

POLITICHE GENERALI

Politica sulla Protezione dei Dati Personali

INFORMAZIONI DI CONTROLLO DEL DOCUMENTO

Nome del documento:	Politica sulla Protezione dei Dati Personali
Nome del progetto / servizio:	Conformità al Regolamento Generale sulla Protezione dei Dati (GDPR)
Autori del documento:	Vincenzo Mautone
Versione documento:	1.0
Data di emissione:	
Funzione responsabile:	Alta direzione
Classificazione:	Pubblico
Lista di distribuzione:	Tutti i dipendenti e i collaboratori della scuola; tutti gli studenti e docenti e i fornitori connessi al trattamento di dati personali.

REVISORI E APPROVATORI DEL DOCUMENTO

Nome/Ruolo	Azione	Data
V. Mautone, Ufficio Legale	Redazione	1 giugno 2021
Joseph Zurlo, Direzione Didattica	Approvazione	

CRONOLOGIA DELLE MODIFICHE

Revisione	Data	Apportata da	Breve descrizione delle modifiche
	1 giugno 2021	V. Mautone	Prima stesura
1.0			Aggiornamento numero di versione

Indice

1	Introduzione	3
1.1	Finalità	3
1.2	Destinatari	3
1.3	Ambito di applicazione	3
1.4	Gestione del documento	3
1.5	Elenco allegati	3
1.6	Documenti correlati	3
1.7	Termini e definizioni	3
2	Impegno della Direzione	4
3	Requisiti per il trattamento dei dati personali	4
3.1	Principi fondamentali	4
3.2	Liceità del trattamento	4
3.3	Condizioni per il consenso	5
3.4	Trattamento di categorie speciali di dati personali	5
3.5	Trasferimento di dati verso un paese terzo	6
4	Diritti degli Interessati	7
4.1	Comunicazioni da prestare all'Interessato	7
4.2	Informazioni da fornire all'Interessato	7
4.3	Diritto di accesso dell'Interessato	8
4.4	Diritto di rettifica e cancellazione	9
4.5	Diritto di limitazione del trattamento	9
4.6	Diritto alla portabilità dei dati personali	10
5	Deleghe al trattamento dei dati personali	10
5.1	Delega al trattamento dei Dati Personali ricevuta da un Titolare	10
5.2	Delega al trattamento dei dati personali conferita a un Responsabile	11
5.3	Delega al trattamento dei dati personali ai dipendenti della Scuola	11
6	Misure tecniche e organizzative	11
6.1	Valutazione d'impatto sulla protezione dei dati	11
6.2	Misure di sicurezza nel trattamento dei dati	12
6.3	Protezione dei dati <i>by-default</i> e <i>by-design</i>	12
6.4	Registri delle attività di trattamento	13
7	Cooperazione con l'Autorità di Controllo e con la Scuola	14
7.1	Cooperazione con l'Autorità di Controllo	14

7.2	Cooperazione con la Scuola	14
7.3	Notifica di una violazione dei dati personali all’Autorità di Controllo	14
7.4	Comunicazione di una violazione dei dati personali agli Interessati	15

1 Introduzione

1.1 Finalità

La finalità della Politica sulla Protezione dei Dati Personali è quella di comunicare, a tutti i suoi destinatari, i principi generali che la C.E.R.D.O. Srl (d’ora innanzi, anche *la Scuola*) deve costantemente perseguire al fine di:

- 1) Tutelare i diritti e le libertà degli interessati;
- 2) Rispettare le norme cogenti applicabili;
- 3) Salvaguardare la Scuola da possibili sanzioni.

1.2 Destinatari

I destinatari della presente Politica sono tutti i dipendenti, i collaboratori, gli studenti, i fornitori che si trovino a vario titolo a trattare dati personali per i quali *la Scuola* è Titolare, Contitolare o Responsabile rispetto a detto trattamento.

1.3 Ambito di applicazione

La presente Politica si applica a tutti i trattamenti di dati personali operati in veste di Titolare, di Contitolare, o di Responsabile del trattamento, effettuati con mezzi automatizzati, parzialmente automatizzati o manuali. Si configura come trattamento qualsiasi operazione effettuata sui dati personali, inclusa la mera raccolta, conservazione, trasferimento o cancellazione di dati personali. I dati oggetto della presente Politica sono tutti e soli i dati personali afferenti a persone fisiche.

1.4 Gestione del documento

Il presente documento dovrà essere aggiornato e autorizzato in conformità al Sistema di Gestione Qualità della *Scuola*.

1.5 Elenco allegati

Nessuno

1.6 Documenti correlati

- Regolamento UE 2016/679;
- Decreto Legislativo 196/2003;
- Decreto Legislativo 101/2018.

1.7 Termini e definizioni

Vedere art. 4 Regolamento UE 2016/679.

2 Impegno della Direzione

La Direzione si impegna, e impegna tutti i propri dipendenti, studenti, collaboratori e fornitori a trattare i dati personali secondo le istruzioni impartite di volta in volta dalla *Scuola*, in accordo alla presente Politica e in osservanza dei principi e delle regole definite dal Regolamento Europeo UE 2016/679 e dal Codice Privacy nazionale, così come novellato dal D.Lgs. 101/2018 in recepimento del Regolamento Europeo.

3 Requisiti per il trattamento dei dati personali

3.1 Principi fondamentali

Nel corso dei trattamenti operati dalla *Scuola*, direttamente o da terzi per suo conto, i responsabili della pertinente Funzione Aziendale e gli Incaricati al Trattamento dovranno assicurare che i dati personali siano:

- a) trattati in modo lecito, corretto e trasparente nei confronti dei soggetti Interessati;
- b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità;
- c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
- d) esatti e, se necessario, aggiornati; a tal fine devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- e) conservati in una forma che consenta l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati;
- f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti, e dalla perdita, dalla distruzione o dal danno accidentali.

3.2 Liceità del trattamento

Un trattamento potrà considerarsi lecito solo laddove ricorra almeno una delle seguenti condizioni:

- a) l'Interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;
- b) il trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso;
- c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetta *la Scuola* in veste di Titolare del trattamento, sulla scorta di quanto previsto dal diritto nazionale o dell'U.E;
- d) il trattamento è necessario per la salvaguardia degli interessi vitali dell'Interessato o di un'altra persona fisica;

- e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico di cui sia stata investita *la Scuola*, posto che tale circostanza sia prevista nel diritto nazionale o dell'U.E.;
- f) il trattamento è necessario per il perseguimento del legittimo interesse della *Scuola* o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'Interessato che richiedono la protezione dei dati personali, in particolare se l'Interessato è un minore.

Qualora il trattamento avvenga per una finalità diversa da quella per la quale i dati personali sono stati raccolti, e non sia basato sul consenso dell'Interessato o sul diritto nazionale o dell'U.E., al fine di verificare se il trattamento per un'altra finalità sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti bisognerà tener conto, tra l'altro:

- a) di ogni nesso tra le finalità per cui i dati personali sono stati raccolti e le finalità dell'ulteriore trattamento previsto;
- b) del contesto in cui i dati personali sono stati raccolti, in particolare tendo conto della relazione che intercorre tra l'Interessato e *la Scuola*;
- c) della natura dei dati personali, specialmente se sono trattate categorie speciali di dati personali (dati sensibili, dati genetici, dati biometrici), oppure se siano trattati dati relativi a condanne penali;
- d) delle possibili conseguenze per gli Interessati causate dall'ulteriore trattamento previsto;
- e) dell'esistenza di garanzie adeguate, in termini di misure tecniche e organizzative.

3.3 Condizioni per il consenso

Qualora la liceità del trattamento sia basata esclusivamente sul consenso dell'Interessato, questa potrà essere considerata un'adeguata base legale per il trattamento laddove siano fatte salve le seguenti condizioni:

- a) la pertinente Funzione Aziendale sia sempre in grado di dimostrare, in maniera inequivoca, che l'Interessato abbia effettivamente prestato il proprio consenso;
- b) se il consenso è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso sia presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile;
- c) l'Interessato sia posto nelle condizioni di revocare il proprio consenso in qualsiasi momento, con la stessa facilità con cui l'ha accordato, e sia stato informato di questa possibilità prima di prestare il proprio consenso;
- d) se il consenso è prestato nel contesto dell'erogazione di un servizio, tale consenso sia stato liberamente prestato dall'Interessato senza che l'erogazione di tale servizio sia subordinata alla prestazione del consenso.

3.4 Trattamento di categorie speciali di dati personali

Salvo non ricorrano specifiche condizioni, dovrà essere evitato il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche,

l'appartenenza sindacale, nonché lo stato di salute, la vita sessuale o l'orientamento sessuale della persona; dovrà essere altresì evitato il trattamento di dati genetici e di dati biometrici intesi a identificare in modo univoco una persona fisica; dovrà essere infine evitato il trattamento di dati relativi a crimini e condanne di natura penale.

Il presente divieto può trovare giustificata eccezione solo qualora ricorra una o più delle seguenti condizioni:

- a) l'Interessato abbia prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo che il diritto nazionale o dell'U.E. non limiti tale facoltà;
- b) il trattamento sia necessario per assolvere agli obblighi o per esercitare specifici diritti della *Scuola* o dell'Interessato in materia di diritto del lavoro o ai fini della previdenza sociale, nella misura in cui ciò sia consentito dal diritto nazionale o dell'U.E., o da un contratto collettivo di lavoro, in presenza di garanzie appropriate per i diritti fondamentali dell'Interessato;
- c) il trattamento sia necessario a tutelare un interesse vitale dell'Interessato o di un'altra persona fisica, qualora l'interessato si trovi nell'incapacità materiale o giuridica di prestare il proprio consenso;
- d) il trattamento riguardi dati personali resi manifestamente pubblici da parte dello stesso Interessato;
- e) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- f) il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, ovvero per la valutazione della capacità lavorativa del dipendente, sulla scorta di quanto previsto dal diritto nazionale o dell'U.E.

3.5 Trasferimento di dati verso un paese terzo

Il trasferimento di dati personali verso un paese non membro dell'Unione Europea o verso un'organizzazione internazionale è ammesso solo nelle seguenti circostanze:

- a) la Commissione Europea abbia stabilito che il paese terzo, un suo territorio o un suo settore specifico, o l'organizzazione internazionale in questione garantiscano un livello di protezione adeguato;
- b) *la Scuola* sia in grado di fornire garanzie adeguate come da Regolamento e, nel paese di destinazione, gli Interessati dispongano di diritti realmente esercitabili e di efficaci strumenti di ricorso giuridico;
- c) esista un accordo internazionale in vigore tra il paese terzo e l'Italia oppure l'Unione Europea;
- d) l'Interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'Interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;
- e) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'Interessato e *la Scuola*, ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'Interessato;
- f) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra *la Scuola* e un'altra persona fisica o giuridica a favore dell'Interessato;
- g) il trasferimento sia necessario per importanti motivi di interesse pubblico;

- h) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
- i) il trasferimento sia necessario per tutelare gli interessi vitali dell'Interessato o di altre persone, qualora l'Interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
- j) il trasferimento sia effettuato a partire da un registro che, a norma del diritto nazionale o dell'U.E., mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto nazionale o dell'U.E.

4 Diritti degli Interessati

4.1 Comunicazioni da prestare all'Interessato

Al fine di consentire agli Interessati l'esercizio dei propri diritti, le pertinenti Funzioni Aziendali dovranno assicurare l'adozione di specifiche misure tecniche ed organizzative volte a:

- a) fornire all'Interessato tutte le informazioni e le comunicazioni relative al trattamento dei propri dati in forma concisa, trasparente, intelligibile e facilmente accessibile, con linguaggio semplice e chiaro;
- b) agevolare l'esercizio dei diritti dell'Interessato, salvo non sussista l'impossibilità di accertare l'identità del richiedente, ovvero di attribuire con sufficiente esattezza i dati trattati allo specifico Interessato;
- c) fornire all'Interessato le informazioni relative all'azione intrapresa riguardo a una richiesta effettuata, senza ingiustificato ritardo e al più tardi entro un mese dal ricevimento della richiesta stessa;
- d) informare l'Interessato senza ritardo, e al più tardi entro un mese dal ricevimento della richiesta, dei motivi di un'eventuale impossibilità di dare seguito a tale richiesta, e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

4.2 Informazioni da fornire all'Interessato

Contestualmente all'acquisizione dei dati personali, o comunque prima del loro utilizzo se raccolti da fonti diverse dall'Interessato stesso, sarà d'obbligo fornire all'Interessato le seguenti informazioni:

- a) l'identità e i dati di contatto della *Scuola* in qualità di Titolare del trattamento;
- b) i dati di contatto del responsabile della protezione dei dati (DPO), se nominato;
- c) le finalità del trattamento dei dati personali raccolti, nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sul legittimo interesse, quali siano nello specifico i legittimi interessi perseguiti dalla *Scuola* o da terzi;
- e) se i dati saranno trasmessi ad altri soggetti, quali siano gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione,

- ovvero il riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili;
- g) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
 - h) l'esistenza del diritto dell'Interessato di chiedere l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati;
 - i) l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
 - j) il diritto di proporre reclamo a un'autorità di controllo;
 - k) se la comunicazione di dati personali è un obbligo legale o contrattuale, oppure un requisito necessario per la conclusione di un contratto, e se l'Interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
 - l) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e almeno in tali casi, le informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'Interessato.
 - m) in caso di raccolta presso fonti diverse dall'Interessato, la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico.

Qualora si intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui sono stati raccolti, prima di tale ulteriore trattamento bisognerà fornire all'Interessato tutte le informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente.

4.3 Diritto di accesso dell'Interessato

Apposite misure tecniche e organizzative devono essere attuate per consentire agli Interessati di chiedere conferma se sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di poter ottenere l'accesso ai propri dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'Interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali, o la limitazione del trattamento dei dati personali che lo riguardano, o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano stati raccolti presso l'Interessato, tutte le informazioni disponibili sulla loro origine;

- h) l'esistenza di un processo decisionale automatizzato, compresa la profilazione, e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'Interessato dovrà essere informato dell'esistenza di garanzie adeguate relative al trasferimento.

4.4 Diritto di rettifica e cancellazione

Apposite misure tecniche e organizzative devono essere attuate per consentire agli Interessati di ottenere, senza ingiustificato ritardo, la rettifica dei dati personali inesatti che lo riguardano, inclusa l'eventuale integrazione dei dati personali incompleti, anche fornendo dati aggiuntivi.

Analoghe misure devono essere attuate per consentire agli Interessati di ottenere, senza ingiustificato ritardo, la cancellazione dei dati personali che lo riguardano, laddove sussista almeno uno dei seguenti motivi:

- a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;
- b) l'Interessato revoca il consenso su cui si basa il trattamento, e non sussiste altro fondamento giuridico per il trattamento;
- c) l'Interessato si oppone al trattamento, e non sussiste alcun motivo legittimo prevalente per procedere con il trattamento;
- d) i dati personali sono stati trattati illecitamente;
- e) i dati personali devono essere cancellati per adempiere a un obbligo giuridico previsto dal diritto nazionale o dell'U.E.;
- f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione.

La richiesta di rettifica o cancellazione deve essere poi inoltrata dalla *Scuola* a qualsiasi altro soggetto (Contitolare o Responsabile del trattamento) cui siano stati in precedenza trasmessi tali dati personali.

4.5 Diritto di limitazione del trattamento

Apposite misure tecniche e organizzative devono essere attuate per consentire agli Interessati di ottenere la limitazione del trattamento dei dati personali che lo riguardano, laddove ricorra una delle seguenti circostanze:

- a) l'Interessato contesta l'esattezza dei dati personali, e il trattamento può essere limitato per il periodo necessario a verificare l'esattezza di tali dati personali;
- b) il trattamento è illecito e l'Interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo;
- c) i dati personali sono necessari all'Interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;

- d) l'Interessato si è opposto al trattamento, e il trattamento può essere limitato in attesa della verifica circa l'eventuale prevalenza dei motivi legittimi *della Scuola* rispetto a quelli dell'Interessato.

Se il trattamento è limitato a causa di una delle circostanze elencate, tali dati personali sono trattati, salvo che per la conservazione, soltanto con il consenso dell'Interessato, oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria, o per tutelare i diritti di un'altra persona fisica. Nel momento in cui la limitazione al trattamento viene revocato, l'Interessato deve ricevere tempestiva notizia.

4.6 Diritto alla portabilità dei dati personali

Apposite misure tecniche e organizzative devono essere attuate per consentire agli Interessati di ottenere i propri dati personali in un formato strutturato, di uso comune e leggibile da un elaboratore elettronico, laddove ricorrano contemporaneamente le seguenti circostanze:

- a) il trattamento si basi sulla prestazione del consenso, o sia correlato all'esecuzione di un contratto;
- b) il trattamento sia effettuato con mezzi automatizzati.

Se richiesto dall'Interessato e se tecnicamente fattibile, i dati personali così strutturati dovranno poter essere trasmessi direttamente ad un altro titolare del trattamento.

5 Deleghe al trattamento dei dati personali

5.1 Delega al trattamento dei Dati Personali ricevuta da un Titolare

Qualora un trattamento di dati personali venga delegato da un soggetto terzo (Titolare del trattamento) alla *Scuola* (Responsabile del trattamento), tutte le Funzioni Aziendali coinvolte devono far sì che *la Scuola* possa operare nel pieno rispetto del Regolamento e, in particolare, che:

- 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;
- 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) assista il Titolare del trattamento con misure tecniche e organizzative adeguate, al fine di soddisfare l'obbligo del Titolare di dare seguito alle richieste per l'esercizio dei diritti dell'Interessato;
- d) restituisca al Titolare del trattamento tutti i dati personali una volta che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo diverso obbligo di legge;
- e) metta a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi sanciti dal Regolamento e consenta/contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

- f) informi immediatamente il Titolare del trattamento qualora un'istruzione ricevuta violi il Regolamento o altre disposizioni di legge, nazionali o dell'U.E., relative alla protezione dei dati;
- g) non ricorra a un altro soggetto terzo per il trattamento dei dati (Sub-responsabile) senza previa autorizzazione scritta, specifica o generale, del Titolare del trattamento.

5.2 Delega al trattamento dei dati personali conferita a un Responsabile

Qualora un trattamento di dati personali debba essere delegato dalla *Scuola* (Titolare del trattamento) a un soggetto terzo (Responsabile del trattamento), la scelta di tale soggetto deve essere limitata a quei soggetti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'Interessato.

Il mandato a trattare dati personali per conto della *Scuola* deve essere disciplinato da un contratto o da altro atto giuridico a norma del diritto italiano o dell'U.E., che vincoli il Responsabile 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.

5.3 Delega al trattamento dei dati personali ai dipendenti della Scuola

Chiunque agisca sotto l'autorità della *Scuola*, e in particolare sotto l'autorità dei responsabili della specifica Funzione Aziendale cui il dipendente (o il collaboratore, o il consulente) fa riferimento, e abbia accesso occasionale oppure sistematico a dati personali nel corso dell'espletamento delle proprie mansioni, non potrà trattare in alcun modo tali dati se non è istruito in tal senso dal responsabile della pertinente Funzione Aziendale. Tali istruzioni dovranno essere impartite per iscritto, in maniera tempestiva e in forma vincolante; le istruzioni al trattamento dovranno essere inoltre aggiornate ogni qualvolta se ne presenti la necessità.

La delega al trattamento dovrà essere riportata in un apposito registro, ove andranno riportate tutte le informazioni relative allo specifico trattamento, incluso il riferimento alle istruzioni fornite, e l'eventuale scadenza temporale della delega operata.

6 Misure tecniche e organizzative

6.1 Valutazione d'impatto sulla protezione dei dati

Quando un tipo di trattamento preveda in particolare l'uso di nuove tecnologie e, considerati natura, oggetto, contesto e finalità del trattamento, possa presentare un rischio elevato per i diritti degli Interessati, prima di procedere al trattamento è richiesta l'esecuzione di una valutazione d'impatto di tali trattamenti sulla protezione dei dati personali.

Una valutazione d'impatto sulla protezione dei dati personali è richiesta per quei trattamenti appositamente specificati dal Garante Privacy nazionale e, più in generale, nei casi di:

- a) valutazione sistematica e globale di aspetti personali relativi agli Interessati, basata su un trattamento automatizzato, compresa la profilazione, sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- b) trattamento, su larga scala, di categorie speciali di dati personali, o di dati relativi a condanne penali;
- c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Tale valutazione deve contenere almeno le seguenti informazioni:

- 1) una descrizione sistematica del trattamento previsto e delle finalità di tale trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dalla *Scuola*;
- 2) una valutazione della necessità e della proporzionalità del trattamento in relazione alle finalità;
- 3) una valutazione dei rischi che il trattamento comporta per i diritti e le libertà degli Interessati;
- 4) le misure previste per contenere i rischi, indicando le garanzie, le misure di sicurezza e i meccanismi di protezione dei dati personali.

Quando insorgono variazioni del rischio relative alle attività di trattamento, è necessario procedere a un riesame per valutare se il trattamento dei dati personali possa proseguire invariato o se debbano essere introdotte ulteriori misure di controllo e salvaguardia.

6.2 Misure di sicurezza nel trattamento dei dati

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 degli Interessati, tutte le pertinenti Funzioni Aziendali devono porre in essere misure tecniche e organizzative adeguate a garantire un livello di sicurezza conforme al rischio individuato, comprendendo, se necessario:

- a) misure di pseudoanonimizzazione e/o di cifratura dei dati personali;
- c) misure atte ad assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- d) misure atte ad assicurare la capacità di ripristino tempestivo della disponibilità e l'accesso dei dati personali in caso di incidente fisico, umano o tecnico;
- e) procedure apposite per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel valutare l'adeguato livello di sicurezza, si tiene conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

6.3 Protezione dei dati *by-default* e *by-design*

All'atto di definire le modalità e i mezzi di trattamento dei dati personali devono essere identificate opportune misure tecniche e organizzative volte a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale principio

deve essere applicato alla quantità dei dati personali raccolti, alla portata del trattamento, al periodo di conservazione e all'accessibilità dei dati stessi. In particolare, dette misure devono garantire che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza che ciò sia voluto.

Inoltre, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti degli Interessati, al momento di determinare le modalità e i mezzi del trattamento devono essere identificate opportune misure tecniche e organizzative volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti della presente Politica e quelli del Regolamento Europeo sulla Protezione dei Dati.

6.4 Registri delle attività di trattamento

Al fine di conformarsi agli obblighi di legge e di garantire un efficace ed efficiente governo dei trattamenti operati, è richiesta la tenuta di appositi registri per le attività di trattamento prestate in qualità di Titolare.

Se *la Scuola* opera in qualità di Titolare del trattamento, tale registro deve contenere, al minimo, le seguenti informazioni:

- a) le finalità dello specifico trattamento o dello specifico insieme di trattamenti;
- b) la descrizione delle categorie di Interessati e delle categorie di dati personali;
- c) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, specificando se si tratta di destinatari di paesi terzi o di organizzazioni internazionali;
- d) nel caso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, l'identificazione del paese terzo o dell'organizzazione internazionale e, nei casi previsti dalla norma, la documentazione relativa alle garanzie adeguate;
- e) i termini ultimi previsti per la cancellazione delle diverse categorie di dati, ovvero il criterio temporale applicato per la cancellazione delle diverse categorie di dati;
- f) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate a protezione dello specifico trattamento.

Se *la Scuola* opera in qualità di Responsabile del trattamento, tale registro deve contenere, al minimo, le seguenti informazioni:

- a) il nome e i dati di contatto di ogni Titolare del trattamento per conto del quale si opera il trattamento o l'insieme dei trattamenti e, ove applicabile, i dati del Responsabile della Protezione dei Dati;
- b) le categorie dei trattamenti effettuati per conto di ogni Titolare del trattamento;
- c) nel caso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, l'identificazione del paese terzo o dell'organizzazione internazionale e, nei casi previsti dalla norma, la documentazione relativa alle garanzie adeguate;

- d) una descrizione generale delle misure di sicurezza tecniche e organizzative adottate a protezione dello specifico trattamento.

7 Cooperazione con l’Autorità di Controllo e con la *Scuola*

7.1 Cooperazione con l’Autorità di Controllo

L’intero personale aziendale, e in particolare i responsabili delle pertinenti Funzioni Aziendali, devono porsi a disposizione della Autorità di Controllo per supportarla nell’esecuzione dei propri compiti, fornendo la documentazione richiesta e accompagnando le figure incaricate nel corso delle eventuali verifiche ispettive.

Salvo ciò non sia contrario alle disposizioni di legge vigenti al momento, o in contrasto con uno specifico ordine dell’Autorità di Controllo, i dipendenti e consulenti e collaboratori coinvolti nelle verifiche ispettive dovranno opportunamente informare la Direzione sull’andamento e sugli esiti delle verifiche stesse.

7.2 Cooperazione con la *Scuola*

L’intero personale aziendale, e in particolare i soggetti incaricati di definire, effettuare o controllare l’esecuzione di un trattamento di dati personali deve – senza ingiustificato ritardo – riportare ai responsabili delle pertinenti Funzioni Aziendali e, se necessario, ai rappresentanti di Direzione, qualsiasi violazione della presente Politica o comunque qualsiasi irregolarità egli reputi lesiva dei diritti degli Interessati, ovvero contraria alle norme di legge in materia di protezione dei dati personali.

L’intero personale dovrà, più in generale, adoperarsi per supportare *la Scuola* nella piena applicazione della presente Politica e al rispetto di tutte le norme cogenti in materia di protezione dei dati personali.

7.3 Notifica di una violazione dei dati personali all’Autorità di Controllo

In caso di violazione dei dati personali, i responsabili delle pertinenti Funzioni Aziendali devono immediatamente notificare tale violazione alla direzione e, congiuntamente ad essa, approntare e inoltrare una formale notifica della violazione all’Autorità di Controllo competente, ove possibile entro 72 ore dal momento in cui si è venuti a conoscenza della violazione, salvo sia improbabile che tale violazione dei dati personali presenti un rischio per i diritti degli Interessati.

Nel caso in cui *la Scuola* operi in qualità di Responsabile del trattamento, tale notifica dovrà essere trasmessa, con le medesime modalità, al Titolare del trattamento dati pertinente la specifica violazione.

Tale notifica deve, almeno:

- descrivere la natura della violazione dei dati personali comprese, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto presso cui ottenere maggiori informazioni circa la violazione;
- descrivere le probabili conseguenze della violazione occorsa ai dati personali;

- d) descrivere le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Tutte le violazioni occorse ai dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio, devono essere riportate in un apposito registro. La trascrizione della violazione è dovuta anche quando questa, per l'esigua gravità, non è stata né sarà notificata all'Autorità di Controllo. Tale registro deve essere reso prontamente disponibile in caso di verifica ispettiva.

7.4 Comunicazione di una violazione dei dati personali agli Interessati

In aggiunta a quanto definito nella clausola precedente, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà degli Interessati, *la Scuola* deve, senza ingiustificato ritardo, comunicare la violazione a tutti gli Interessati coinvolti nella violazione. Tale comunicazione deve seguire la notifica all'Autorità di Controllo.

Tale comunicazione agli Interessati deve essere formulata con un linguaggio semplice e chiaro, e deve descrivere la natura della violazione dei dati personali riportando le informazioni già indicate nella precedente clausola.

Non è invece richiesta la comunicazione agli Interessati se è soddisfatta una delle seguenti condizioni:

- a) *la Scuola* ha posto in essere adeguate misure tecniche e organizzative di protezione, e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- b) *la Scuola* ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli Interessati.

Nei casi in cui la comunicazione sia dovuta ma, per numerosità o per irraggiungibilità diretta degli Interessati, non sia fattibile o richieda comunque sforzi sproporzionati, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli Interessati sono informati con analoga efficacia.

Roma, 1 giugno 2021

C.E.R.D.O. S.r.l.
L'Amministratore
(dott. Massimo Castellacci)