GDPR - EU General Data Protection Regulation

Regolamento Europeo 2016/679

in materia di protezione dei dati personali

GDPR

Registro dei Trattamenti

Ai sensi dell'Art. 30 del R.E. 2016/679

TITOLARE DEL TRATTAMENTO:

DIRIGENTE SCOLASTICO

ROSARIA CORONELLA

SECONDO CIRCOLO "DON PEPPE DIANA" ACERRA

Versione
1.0

Data Agg.to
13.01.2021

DPO
GIS CONSULTING

Indice

1. SCOPO

Il presente Registro dei Trattamenti (di seguito "Registro") è adottato ai sensi dell'Art. 30 del Regolamento Europeo 2016/679 (di seguito "Regolamento"), per tracciare le attività di trattamento in materia di dati personali, i criteri organizzativi adottati e le misure per la protezione dei dati personali.

In particolare il Registro dei Trattamenti contiene idonee informazioni riguardo:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinataria cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
- ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- ove possibile, una descrizione eneraledellemisuredisicurezzatecnicheeorganizzativedicuiall'arti colo32, paragrafo 1.

Il Registro è tenuto in forma scritta, anche in formato elettronico.

Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

Gli obblighi di tenuta del Registro non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1 (che l'istituto può trattare in varie forme), o i dati personali relativi a condanne penali e a reati di cui all'articolo 10 del Regolamento.

2. DEFINIZIONI

Ai fini del presente registro s'intende per:

1) «dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) «trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) «limitazione di trattamento»: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) «profilazione»: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) «pseudonimizzazione»: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) «archivio»: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) «titolare del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) «responsabile del trattamento»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) «destinatario»: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) «terzo»: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) «consenso dell'interessato»: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) «violazione dei dati personali»: la violazione di sicurezza che comporta accidentalmente o in modo illecito

la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) «dati genetici»: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) «dati biometrici»: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) «dati relativi alla salute»: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) «stabilimento principale»:

a)per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b)con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) «rappresentante»: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) «impresa»: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) «gruppo imprenditoriale»: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) «norme vincolanti d'impresa»: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) «autorità di controllo»: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo51;

22) «autorità di controllo interessata»: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) «trattamento transfrontaliero»:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) «obiezione pertinente e motivata»: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) «servizio della società dell'informazione»: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio (19);

26) «organizzazione internazionale»: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

27) trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

3. RIFERIMENTO NORMATIVO

Il Registro è tenuto in osservanza alle seguenti normative:

- Regolamento Europeo 2016/679, Art. 30

4. CAMPO DI APPLICAZIONE

Il Registro ha lo scopo di censire le banche dati in cui vengono memorizzati i dati personali e i relativi flussi informativi che li coinvolgono, le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Questa attività riguarda tutti i dati personali e ogni banca di dati o archivio è classificato in relazione alle informazioni in essa contenute e in relazione al tipo di trattamento eseguito indicando se si trattadi:

- Dati personali (Definizioni, comma 1)
- Dati personali particolari (Art. 9 comma 1, classificazione P)
- Dati personali relativi alla salute (Art. 9 comma 1, classificazione S)
- Dati personali relativi a condanne penali e reati (Art. 10) (classificazione R)
- Dati personali genetici (Definizioni, comma 13) (classificazione G) – non applicabile
- Dati personali biometrici (Definizioni, comma 14) (classificazione B) – non applicabile

I dati personali sono classificati secondo le seguenti

definizioni: Dato personale:
qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale

P - Dati personali particolari
Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale

S - Dati personali relativi alla salute
Dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona

R - Dati personali relativi a condanne penali
e reati Dati e notizie relativi a condanne
penali e reati

G – Dati personali genetici
Dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione

B – Dati personali biometrici

Dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.

5. IL TITOLARE DEL TRATTAMENTO

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario.

Se ciò è proporzionato rispetto alle attività di trattamento, le misure di cui al paragrafo 1 includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.

L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.

Il Titolare del trattamento dati che redige il presente Registro è:

DIRIGENTE DEL 2° CIRCOLO DI ACERRA DON PEPPE DIANA Prof.ssa. ROSARIA CORONELLA

Dati di contatto del titolare: ROSARIA CORONELLA

E-mail:

NAEE10200G@ISTRUZIONE.IT

Il titolare è una istituzione scolastica statale, rappresentata legalmente dal dirigente

6. IL RESPONSABILE DEL TRATTAMENTO (DATA CONTROLLER)

Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.

Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.

I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento:

a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico;

b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza;

c) adotti tutte le misure richieste ai sensi dell'articolo32;

d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento;

e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III;

f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;

g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati;

h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

All'interno della sua organizzazione, il Titolare ha stabilito i seguenti responsabili esterni del trattamento dei dati:

Identificativo	Funzione / Incarico	Tipologia	Modalità
SPAGGIARI SOFTWARE	Fornitore	Responsabile del trattamento	Nomina
GOOGLE	Fornitore	Responsabile del trattamento	Termini di contratto
AXIOS	Fornitore	Responsabile del trattamento	Nomina

7. IL RESPONSABILE DEL DELLA PROTEZIONE DEI DATI (RDP/DPO)

Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta:

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

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nei casi diversi da quelli di cui al paragrafo 1, il titolare e del trattamento, il responsabile del trattamento o le associazioni e gli altri organismi rappresentanti le categorie di titolari del trattamento o di responsabili del trattamento possono o, se previsto dal diritto dell'Unione o degli Stati membri, devono designare un responsabile della protezione dei dati. Il responsabile della protezione dei dati può agire per dette associazioni e altri organismi rappresentanti i titolari del trattamento o i responsabili del trattamento.

Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39.

Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi.

Il titolare del trattamento o il responsabile del trattamento pubblica i dati di contatto del responsabile della protezione dei dati e li comunica all'autorità di controllo.

All'interno della sua organizzazione, il Titolare ha stabilito i seguenti responsabili della protezione dei dati

Identificativo	Funzione / Incarico	Periodo di incarico	Modalità
GIS CONSULTING srl (tecnici: Ing.V.Pianese Dott. G.Miraglia)	RDP (DPO)	1 anno (rinnovo tacito)	AFFIDAMENTO DIRETTO

8. L'ORGANIZZAZIONE CHE EFFETTUA I TRATTAMENTI

La struttura organizzativa è composta dalle seguenti sedi site

Sede: VIA DEI MILLE n. 2 ACERRA

Nella tabella indicate struttura e prestazioni fornite relative alla tenuta della contabilità, della gestione dei dipendenti e dell'infrastruttura informatica.

Struttura	Trattamentioperatidalla llastruttura	Compitidellastruttura	Responsabile
Ufficio Amministrazione Unico (segreteria)	Trattamento dei dati relativi a utenti, fornitori, dipendenti	Tenuta della contabilità aziendale, gestione delle pratiche del personale, pagamento degli stipendi, bonifici, fatturazione, gestione della contabilità dei clienti	– DSGA – INCARICATI – SEGRETERIA
	Trattamento dei dati relativi a clienti	Redazione di preventivi, offerte, contratti di vendita, gestione delle attività di marketing, procacciamento nuovi clienti, Invio, ricezione e smistamento della corrispondenza commerciale, servizi di consulenza di vendita alla clientela	
	Trattamento dei dati relativi a fornitori	Redazione di ordini di acquisto, analisi e selezione dei fornitori, verifica dei listinidi acquisto	
	Trattamento dei dati relativi a dipendenti	Assunzioni, selezione dei candidati, raccolta e verifica delle presenze, gestione pratiche del personale	
	Trattamento dei dati relativi a dipendenti	Elaborazione delle buste paga	
SPAGGIARI	Fornitura di registro elettronico	Responsabile esterno del trattamento	SPAGGIARI
SPAGGIARI/AXIOS	Fornitura segreteria digitale e gestione documentale	Responsabile esterno del trattamento	SPAGGIARI/AXIOS
SPAGGIARI	Fornitura dominio posta elettronica	Responsabile esterno del trattamento	SPAGGIARI
SARES s.r.l.	Gestione sito web	AUTORIZZATI AL TRATTAMENTO	TERRACCIANO ANTONIETTA SPAMPANATO CLAUDIO

All'interno di questa struttura organizzativa, operano a vario titolo figure di responsabili del trattamento (Data Controller) e incaricati al trattamento (Data Processor), secondo quanto previsto dal Regolamento.

Gli Incaricati del trattamento ricevono idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti. Agli Incaricati del trattamento il Responsabile del trattamento consegna una copia di tutte le policy aziendali che riguardano la sicurezza del trattamento dei dati.

9. ISTRUZIONI PER IL TRATTAMENTO DEI DATI PERSONALI E PROTEZIONE DEIDATI PERSONALI

9.1. Principi ed obiettivi in materia di sicurezza e della determinazione delle modalità di trattamento dei dati personali

Gli obiettivi di sicurezza, che l'Istituto, ovvero il titolare, si pone con la redazione e l'aggiornamento del presente manuale, sono:

1. dimostrare che sono adottate le misure tecniche ed organizzative adeguate, secondo quanto previsto dall' art. 24 del GDPR;
2. garantire il rispetto del principio della privacy by design, ai sensi dell'art. 25, comma 1 del GDPR;
3. mettere in atto le misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default), ai sensi dell'art. 25, comma 2 del GDPR;
4. ridurre, a livelli accettabili e gestibili, i principali rischi di sicurezza, a cui il sistema informativo aziendale può essere sottoposto;
5. mantenere, compatibilmente con i vincoli di sicurezza previsti dal GDPR e dalle eventuali indicazioni dell'Autorità Nazionale di Controllo, il massimo livello di usabilità del sistema.

La determinazione dei compiti e delle istruzioni da impartire agli incaricati del trattamento è riportata in apposito allegato (ALL01 IST) e tiene conto altresì dell'organigramma aziendale e dei manuali operativi e di organizzazione, ai quali si rinvia in modo dinamico e funzionale e che costituiscono parte integrante e sostanziale del presente manuale.

9.2. Attività e azioni del titolare del trattamento per la garanzia della conformità dei trattamenti di dati al GDPR

Il titolare del trattamento, provvede a determinare le finalità e le modalità dei trattamenti.

Pertanto, al fine di garantire la conformità delle attività di trattamento dei dati al GDPR, il titolare procede a:

a) Divulgare attraverso sito scolastico o inviare per posta elettronica (all'indirizzo individuale assegnato dall'Istituto o a quello dichiarato all'atto della sottoscrizione del contratto di collaborazione) a ciascuna persona (sia dipendente, sia collaboratore strutturato) le istruzioni scritte per il trattamento dei dati (riportate nell'allegato ALL.01 IST);

b) designare in qualità di autorizzati al trattamento (ossia incaricati al trattamento dei dati) le persone fisiche preposte allo svolgimento delle operazioni di trattamento, utilizzando l'apposita lettera (ALL.02N a-b-c);

d) vigilare sul rispetto da parte degli incaricati e dei soggetti nominati in qualità di responsabili esterni delle istruzioni relative alle misure di sicurezza previste dalla società, adottando le misure correttive e integrative necessarie;

e) collaborare, con i soggetti preposti alla gestione e alla amministrazione dei sistemi, alla definizione del profilo di autorizzazione da associare alle credenziali di autenticazione assegnate a ciascun incaricato del trattamento dei dati. **Per profilo di autorizzazione** si intende "l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti"; il "**sistema di autorizzazione**" è costituito dall'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente;

f) provvedere a richiedere la disattivazione, ovvero la variazione del profilo di autorizzazione associato a ciascun incaricato, nel caso in cui la persona fisica cessi di operare all'interno della struttura di propria competenza ovvero, per qualsiasi motivo, fosse stato modificato il suo profilo professionale;

g) vigilare sull'attività svolta dagli incaricati del trattamento, verificando il rispetto delle procedure operative e delle istruzioni impartite dall'azienda, anche in materia di misure di sicurezza.

Il titolare inoltre, per quanto riguarda la gestione e la manutenzione degli strumenti elettronici, si avvale sia di personale interno, sia di soggetti esterni, che sono nominati amministratori di sistema, in conformità alle indicazioni fornite dal Garante per la protezione dei dati personali nel provvedimento generale del 27 novembre 2008, così come modificato ed integrato con deliberazione del 25 giugno 2009.

La designazione delle persone fisiche in qualità di amministratore di sistema avviene mediante l'utilizzo del modello di lettera di nomina riportata in allegato ALL. 03N, che deve essere consegnata personalmente ovvero trasmessa a mezzo PEC alla persona o al consulente da nominare in qualità di amministratore di sistema o di responsabile esterno del trattamento, con funzioni di amministrazione di sistema.

9.3. – Liceità del trattamento e obblighi di informazione

Il trattamento dei dati personali deve essere svolto in modo lecito, corretto e trasparente, secondo quanto previsto dall'art. 5 del GDPR. Inoltre, la raccolta dei dati deve avvenire per finalità determinate, esplicite e legittime e i dati possono essere trattati in modo che l'attività da svolgere non sia incompatibile con tali finalità. Pertanto, all'interessato o alla persona che fornisce i dati, al momento della raccolta degli stessi, deve essere fornita una idonea informativa, secondo quanto previsto e nelle forme di cui agli articoli 12 –13 – 14 del GDPR.

A tal fine, il titolare ha predisposto un formulario, contenente le diverse informative da utilizzare per tale adempimento. Oltre, all'obbligo di informativa, affinché il trattamento dei dati sia lecito, occorre che siano rispettate le regole di legittimazione, previste rispettivamente per la raccolta ed il trattamento dei dati comuni e dei dati particolari dagli articoli 6 e 9 del GDPR.

10. CATEGORIE DI INTERESSATI E DI DATI PERSONALI TRATTATI

L'elenco delle categorie di interessati e dei relativi dati personali trattati è da tenersi aggiornato continuamente ad ogni variazione dell'elenco delle tipologie di trattamenti effettuati e delle relative banche dati.

Le categorie di interessati e di dati personali oggetto del trattamento da parte del titolare sono:

Trattamento	Finalità del trattamento	Descrizione del trattamento	Categorie di interessati	Categorie di datipersonali	Categorie di destinatari	Trasferimenti a paesi terzi o organizzazioni internazionali	Termini di cancellazione dei dati	Misure di sicurezza tecniche e organizzative specifiche
Busta paga dipendenti	Pagamento delle competenze	Dati anagrafici e contabili	Dipendenti	dati identificativi appartenenza sindacati (P) dati retribuzione	Dipendenti	NO	Termini di legge	Utilizzo di portale con protocollo sicuro HTTPS Cifratura dei dati e delle e-mail Misure di sicurezza generali
Anagrafica dipendenti	Permettere la gestione organizzativa dei lavoratori (turni, ferie, permessi, malattie)	I dati anagrafici vengono acquisiti in fase di assunzione e memorizzati nel gestionale per utilizzi organizzativi quali la gestione interna delle turnazioni, ferie e permessi	Dipendenti e collaboratori	datiidentificativi	Dipendenti	NO	Termini di legge	Verifica delle autorizzazioni di accesso al gestionale Misure di sicurezzageneral i
Fascicolo dipendenti	Permettere la gestione degli oneri fiscali e previdenziali	I fascicoli correnti sono conservati in armadio protetto in ufficio personale e gestiti solo dagli addetti autorizzati	Dipendenti	dati carriera dati sulla salute (P)	Enti pubblici	NO	Termini di legge	Chiusura a chiave di uffici e armadi Misure di sicurezza generali

Anagrafica utenti	Gestione documenti scolastici	I dati sono trattati al fine dell'erogazione dei servizi di istruzione	utenti	dati identificativi dati contabili e bancari dati carriera datisulla salute (P)	Utenti Banche Commercialisti	NO	Termini di legge	Misure di sicurezza generali
Trattamento	**Finalità del trattamento**	**Descrizione del trattamento**	**Categorie di interessati**	**Categorie di datipersonali**	**Categorie di destinatari**	**Trasferimenti a paesi terzi o organizzazioni internazionali**	**Termini di cancellazione dei dati**	**Misure di sicurezza tecniche e organizzative specifiche**
Archiviazione documentale	Archiviazione delle fatture e altri documenti contabili in digitale	In questa banca dati sono gestite le immagini di documenti contabili, fiscale e commerciali, al fine di facilitare la gestione aziendale	utentiFor nitori	dati identificativi fatture e documenti commerciali		NO	Termini di legge	Misure di sicurezza generali
Anagrafiche fornitori	Acquisto di prodotti e servizi	Gestione delle anagrafiche di base e dei dati contabili e bancari del fornitore al fine di acquisire beni e servizi	Fornitori	dati identificativi dati contabili e bancari	BancheCommer cialisti	NO	Termini di legge	Misure di sicurezza generali
Posta elettronica e rubriche	Corrispondenza e contatti con utenti e fornitori	I dati di contatto dei clienti sono gestiti nelle anagrafiche del gestionale	utenti Potenzialiclienti	dati commerciali dati di contatto	ARGO	NO	Termini di legge	Misure di sicurezza generali
Registroelettronico	Servizio per valutazione, comunicazioni e didattica	Gestione anagrafiche, valutazioni, documenti didattici: relazioni con utenti	utenti	Dati anagrafici Dati di contatto valutazioni	ARGO	No	Termini di legge	Misure di sicurezza generali
Sito web	Gestore sito con documentazione didattica, contabile, amministrativa	Gestisce informazioni pubbliche e riservate (area riservata)	Utenti Fornitori Potenziali clienti e fornitori	Dati di contatto, dati contabili e amministrativi	HORIZON	No	Termini di legge	Misure di sicurezza generali

Gestionale segreteria digitale e conservativa	Gestionale, protocollazione , bilancio, documenti riservati	Gestisce informazioni interne e riservate (area riservata)	Ufficio amministrativo	Servizi generali e amministrativi: Dati di contatto, dati contabili, commerciali, didattici, anagrafici e amministrativi	ARGO	No	Termini di legge	Misure di sicurezza generali

11. MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE GENERALI

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio

Il titolare ha adottato o è in procinto di adottare una serie di misure tecniche e organizzative atte a proteggere i dati personali e ad evitare che vi siano rischi per i diritti e le libertà delle persone fisiche.

MISURA ADOTTATA O ADOTTABILE	STATO MISURA	EVENTUALE DESCRIZIONE MISURA
Misure Organizzative		
Determinazione dei termini di conservazione dei dati personali	Attiva	
Formazione di incaricati e responsabili	Attiva	
Policy per l'uso del sistema informatico	Attiva	
Policy per l'uso di internet e la posta elettronica	Attiva	
Policy aziendali per l'uso dei dispositivi mobili (smartphone e tablet)	Attiva	
Policy aziendali per la prevenzione della violazione dei dati	Attiva	
Accordi contrattuali con responsabili esterni	Attiva	
Valutazione dei rischi periodica	Attiva	Annuale, DPO
Policy per inserimento di nuovo personale	Attiva	
Rispetto art.4 L. 300/1973 controllo dei lavoratori	Attiva	
Regole per l'accesso alla posta elettronica in caso di assenza	Attiva	
Misure tecniche		
Verifica periodica delle misure di sicurezza adeguate al rischio	Attiva	Amm. Sistema
Verifica periodica delle banche dati presenti (Data Discovery)	Non Attiva	
Procedure Data Breach	Attiva	Amm. Sistema
Procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento	Attiva	DPIA – AUDIT ANNUALE
Salvataggio dei dati personali	Attiva	Sui server sono presenti backup settimanali.
Ripristino tempestivo della disponibilità e dell'accesso dei dati personali in caso di incidente fisico o tecnico	Attiva	Ci si basa sui report degli ultimi salvataggi fatti (sia per i backup globali sia per quelli parziali) e da lì si procede con i ripristini necessari e/o richiesti in tempi brevi attraverso supporto ditta

Permanenza di riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi di trattamento	Attiva	1 server in sede 1 server in remoto (ARGO) 2 nas di backup in sede
Protezione da intrusion esterne	Attiva	1 firewall Microtec Netger
Protezione da virus e malware	Attiva	ANTIVIRUS ESET NOD32
Procedure per la gestione di possibili infezioni da malware	Attiva	Amm. Sistema
Protezione da accessi interni non autorizzati	Attiva	Password
Protezione delle reti wifi	Attiva	La rete sia wifi sia ethernet è comunque gestita con password.
Aggiornamenti periodici dei software	Attiva	
Regole per la dismissione dell'hardware	Attiva	Prima di smaltire l'hardware presso un o smaltitore accreditato, si provvede a rendere illeggibili i dati contenuti nei dischi
Accesso riservato alla sala	Attiva	Chiusura a chiave
Protezione da interruzioni di energia elettrica	Attiva	Sono presenti 1 gruppi di continuità. La durata della continuità fornita è di circa 40 minuti.
Verifica della sicurezza sito internet	Attiva	Amm. Sistema
Uscita personale – blocco accessi locali e remoti	Attiva	Amm. Sistema
Protezione delle postazioni di lavoro da accessi indesiderati	Attiva	Amm. Sistema
Protezione da installazioni di software non autorizzato	Attiva	Amm. Sistema
Sicurezza delle credenziali di accesso	Attiva	Amm. Sistema
Controllo accessi al sistema informativo	Attiva	Amm. Sistema
Protezione del sito internet da minacce hacker	Attiva	Amm. Sistema
Controllo virus in invio e ricezione posta elettronica	Attiva	Amm. Sistema
Adozione di crittografia in trasmissione di dati particolari	Attiva	Amm. Sistema
Protezione dei log di navigazione internet	Attiva	Amm. Sistema
Cancellazione periodica dei log di navigazione internet	Attiva	Amm. Sistema
Applicazione di filtri alla navigazione internet	Attiva	Attraverso Firewall

11.1.AMMINISTRATORE DI SISTEMA

Il titolare, in ottemperanza al provvedimento del Garante della Privacy del 27 novembre 2008 *("Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema")* ha provveduto alla individuazione ed alla nomina della figura di "Amministratore di sistema".

Elenco Amministratori di Sistema

SARES s.r.l.	*FUNZIONI* Amministrazione della rete informatica Installazione e manutenzione del software Salvataggi e ripristino dei dati e dei sistemi Sicurezza informatica

E' il soggetto che sovrintende alle gestione delle infrastrutture informatiche aziendali, ivi comprese le banche dati oggetto del trattamento dei dati personali.

E' compito di questo soggetto:

- Attivare le credenziali di autenticazione agli incaricati del trattamento
- Prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di back-up;
- Assicurarsi della qualità delle copie di back-up dei dati e della loro conservazione in luogo adatto e sicuro;
- Fare in modo che sia prevista la disattivazione dei Codici identificativi personali (USER-ID), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali (USER-ID) per oltre 6mesi;
- Proteggere gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.

Nota: Il Titolare del trattamento dei dati può nominare ulteriori Amministratori di sistema, specificando gli elaboratori o le banche dati che sono chiamati a sovrintendere, informandoli delle responsabilità che gli sono state affidate in relazione a quanto disposto dalle normative in vigore.

11.2. ADDETTI AL TRATTAMENTO DEI DATI (DATA PROCESSOR)

Ogni persona che all'interno dell'organizzazione tratta dati personali si qualifica come addetto al trattamento dei dati.

Gli addetti al trattamento ricevono idonee ed analitiche istruzioni, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

In caso di trattamento automatizzato di dati, per ogni addetto al trattamento viene indicato lo USER-ID assegnato.

Il tipo di trattamento effettuato da ogni singolo addetto al trattamento può essere differenziato. In particolare ad ogni addetto al trattamento può essere data dal Responsabile del trattamento la possibilità di:

- Inserire nuove informazioni nella banca di dati personali
- Accedere alle informazioni in visualizzazione e stampa
- Modificare le informazioni esistenti nella bancadidatipersonali

- Cancellare le informazioni esistenti nella banca di dati personali

Ad ogni addetto sono state comunicate le credenziali per l'autenticazione per l'accesso al sistema e le relative istruzioni di sicurezza (segretezza delle credenziali, blocco del computer in propria assenza temporanea durante una sessione di trattamento).

All'amministratore di sistema è affidato il compito di verificare ogni sei mesi le autorizzazioni di accesso ai dati oggetto del trattamento e di aggiornare l'elenco degli utenti autorizzati.

11.3. ASSEGNAZIONE E GESTIONE DELLE CREDENZIALI DI ACCESSO AI SISTEMI INFORMATICI

Nel caso in cui il trattamento di dati personali è effettuato con strumenti elettronici, l'amministratore di sistema deve assicurarsi che il trattamento sia consentito solamente agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

Il Responsabile del trattamento dei dati, in accordo con l'amministratore di sistema, definisce le modalità di assegnazione dei nomi identificativi per consentire a ciascun addetto al trattamento di accedere ai sistemi di trattamento delle banche di dati.

All'addetto viene assegnato un codice per l'identificazione associato a una parola chiave riservata conosciuta solamente dal medesimo, oppure un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

L'amministratore di sistema si assicura che il codice per l'identificazione, laddove utilizzato, non potrà essere assegnato ad altri incaricati, neppure in tempi diversi.

In caso si debba accedere, per motivi di manutenzione tecnica o per lavoro, alla postazione dell'addetto in sua assenza, l'amministratore di sistema provvede a modificare la parola chiave dell'addetto e a comunicare la nuova parola chiave al tecnico informatico o al collega che sostituisce l'addetto.
Al ritorno, l'addetto non potrà accedere al sistema e dovrà farsi dire la nuova parola chiave. Una volta avuto accesso al sistema, potrà di nuovo modificarsi la parola chiave in modo da renderla di nuovo riservata.
L'amministratore di sistema si assicura che le credenziali di autenticazione non utilizzate da almeno sei mesi siano disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica. Si assicura che le credenziali siano disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

Ad ogni addetto al trattamento possono essere assegnate o associate individualmente una o più credenziali per l'autenticazione.

La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito. Non deve contenere riferimenti agevolmente riconducibili all'incaricato o al codice di accesso assegnato (user-id). La parola chiave è modificata dall'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi o ogni tre mesi in caso di trattamento di particolari categorie di dati.
Gli addetti adottano le necessarie cautele per assicurare la segretezza della parola chiave e custodire diligentemente ogni altro dispositivo che gli è stato affidato per i sistemi di autenticazione informatica (badge magnetici, tessere magnetiche, ecc..). In particolare è fatto divieto comunicare a chiunque altro addetto le proprie credenziali di accesso al sistema informatico.
Gli addetti hanno l'obbligo di non lasciare incustodito il proprio posto di lavoro e di prendere i necessari accorgimenti per evitare che, durante la loro assenza anche breve, altri addetti o persone non autorizzate possano accedere alla postazione di lavoro.

11.4. SALVATAGGIO DEI DATIPERSONALI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita l'amministratore di sistema stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle Banche di Dati trattate, che in ogni caso vanno effettuate almeno con cadenza settimanale.

In particolare per ogni Banca di dati sono definite le seguenti specifiche:

- il tipo di supporto da utilizzare per le copie di salvataggio
- il numero di copie di salvataggio effettuate ogni volta
- se i supporti utilizzati per le copie di salvataggio sono riutilizzati e in questo caso con quale periodicità
- se per effettuare le copie di salvataggio si utilizzano procedure automatizzate e programmate
- le modalità di controllo delle copie di salvataggio
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati
- l'incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di salvataggio
- le istruzioni e i comandi necessari per effettuare le copie di

salvataggio E' compito degli addetti alle copie di sicurezza delle banche

dati:

- prendere tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere al ricovero periodico degli stessi con copie di sicurezza secondo i criteri stabiliti
- assicurarsi della qualità delle copie di sicurezza dei dati e della loro conservazione in luogo adatto e sicuro ad accesso controllato
- provvedere a conservare con la massima cura e custodia i dispositivi utilizzati per le copie di sicurezza, impedendo l'accesso agli stessi dispositivi da parte di personale non autorizzato
- segnalare tempestivamente al Responsabile della gestione e della manutenzione degli strumenti elettronici, ogni eventuale problema dovesse verificarsi nella normale attività di copia delle banche dati

11.5- CRITERI PER GARANTIRE LA SICUREZZA E LA RESILIENZA DEI SISTEMI E DEI DATI

All'amministratore di sistema è affidato il compito di verificare la situazione delle apparecchiature hardware e software installate con cui vengono trattati i dati, delle apparecchiature periferiche, ed 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, tenendo in particolare conto di:
    - disponibilità di nuove versioni migliorative dei Sistemi operativi utilizzati
    - segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti
    - segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati

- 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 l'amministratore di sistema deve informarne il Responsabile o il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore.

11.6- CRITERI E PROCEDURE PER GARANTIRE LA DISPONIBILITA' E L'INTEGRITA' DEI DATI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, il Titolare o Responsabile del trattamento dei dati dove designato stabilisce, con il supporto tecnico dell'amministratore di sistema, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.

Il titolare ha realizzato un dettagliato piano di ripristino dei dati per riattivare la disponibilità dei dati sui sistemi di elaborazione in seguito ad un eventuale danneggiamento degli stessi.

La decisione di ripristinare la disponibilità dei dati in seguito a distruzione o danneggiamento è compito esclusivo del Responsabile del trattamento dei dati personali. La decisione di ripristinare la disponibilità dei dati deve essere presa rapidamente e in ogni caso la disponibilità dei dati deve essere ripristinata al massimo entro sette giorni.

11.7- PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita di dati a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Gli aggiornamenti dei sistemi antivirus utilizzati sono tempestivi ed effettuati più volte al giorno al fine di ottenere un accettabile standard di sicurezza delle banche dati trattati.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezione o contagio da virus informatici l'amministratore di sistema deve provvedere a:

- Isolare il sistema
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

11.8- PROTEZIONE DEI DATI DA ATTACCHI E INTRUSIONI

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione o di hacker su ogni sistema collegato in rete pubblica.

Inoltre, al fine di tutelare i dati personali contenuti all'interno delle banche dati informatiche occorre installare e configurare un sistema di protezione da eventuali intrusioni da parte di personale non autorizzato. Tale Sistema viene mantenuto costantemente aggiornato.

11.9- TRATTAMENTO DEI DATI SENZA STRUMENTI ELETTRONICI

In considerazione di quanto disposto dal Regolamento, è fatto divieto a chiunque di:

- Effettuare copie su supporti magnetici o trasmissioni non autorizzate dal Responsabile del trattamento dei dati di dati oggetto del trattamento.
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.
- Consegnare a persone non autorizzate dal Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.
- Ulteriori disposizioni agli incaricati vengono fornite nelle istruzioni allegate alle lettere di incarico

11.10- PROCEDURE PER CONTROLLARE L'ACCESSO ALLE STRUTTURE IN CUI VENGONO TRATTATI IDATI

Il Responsabile del trattamento dei dati ha definito le modalità di accesso agli uffici in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati in modo che venga controllato l'accesso da parte di personale non autorizzato.

Per ogni archivio i Responsabili del trattamento dei dati definiscono l'elenco degli addetti autorizzati ad accedervi e impartiscono istruzioni tese a garantire un controllo costante nell'accesso degli archivi.

Gli addetti che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle operazioni.

Qualora i documenti contengano particolari categorie di dati gli addetti sono tenuti a conservarli fino alla restituzione in contenitori muniti di serratura.

L'accesso agli archivi contenenti documenti ove sono presenti particolari categorie di dati è consentito, dopo l'orario di chiusura, previa identificazione e registrazione dei soggetti.

11.11- FORMAZIONE

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno le necessità di formazione del personale addetto al trattamento dei dati con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati.

In particolare gli addetti sono edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Per ogni addetto o gruppi di addetti il Responsabile del trattamento dei dati definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali variazioni della normativa, le necessità di formazione.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

11.12- TRATTAMENTO DI DATI PERSONALI AFFIDATO ALL'ESTERNO

Il Titolare del trattamento ha deciso di affidare il trattamento dei dati in tutto o in parte a soggetti terzi che sono stati individuati quali responsabili del trattamento in esterno.

Sono quindi stati specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.

I Responsabili del trattamento in esterno devono intendersi autonomi titolari del trattamento e quindi soggetti ai corrispettivi obblighi, e pertanto rispondono direttamente ed in via esclusiva per le eventuali violazioni alla legge.

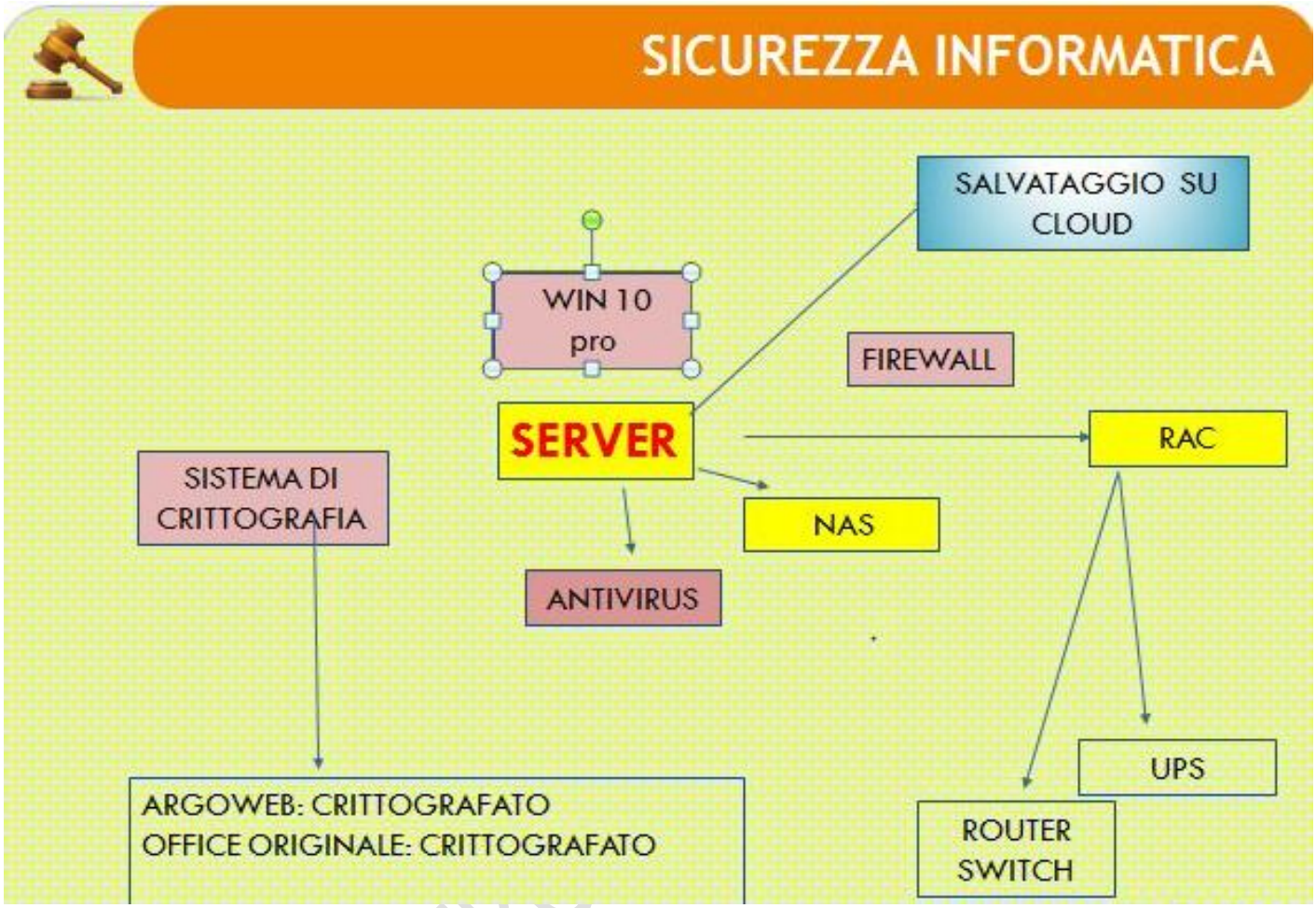
Il Titolare mantiene aggiornato l'elenco dei soggetti esterni che effettuano il trattamento dei dati in qualità di Responsabile del trattamento, ed indica per ognuno di essi il tipo di trattamento effettuato.

Per ogni trattamento affidato ad un soggetto esterno, il Titolare del trattamento stipula un accordo contrattuale che preveda al suo interno il rispetto per entrambe le parti di tutte le norme previste dal Regolamento in questi casi. Nell'accordo vengono inoltre specificati i compiti che sono affidati al Responsabile esterno. Al momento non applicabile in Istituto.

12. AGGIORNAMENTO COSTANTE

Il Registro è da tenersi costantemente aggiornato, almeno annualmente, con le decisioni e le operazioni rilevanti svolte dal Titolare in materia di trattamento di dati personali.

13.ELENCO ALLEGATI



ALLEGATI AL REGISTRO TRATTAMENTO

Documento	Descrizione	Ultima Revisione	Causali aggiornamento	Destinatari	Modalità distribuzione
ALL01-A	SCHEMA FIGURATIVO GESTIONE TRATTAMENTO DATI	NOVEMBRE 2020	Prima redazione	DSGA	
ALL02-N	Designazione responsabile della protezione dei dati personali	NOVEMBRE 2020	Prima redazione	Responsabile Protezione Dati (RPD)	Designazione tramite consegna cartacea
ALL03-Na ALL03-Nb ALL03-Nc ALL03-Nd ALL03-Ne	Lettera designazione autorizzati al trattamento	NOVEMBRE 2020	Prima redazione	Docenti Assistenti Amministivi, Collaboratori scolastici, Funzioni strumentali, DSGA	Designazione tramite consegna cartacea o registro elettronico o pubblicazione in area riservata sito o invio per posta elettronica
ALL04-N	Designazione Amministratore di sistema	NOVEMBRE 2020	Prima redazione	Amm di sistema	Designazione tramite consegna cartacea opec
ALL05-N	Designazione Amministratore Web-social	NOVEMBRE 2020	Prima redazione	Amministratore di sistema web-social	Designazione tramite consegna cartacea o pec
ALL01-IST	Istruzioni in tema di trattamento dei dati	NOVEMBRE 2020	Prima redazione	Docenti Assistenti Amministrativi, Collaboratori scolastici.	Consegna mediante invio per PEC ovvero pubblicazione in area riservata con flag di p.v. o consegna manuale o registro elettronico

MOD01-INF	Formulario informative	NOVEMBRE 2020	Prima redazione	Dipendenti, collaboratori, lavoratori	Consegna a ciascun dipendente o collaboratore all'atto dell'assunzione o della sottoscrizione del contratto
MOD02-INF	Modulistica per consenso dati	NOVEMBRE 2020	Prima redazione	Famiglie	Raccolta del consenso, ove necessario, mediante sottoscrizione di una copia del modulo (all'atto iscrizione)
MOD03-INF	Modulistica per consenso dati	NOVEMBRE 2020	Prima redazione	Fornitori	Raccolta del consenso, ove necessario, mediante sottoscrizione di una copia del modulo
MOD04-INF	Modulistica per consenso per l'utilizzo di immagini di alunni e/o studenti	NOVEMBRE 2020	Prima redazione	Famiglie	Raccolta del consenso, ove necessario, mediante sottoscrizione di una copia del modulo per immagini e video

DOCUMENTAZIONE DI SUPPORTO

				DESTINATARI	**MISSION**
ALL01-PCY	AUDIT01 DI MONITORAGGIO	NOVEMBRE 2020		TITOLARE	Analisi dello stato dell'arte sistema di trattamento dati per prima redazione ed aggiornamento registro
ALL02-PCY	AUDIT02 DI MONITORAGGIO	NOVEMBRE 2020		TITOLARE	Analisi dello stato dell'arte sistema di protezione dati
ALL03-PCY	REGISTRO DATA BREACH	NOVEMBRE 2020		TITOLARE	Registrazione violazioni
ALL04 –PCY	VALUTAZIONE RISCHI TRATTAMENTO DATI (DPIA)	NOVEMBRE 2020		TITOLARE	Valutazione del Rischio correlato al trattamento dei dati personali (DPIA).
ALL05 –PCY	GESTIONE UTILIZZO PIATTAFORME DIGITALI	NOVEMBRE 2020		FAMIGLIE E DIPENDENTI	INFORMATIVE E NORME DI COMPORTAMENTO