 - Tratti innovativi del G.D.P.R., definizioni di "Privacy" e "Accountability" - I dati delle persone fisiche, perché bisogna tutelarli, la scuola è in prima linea - I dati personali, definizione, riferimenti diretti e indiretti, i dati che non ti aspetti - I soggetti del trattamento: Titolare, Responsabili ed Autorizzati - La figura del Data Protection Officer (D.P.O.) - Le informative e le richieste di consenso, i diritti degli interessati, le liberatorie - Misure adeguate di sicurezza sui dati realmente trattati dal personale scolastico - Il Data breach - Uso delle CREDENZIALI DI ACCESSO ALLA RETE - Concetti di "IGIENE INFORMATICA" - Rilevanza legale del BACK-UP - Il Modello Operativo Privacy (M.O.P.)	TITOLARE DEL TRATTAMENTO I e II COLLABORATORE DEL DIRIGENTE SCOLASTICO RESPONSABILI DI PLESSO FUNZIONI STRUMENTALI CON ACCESSO A DATI PARTICOLARI (ART. 9 G.D.P.R.)
CORSO DI FORMAZIONE PER SOGGETTI DEL TRATTAMENTO - Informazione sul contenuto e disposizioni del Regolamento UE 2016/679 - Cenni di diritto scolastico (potestà genitoriale, uso delle immagini etc.) - Il Modello Operativo Privacy (M.O.P.) - Analisi dei rischi collegati alle attività proprie della categoria - Organizzazione e procedure di sicurezza - Il Data breach - Uso delle CREDENZIALI DI ACCESSO ALLA RETE - Concetti di "IGIENE INFORMATICA"	DOCENTI FUNZIONI STRUMENTALI CON ACCESSO A DATI COMUNI COLLABORATORI SCOLASTICI

XIII. REVISIONI

Il presente Modello Operativo Privacy (M.O.P.) dovrà essere revisionato annualmente.

Il presente Modello Operativo Privacy (M.O.P.) è stato redatto da Luca Corbellini, di concerto con il Titolare del trattamento, in seguito all'acquisizione dell'incarico di Responsabile della Protezione dei Dati Personali (D.P.O. – R.P.D.) sulla base delle informazioni acquisite in uno o più colloqui intercorsi con il personale incaricato dal titolare del trattamento dei dati, a descrivere l'attività svolta negli uffici.
Il Responsabile della Protezione dei Dati non è responsabile per l'esattezza delle informazioni fornite non altrimenti verificabili.

Il Modello Operativo Privacy (M.O.P.) viene letto e confermato in ogni suo punto.

Data _____

Responsabile della Protezione dei Dati Personali (D.P.O.)

_____

Titolare del trattamento

_____