MINISTERO DELL' ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA

Guida alla compilazione del Registro delle attività di trattamento

Luglio 2018

Sommario

1. Struttura e obiettivi del documento 2

2. Modalità di compilazione e aggiornamento del Registro delle attività di trattamento 2

3. Definizioni 2

4. Elenco trattamenti 4

4.1 Campo "Riferimenti" 4
4.2 Campo "Attività di trattamento" 4
4.3 Campo "Descrizione dell'attività di trattamento" 5
4.4 Campo "Modalità di trattamento" 5
4.5 Campo "Finalità" 6
4.6 Campo "Tipologia di trattamento" 6
4.7 Campo "Base giuridica del trattamento" 7
4.8 Campo "Informativa" 8
4.9 Campo "Categoria di interessati" 9
4.10 Categoria di dati trattati 10
4.10.1 Campo "Dati comuni" 10
4.10.2 Campo "Categorie particolari di dati personali" 11
4.10.3 Campo "Dati personali relativi a condanne penali e reati" 12
4.11 Campo "Termini di cancellazione (ove possibile)" 12
4.12 Campo "Destinatari esterni dei dati" 13
4.13 Campo "Trasferimenti all'estero" 14
4.14 Campo "Paesi extra-UE o organizzazioni internazionali verso i quali vengono trasferiti i dati" 15
4.15 Campo "Misure di sicurezza" 15
4.15.1 Misure specifiche per la protezione dei dati 15
4.15.2 Misure generali di sicurezza fisica e logica 16
4.15.3 Misure organizzative e processi di governo 18
4.16 Campo "Contitolare del trattamento dei dati" 22
4.17 Campo "Responsabile esterno del trattamento dei dati" 22

5. Contatti dei Contitolari del trattamento dei dati 22

6. Contatti dei Responsabili del trattamento dei dati 23

7. Contatti del Responsabili della protezione dei dati 23

1. Struttura e obiettivi del documento

Il presente documento si pone l'obiettivo di supportare gli utenti nella compilazione e nella predisposizione del Registro delle attività di trattamento, previsto dall'art. 30 del Regolamento UE 679/2016, che è direttamente applicabile negli Stati membri a decorrere dal 25 Maggio 2018.

Il Registro delle attività di trattamento è uno strumento fondamentale per disporre di un quadro aggiornato dei trattamenti in essere all'interno dell'Istituzione scolastica. Esso, inoltre, è indispensabile per la valutazione e l'analisi del rischio.

La tenuta del Registro delle attività di trattamento è parte integrante di un sistema di corretta gestione dei dati personali in quanto consente l'analisi, la ricognizione, la mappatura e la valutazione di conformità delle attività di trattamento svolte rispetto a quanto previsto dal Regolamento.

Al presente documento si allega il *template* del Registro delle attività di trattamento composto dalle seguenti sezioni:

1. Elenco trattamenti
2. Contatti dei contitolari del trattamento dei dati
3. Contatti dei responsabili esterni del trattamento dei dati
4. Contatti del responsabile della protezione dei dati

Per ciascuna sezione sono di seguito descritte le informazioni necessarie alla compilazione del Registro delle attività di trattamento.

2. Modalità di compilazione e aggiornamento del Registro delle attività di trattamento

Al fine di definire il Registro delle attività di trattamento, la sezione "Elenco trattamenti" del file Excel, allegato alla presente guida, deve essere compilata da ogni Istituzione scolastica che effettua, nell'ambito delle proprie attività di competenza, un trattamento di dati personali.

Si ricorda che, ogni qualvolta venga censita una nuova attività di trattamento e/o intervenga una modifica nelle attività di trattamento precedentemente censite, è necessario aggiornare tempestivamente il Registro delle attività di trattamento. Di conseguenza, ogni Istituzione scolastica è tenuta a modificare, eliminare o integrare le informazioni contenute nel Registro delle attività di trattamento precedentemente compilato.

3. Definizioni

Ai fini del presente documento, ai sensi dell'art. 4 del Regolamento UE 679/2016, si intende per:

a) «**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;
b) «**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;

c) «**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;

d) «**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;

e) «**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;

f) «**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;

g) «**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;

h) «**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;

i) «**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;

j) «**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;

k) «**Trattamento transfrontaliero**»:

1. 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

2. 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.

4. Elenco trattamenti

Nell'"Elenco trattamenti" devono essere riportate da ciascuna Istituzione scolastica tutte le informazioni richieste dal Regolamento UE 679/2016 relative alle attività di trattamento di **dati personali** effettuate nell'ambito di propria competenza.

4.1 Campo "Riferimenti"

Istituzione scolastica	
Responsabile della protezione dei dati	
Data di compilazione	

Nel campo "Istituzione scolastica" indicare la denominazione completa e i dati di contatto dell'Istituzione scolastica a cui il Registro delle attività di trattamento si riferisce.

Nel campo "Responsabile della protezione dei dati" indicare la denominazione del Responsabile della protezione dei dati personali designato dall'Istituzione scolastica.

Nel campo "Data di compilazione" indicare la data di compilazione del Registro delle attività di trattamento.

4.2 Campo "Attività di trattamento"

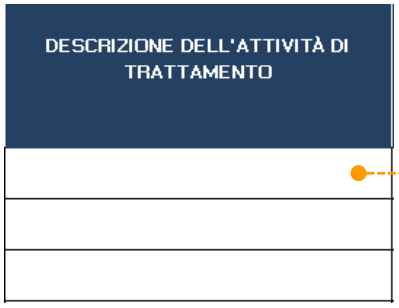
In questo campo indicare la tipologia di attività nell'ambito della quale vengono trattati i dati personali.

L'attività di trattamento è rappresentata dalla tipologia di attività effettuata dall'Istituzione scolastica, che comprende uno o più procedimenti caratterizzati dalla medesima modalità di trattamento, finalità, tipologia di trattamento, base giuridica e categoria o categorie di interessati.

- Indicare la tipologia di attività nell'ambito della quale è effettuato il trattamento di dati

4.3 Campo "Descrizione dell'attività di trattamento"

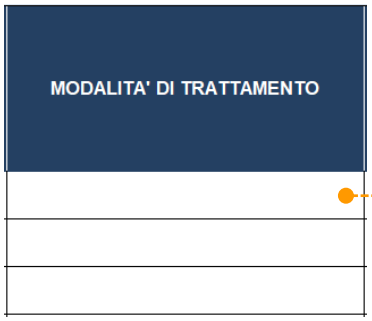
In questo campo inserire una descrizione sintetica dell'attività nell'ambito della quale vengono trattati i dati personali.



- Inserire una breve descrizione dell'attività nell'ambito della quale è effettuato il trattamento dei dati, con indicazione delle sue principali caratteristiche

4.4 Campo "Modalità di trattamento"

In questo campo indicare i mezzi e gli strumenti attraverso i quali viene effettuato il trattamento.



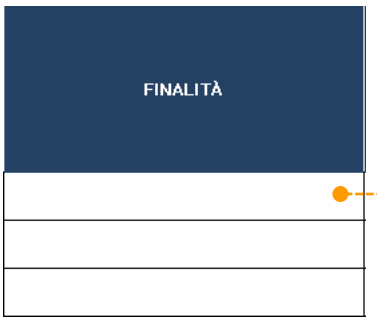
- Indicare **una o più** modalità di trattamento
- Le modalità di trattamento sono:
  - Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici)
  - Utilizzo di strumenti di *office automation* (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc., presenti su una postazione di lavoro)
  - Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Utilizzo di servizi ICT; Utilizzo di strumenti di office automation; Gestione Manuale*".

4.5 Campo "Finalità"

In questo campo indicare lo scopo determinato, esplicito e legittimo, perseguito nell'ambito dell'attività di trattamento di dati personali.

Si precisa che il trattamento è strettamente legato alla finalità.



- Indicare la finalità per cui è effettuato il trattamento

4.6 Campo "Tipologia di trattamento"

In questo campo indicare l'operazione o le operazioni materialmente effettuate sui dati trattati.

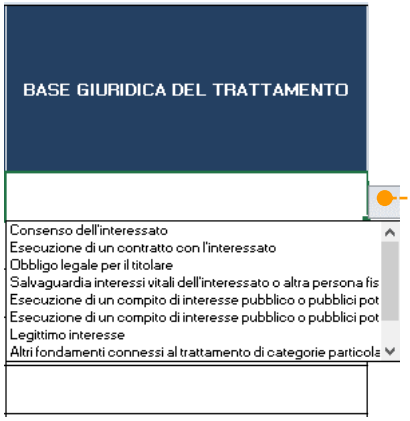
Come riportato nel paragrafo "3. Definizioni", ai sensi dell'art. 4 del Regolamento UE 679/2016, per trattamento si intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a* ***dati personali*** *o insiemi di dati personali, come* ***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***".

- Indicare una o più tipologie di trattamento
- Le tipologie di trattamento sono:
  - Raccolta
  - Registrazione
  - Conservazione
  - Estrazione
  - Consultazione
  - Elaborazione
  - Modifica
  - Comunicazione
  - Diffusione
  - Limitazione
  - Cancellazione
  - Distruzione

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Raccolta; Registrazione; Conservazione*".

4.7 Campo "Base giuridica del trattamento"

In questo campo indicare la condizione che, ai sensi dell'art. 6, par. 1 o dell'art. 9 par. 2 del Regolamento UE 679/2016, rende lecito il trattamento di dati.

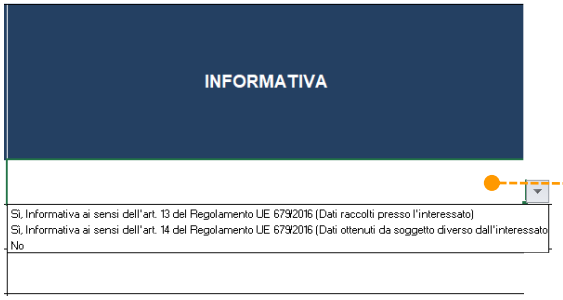


- Selezionare la base giuridica del trattamento cliccando sul pulsante di apertura dell'elenco
- Le basi giuridiche del trattamento sono:
  - Consenso dell'interessato
  - Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso
  - Obbligo legale per il titolare
  - Salvaguardia interessi vitali dell'interessato o altra persona fisica
  - Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
  - Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE
  - Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2 del Regolamento
  - Legittimo interesse

4.8 Campo "Informativa"

In questo campo indicare se è presente un'informativa sul trattamento dei dati personali.

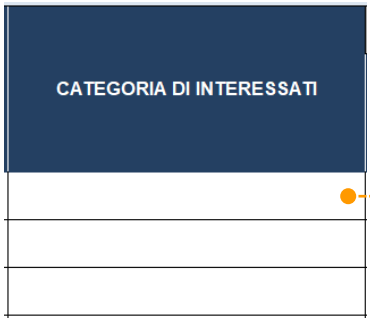
L'informativa è il documento con il quale il titolare del trattamento di dati personali informa l'interessato circa le finalità e le modalità del trattamento medesimo.
I contenuti dell'informativa sono elencati in modo tassativo negli artt. 13 e 14 del Regolamento UE 679/2016.



- Selezionare un'alternativa tra quelle proposte cliccando sul pulsante di apertura dell'elenco
- Le opzioni su "Informativa" sono:
  - Sì, Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato)
  - Sì, Informativa ex art. 14 del Regolamento UE 679/2016 (Dati ottenuti da soggetto diverso dall'interessato)
  - No

4.9 Campo "Categoria di interessati"

In questo campo indicare una o più categorie di interessati al trattamento di dati personali, cioè le categorie di soggetti a cui si riferiscono i dati oggetto del trattamento.



- Indicare una o più categorie di interessati
- Le categorie di interessati sono:

- Studenti
- Studenti minorenni
- Genitori o chi esercita la responsabilità genitoriale
- Personale docente
- Personale ATA
- Dirigenti scolastici
- Familiari del personale scolastico
- Assistenti educativi culturali
- Lavoratori socialmente utili – Altro personale utilizzato
- Contraenti, offerenti e candidati
- Cittadini
- Persone fisiche extra-UE
- Rappresentanti di organizzazioni sindacali
- Rappresentanti e dipendenti di operatori economici
- Rappresentanti e dipendenti di soggetti privati
- Professionisti, intermediari
- Visitatori
- Altri soggetti - Persone fisiche

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Studenti minorenni; Genitori o chi esercita la responsabilità genitoriale*".

4.10 Categoria di dati trattati

I dati personali sono classificabili in varie categorie come di seguito riportato:

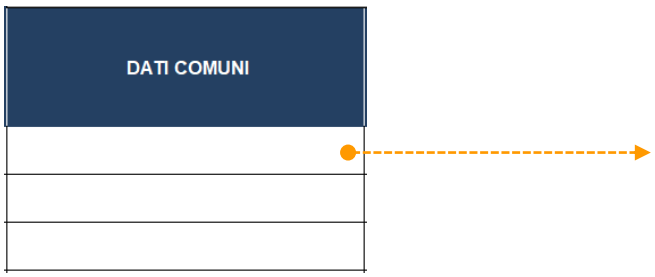
- Dati comuni;
- Categorie particolari di dati personali (in passato c.d. "dati sensibili");
- Dati personali relativi a condanne penali e reati.

Per una stessa attività di trattamento è possibile selezionare una o più voci presenti nei campi a seguire.

Inoltre, la selezione di una o più voci all'interno di una categoria di dati (es. Dati comuni) non esclude la possibilità di selezionare una o più voci all'interno di un'altra categoria di dati (es. Dati personali relativi a condanne penali e reati).

4.10.1 Campo "Dati comuni"

In questo campo indicare le informazioni raccolte che consentono di identificare una persona fisica. Non rientrano nei "Dati comuni" le "Categorie particolari di dati personali" di cui all'art. 9 del Regolamento UE 679/2016 e i "Dati personali relativi a condanne penali e reati" di cui all'art. 10 del Regolamento UE 679/2016.

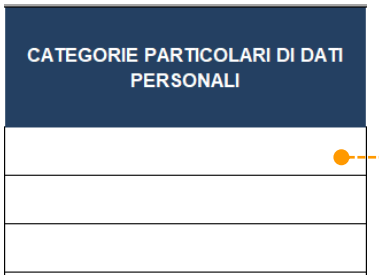


- Indicare una o più categorie di dati comuni
- I dati comuni sono:
  - Dati anagrafici
  - Dati contabili, fiscali e finanziari
  - Dati inerenti il rapporto di lavoro
  - Dati derivanti da tracciamenti (log)
  - Dati inerenti situazioni giudiziarie civili, amministrative, tributarie
  - Dati che consentono la geolocalizzazione
  - Dati audio/foto/video
  - Dati di profilazione

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Dati anagrafici; Dati contabili, fiscali e finanziari*".

4.10.2 Campo “Categorie particolari di dati personali”

In questo campo indicare i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.



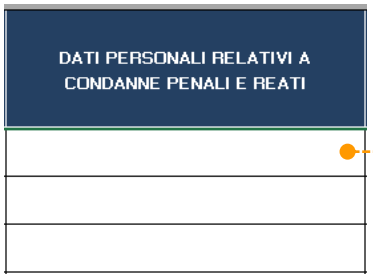
.

- Indicare una o più categorie particolari di dati personali
- Le categorie particolari di dati personali sono le informazioni che rivelano:
  - L'origine razziale ed etnica
  - Le convinzioni religiose, filosofiche o di altro genere
  - Le opinioni politiche
  - L'adesione a partiti
  - L’adesione a sindacati
  - L’adesione ad associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
  - Assistenza sanitaria
  - Lo stato di salute
  - La vita sessuale
  - Dati biometrici

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: “*L’origine razziale ed etnica; Le opinioni politiche*”.

4.10.3 Campo "Dati personali relativi a condanne penali e reati"

In questo campo indicare i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, par. 1 del Regolamento UE 679/2016.



- Indicare una o più categorie di dati personali relativi a condanne penali e reati
- I dati personali relativi a condanne penali e reati sono:
  - Iscrizione nel casellario giudiziale
  - Condizione di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)
  - Sottoposizione a misure detentive carcerarie

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Iscrizione nel casellario giudiziale; Condizione di indagato/imputato o altre situazioni giudiziarie*".

4.11 Campo "Termini di cancellazione (ove possibile)"

In questo campo indicare i termini di cancellazione dei dati personali trattati.

I termini di cancellazione indicano l'arco temporale decorso il quale tali dati dovranno essere cancellati.

Si richiede, ove possibile, di fornire l'indicazione dei termini di cancellazione in mesi o anni oppure i criteri oggettivi utilizzati per determinare tale periodo.

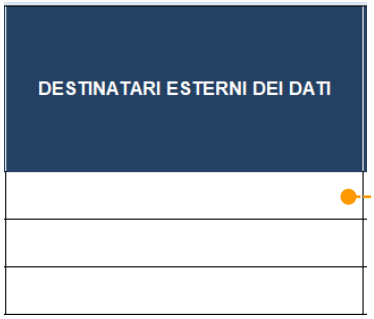
- Indicare i termini di cancellazione dei dati trattati

4.12 Campo "Destinatari esterni dei dati"

In questo campo indicare a quali soggetti vengono comunicati i dati personali trattati al fine di specificare il flusso di informazioni dal titolare verso l'esterno.

I destinatari esterni dei dati sono, quindi, i soggetti ai quali i dati personali possono essere comunicati da parte del titolare.

Si precisa che deve trattarsi di soggetti, diversi dall'interessato, dal titolare, dal responsabile e dai soggetti autorizzati al trattamento dei dati, a cui viene data conoscenza dei dati personali in qualunque forma, anche mediante la loro messa a disposizione o consultazione.



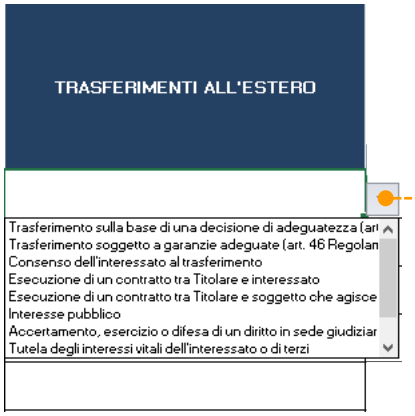
- Indicare uno o più destinatari esterni dei dati
- I destinatari esterni dei dati sono:
  - Pubblica Amministrazione
  - Soggetti privati (persone fisiche o giuridiche)

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Pubblica Amministrazione; Soggetti privati (persone fisiche o giuridiche)*".

4.13 Campo “Trasferimenti all’estero”

In questo campo indicare la condizione che autorizza il trasferimento di dati personali verso paesi terzi (al di fuori dell’UE) oppure organizzazioni internazionali.

L’art. 44 del Regolamento UE 679/2016 definisce il trasferimento come “*qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento* ***dopo il trasferimento verso un paese terzo o un'organizzazione internazionale****, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale*”.



- Selezionare la condizione che autorizza il trasferimento all'estero cliccando sul pulsante di apertura dell’elenco
- Le condizioni che autorizzano il trasferimento all’estero sono:
  - Trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento)
  - Trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento)
  - Consenso dell'interessato al trasferimento
  - Esecuzione di un contratto tra titolare e interessato
  - Esecuzione di un contratto tra titolare e soggetto che agisce per conto dell'interessato
  - Interesse pubblico
  - Accertamento, esercizio o difesa di un diritto in sede giudiziaria
  - Tutela degli interessi vitali dell'interessato o di terzi
  - Predisposizione di un registro normato dal diritto dell'UE
  - Nessun trasferimento all’estero
- Se non vengono effettuati trasferimenti all'estero, scegliere la voce "Nessun trasferimento all'estero"

4.14 Campo “Paesi extra-UE o organizzazioni internazionali verso i quali vengono trasferiti i dati”

Nel caso in cui nel campo "Trasferimenti all'estero" sia stata indicata al presenza di una condizione che autorizza il trasferimento all'estero dei dati personali, in questo campo indicare la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali.

- Inserire la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali

4.15 Campo “Misure di sicurezza”

In questo campo indicare quali misure di sicurezza sono state adottate per la protezione dei dati personali.

Le misure di sicurezza sono costituite dal complesso delle misure organizzative e tecniche volte a ridurre al minimo i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e modifica dei dati.

Nel caso in cui i dati siano trattati attraverso l’utilizzo di servizi ICT, al fine di identificare correttamente le misure di sicurezza adottate, ogni Istituzione scolastica può contattare il proprio fornitore dei sistemi informativi (ovvero il responsabile del trattamento dei dati) per ricevere ulteriori specifiche in merito.

Nel caso in cui i dati sono trattati attraverso l’utilizzo di strumenti di *office automation* o la gestione manuale, ogni Istituzione scolastica, deve elencare le misure tecniche e organizzative che ha posto in essere per la protezione dei dati trattati.

Di seguito si riporta lo schema di sintesi delle misure di sicurezza applicabili, una breve descrizione delle stesse e la modalità di trattamento a cui si riferisce (Servizi ICT, Office, Cartaceo - si veda 4.6 Campo “Modalità di trattamento”)

4.15.1 Misure specifiche per la protezione dei dati

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MPD-1	**Minimizzazione della quantità di dati personali**	Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.	✓	✓	✓
MPD-2	**Partizionamento dei dati**	Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l’archiviazione di documentazione cartacea in faldoni o	✓	✓	✓

		archivi separati.			
MPD-3	**Cifratura**	Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche.	✓	✓	
MPD-4	**Pseudonimizzazione**	Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.	✓		
MPD-5	**Controllo degli accessi logici ed autenticazione**	Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.	✓	✓	
MPD-6	**Cancellazione sicura**	Misura adottata allo scopo di eliminare e distruggere irreversibilmente i dati personali, ad esempio attraverso la smagnetizzazione di un supporto informatico o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.	✓	✓	✓

4.15.2 Misure generali di sicurezza fisica e logica

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MGS-1	**Sicurezza dell'ambiente operativo**	Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT, es file server)	
MGS-2	**Sicurezza della rete e delle comunicazioni**	Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura di rete)	

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
		A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.			
MGS-3	**Tracciatura e monitoraggio**	Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazione svolte. Il monitoraggio delle registrazioni prodotte (c.d. "file di log"), inoltre, consente l'identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-4	**Gestione sicura del cambiamento**	Esistenza ed attuazione di un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell'ultima modifica deve essere conservata.	✓		
MGS-5	**Gestione sicura dell'hardware, delle risorse e dei dispositivi**	Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-6	**Gestione sicura delle postazioni di lavoro**	Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di *office automation*, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	

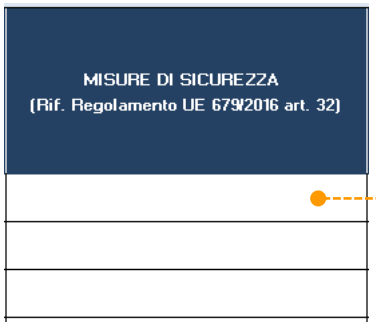
Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
		non autorizzato, accesso a siti potenzialmente pericolosi).			
MGS-7	**Backup e Continuità operativa**	Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MGS-8	**Manutenzione delle apparecchiature**	Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi.	✓	✓	
MGS-9	**Protezione dalle fonti di rischio ambientali**	Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.	✓	✓	✓

4.15.3 Misure organizzative e processi di governo

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
MOG-1	**Modello Organizzativo e di Gestione**	Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.	✓	✓	✓
MOG-2	**Politiche e procedure per la**	La politica per la protezione dei dati personali dimostra l'impegno generale alla	✓	✓	✓

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
	protezione dei dati personali	protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).			
MOG-3	**Gestione dei Responsabili del trattamento e delle terze parti**	I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato.	✓	✓	✓
MOG-4	**Sicurezza del ciclo di vita delle applicazioni e nei progetti**	Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*" introdotti dall'art. 25 del RGPD.	✓	✓ (* per la verifica della presenza della misura rivolgersi al gestore della infrastruttura dei servizi ICT)	
MOG-5	**Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali**	Nel caso si verifichino incidenti di sicurezza che comportano la "*distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati*" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.	✓	✓	✓
MOG-6	**Gestione e formazione del personale**	Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per	✓	✓	✓

Id	Misura	Descrizione	Servizi ICT	Office	Cartaceo
		il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).			
MOG-7	**Controllo degli accessi fisici**	Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.	✓	✓	✓
MOG-8	**Sicurezza dei documenti cartacei**	Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.			✓



- Indicare una o più misure di sicurezza adottate

Le misure di sicurezza sono:

- Minimizzazione della quantità di dati personali
- Partizionamento dei dati
- Cifratura
- Pseudonimizzazione
- Controllo degli accessi logici ed autenticazione
- Cancellazione sicura
- Sicurezza dell'ambiente operativo
- Sicurezza della rete e delle comunicazioni
- Tracciatura e monitoraggio
- Gestione sicura del cambiamento
- Gestione sicura dell'hardware, delle risorse e dei dispositivi
- Gestione sicura delle postazioni di lavoro
- Backup e Continuità operativa
- Manutenzione delle apparecchiature
- Protezione delle fonti di rischio ambientali
- Modello Organizzativo e di Gestione
- Politiche e procedure per la protezione dei dati personali
- Gestione dei Responsabili del trattamento e delle terze parti
- Sicurezza del ciclo di vita delle applicazioni e nei progetti
- Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali
- Gestione e formazione del personale
- Controllo degli accessi fisici
- Sicurezza dei documenti cartacei

Si precisa che, nel caso in cui la scelta ricada su una o più voci di uno stesso elenco, le informazioni devono essere riportate nella cella di testo in modo sequenziale e separate da un **punto e virgola** e uno **spazio**, così come riportato di seguito: "*Minimizzazione della quantità di dati personali; Partizionamento dei dati*".

4.16 Campo "Contitolare del trattamento dei dati"

In questo campo, ove esistente, indicare il nome del contitolare del trattamento.

Sono contitolari del trattamento due o più titolari che determinano congiuntamente le finalità e i mezzi del trattamento.

Nel caso in cui siano individuati uno o più contitolari del trattamento, riportare i riferimenti per esteso nella sezione "Contatti dei Contitolari del trattamento dei dati" del Registro delle attività di trattamento.

Qualora l'indicazione puntuale risulti particolarmente gravosa a causa dell'elevato numero di soggetti, indicare la categoria di riferimento.

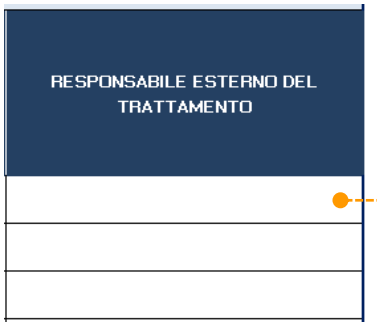
- Indicare il nome del contitolare del trattamento, se presente

4.17 Campo "Responsabile esterno del trattamento dei dati"

In questo campo indicare il nome del responsabile esterno del trattamento.

Il responsabile del trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali **per conto** del titolare del trattamento.

Nel caso in cui sia individuato il responsabile del trattamento, riportare i riferimenti per esteso nella sezione "Contatti dei Responsabili del trattamento dei dati" del Registro delle attività di trattamento.



- Indicare il nome del responsabile del trattamento

5. Contatti dei Contitolari del trattamento dei dati

Nella sezione "Contatti dei Contitolari del trattamento dei dati" devono essere riportati per esteso i contatti dei contitolari, nel caso in cui nella sezione "Elenco trattamenti" – Campo "Contitolari del trattamento dei dati" ne sia stata indicata la presenza.

6. Contatti dei Responsabili del trattamento dei dati

Nella sezione “Contatti dei Responsabili del trattamento dei dati” devono essere riportati per esteso i contatti dei responsabili, nel caso in cui nella sezione “Elenco trattamenti” – Campo “Responsabile esterno del trattamento dei dati” ne sia stata indicata la presenza.

7. Contatti del Responsabili della protezione dei dati

Nella sezione “Contatti del Responsabile della protezione dei dati” devono essere riportati per esteso i contatti del Responsabile della protezione dei dati.