PFP Valtellina
polo di formazione professionale

PFP Valtellina Prot. n. Din. 756/2018 Data 19/12/2018

Azienda Speciale per la Formazione Professionale della Provincia di Sondrio
Via Carlo Besta, 3 - Sondrio
P.IVA: 00867240145

Disciplinare Interno Privacy

Descrizione	Documento interno valido per la verifica della conformità al Regolamento Europeo sulla Protezione dei Dati Personali n. 2016/679.
Luogo e data	Sondrio, 27/11/2018
Approvazione	Titolare del trattamento
Elenco delle revisioni	1 – 27/11/2018
Principali modifiche dalla revisione precedente	-

1 Sommario

2 Finalità del presente documento

Il presente documento è redatto come valutazione interna eseguita dalla struttura per la conformità al Regolamento n. 2016/679.

I riferimenti normativi presi in considerazione nel presente documento sono:

- Regolamento n. 2016/679.
- Provvedimento dell'Autorità Garante per la protezione dei dati del 27 novembre 2008 in materia di amministratori di sistema.
- Provvedimento dell'Autorità Garante per la protezione dei dati del 13 marzo 2007 in materia di posta elettronica e strumento internet.
- Provvedimento dell'Autorità Garante per la protezione dei dati del 8 aprile 2010 in materia di videosorveglianza.
- Provvedimento dell'Autorità Garante per la protezione dei dati in materia di individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie - 8 maggio 2014.

L'esito dell'attività di gestione degli obblighi descritti nei punti precedenti è un insieme di documenti per il sistema di gestione privacy che sono di seguito riepilogati:

- Politica sulla protezione dei dati (POL01)
- Linea guida sul Registro dei trattamenti (LGU01)
- Linea guida sulla Valutazione dei Rischi (LGU02)
- Procedura sui controlli interni (Audit) (PRO01)
- Procedure di gestione dei responsabili esterni (PRO02)
- Procedura di gestione del consenso specifico (PRO03)
- Procedura di gestione del sistema di videosorveglianza (PRO04)
- Procedura di accesso e manutenzione dei dati personali dell'interessato (PRO06)
- Procedura di gestione delle informative (PRO07)
- Procedura di gestione degli incidenti (PRO08)
- Procedura di revoca del consenso (PRO09)
- Procedura di comunicazione agli interessati (PRO10)
- Procedura per l'utilizzo strumentazione informatica (PRO11)
- Procedura di gestione dell'informazione (PRO12)

All'interno dei documenti che descrivono le linee guida, politiche e procedure è descritto lo scopo e i destinatari. I documenti delle linee guida, politiche e procedure e i relativi allegati sono parte del sistema di gestione.

3 Descrizione dell'organizzazione

L'azienda speciale per la Formazione Professionale della Provincia di Sondrio è un CFP che eroga servizi di formazione agli utenti del bacino di Sondrio e Sondalo ed è accreditato dalla Regione Lombardia avente sede legale a Sondrio.

4 L'architettura di sicurezza nel trattamento dei dati personali

Per la conformità al Regolamento è necessario definire un'architettura di sicurezza che permetta di dimostrare le attività e i sistemi che garantiscono la riservatezza, l'integrità e la disponibilità dei dati personali.

L'architettura di sicurezza è l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscono in ogni struttura organizzativa, ambiente informatico, sistema informativo, singolo elaboratore, il rispetto degli standard di sicurezza definiti dalla struttura economica dell'azienda.

Gli elementi essenziali di un'architettura sono:

- ***funzioni di sicurezza***: identificazione e autenticazione degli utenti, controllo accessi ai dati ed alle applicazioni, ecc.
- ***Meccanismi di sicurezza***: i prodotti Hardware, Software e servizi Software esterni utilizzati in Cloud che realizzano le funzioni di sicurezza previste nell'architettura.
- ***Oggetti di sicurezza***: oggetti informatici che sono funzionali ai meccanismi di sicurezza tra cui password, liste d'accesso.
- ***Processi di gestione***: insieme dei processi e delle regole per la gestione delle funzioni, dei meccanismi e degli oggetti di sicurezza che fanno parte della architettura (compresi i processi d'allarme e controllo).

5 Elementi che caratterizzano il programma d'adeguamento, nonché le fasi in cui esso è eventualmente ripartito

Il ciclo sicurezza può essere definito nelle seguenti fasi/operazioni:

- organizzazione;
- individuazione informazioni rilevanti;
- contromisure possibili;
- definizione della politica aziendale sulla sicurezza;
- realizzazione delle misure decise;
- formazione;
- amministrazione;
- auditing e controlli.

5.1 Organizzazione

S'intendono gli elementi fondamentali della struttura organizzativa coinvolti nel trattamento dei dati personali:

- il "titolare del trattamento" dei dati;
- il "responsabile della protezione dei dati", se esistente;
- gli "addetti al trattamento";
- gli amministratori del sistema informatico nel caso di sistemi in rete;
- gli eventuali prestatori di servizi, nominati eventualmente "responsabili esterni del trattamento" che trattano all'esterno dell'impresa dati per conto della stessa impresa

(consulenti elaborazione paghe, professionisti, società di certificazione del bilancio, società d'assistenza software);

- gli eventuali responsabili per la gestione dei salvataggi dei dati personali su supporto informatico.

5.2 Le misure per la protezione dei dati

L'analisi si è svolta preliminarmente con riferimento alla situazione aziendale e successivamente individuando le misure di sicurezza adottate/da adottare:

- modalità di esecuzione delle misure di sicurezza adeguate rispetto al rischio che incombe sui dati e sugli archivi;
- criteri tecnici e organizzativi per la protezione delle aree e dei locali e procedure di controllo per l'accesso;
- criteri e procedure per assicurare l'integrità dei dati;
- criteri e procedure per la sicurezza delle trasmissioni dei dati e per le restrizioni di accesso.

5.3 Definizione della politica aziendale sulla sicurezza

È fondamentale che si prenda atto dei rischi e si definisca un'adeguata risposta in termine di politica aziendale (regole, organizzazione, responsabilità, ecc.) e relativi budget di spesa. Il bilanciamento costi-benefici e l'accettazione dei rischi residui, sono parte non rinunciabile di questa fase. Il risultato concreto è la costruzione dello standard aziendale di sicurezza.

5.4 Formazione

È un elemento determinante; senza una cultura e una preparazione degli incaricati, il piano sicurezza rischia di non essere efficace.

5.5 Amministrazione

Sicurezza vuol dire regole, vincoli, controlli, liste di accesso, permessi; ciò comporta una parte di lavoro amministrativo.

Senza l'attività di amministrazione, dopo qualche tempo, il sistema di sicurezza si degrada e fallisce i suoi obiettivi.

5.6 Auditing e controlli

Costruire un sistema di sicurezza senza, in qualche modo, verificarne l'efficacia, serve a poco. I sistemi informatici sono normalmente molto complessi (sistemi operativi, applicazioni, banche dati, reti, ecc.) e solo con test accurati si può avere una ragionevole certezza di aver costruito un sistema privo di lacune o manchevolezze. Ovviamente non possiamo limitarci ai test iniziali, ma questi vanno ripetuti periodicamente.

E' necessario che almeno una volta l'anno si effettui una revisione dei rischi e, se necessario, anche delle altre fasi, fermo restando le scadenze imminenti previste dalla normativa.

6 Procedure di gestione adottate o da adottare

S'illustra, di seguito, con quali procedure di gestione sono gestiti gli obblighi normativi imposti dal Regolamento n. 2016/679. Le misure minime di sicurezza, previste per le diverse classi o categorie di rischio, sono state descritte nei documenti descritti dalle procedure o dalle attività di valutazione dei rischi.

Nelle sezioni successive sono riportati gli articoli del Regolamento che hanno impatti operativi o che prevedono attività di gestione, per ogni articolo considerato viene fornita una sintesi e vengono definite delle domande di gestione che permettono di definire le procedure di gestione che è presente nel sistema. I rifermenti alle procedure sono definiti sulla base della codifica del sistema di gestione.

6.1 Principi generali

6.1.1 Articolo 3: Ambito di applicazione territoriale

L'articolo definisce l'ambito territoriale del Regolamento. Il regolamento si applica ai titolari del trattamento e ai responsabili del trattamento dei dati che gestiscono o trattano dati di cittadini europei.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Quando si tratta di elaborare dati personali all'interno dell'UE di soggetti interessati al di fuori dell'UE i requisiti del Regolamento sono soddisfatti?	**X**			Nessuna specifica, la domanda è utile per comprendere il perimetro del sistema.
Le imprese, esterne alla UE ma parte del gruppo, che si rivolgono a soggetti interessati in Europa con i loro servizi o che controllano il loro comportamento, sono conformi al Regolamento?			**X**	Nessuna specifica, la domanda è utile per comprendere il perimetro del sistema.

6.1.2 Articolo 4: Definizioni

Le parole chiave come "dati personali", "trattamento", "titolare del trattamento", "responsabile del trattamento" e "consenso", che sono utilizzati all'interno del Regolamento sono definite in questo articolo.

6.1.3 Articolo 5: Principi applicabili al trattamento dei dati personali

L'articolo contiene i principi sulla protezione dei dati in merito a "legittimità, correttezza e trasparenza"; "limitazione della finalità"; "minimizzazione dei dati"; "accuratezza"; "limite di conservazione"; "integrità e riservatezza" e "responsabilità".

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
E' definita una politica generale di gestione dei dati personali in azienda che illustri i ruoli e le responsabilità?	**X**			Politica sulla protezione dei dati

6.1.4 *Articolo 6: Liceità del trattamento*

L'articolo stabilisce le condizioni generali per la liceità del trattamento dei dati personali, compreso il consenso, l'interesse legittimo e le condizioni per l'ulteriore trattamento per uno scopo diverso da quello originario della raccolta dei dati, considerando che il nuovo scopo deve essere compatibile con lo scopo originale. L'articolo elenca tra le altre cose la pseudonimizzazione come misura di salvaguardia per accertare la compatibilità.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Le attività di marketing diretto rispettano gli obblighi del Regolamento?	X			Procedura di gestione del consenso specifico

6.1.5 *Articolo 7: Condizioni per il consenso*

L'articolo 7 stabilisce i requisiti per il consenso (per i requisiti specifici relativi al consenso dei minori, vedere articolo 8) come ad esempio la necessità di essere in grado di dimostrare che il soggetto interessato ha dato il consenso, il form di richiesta, il diritto a revocare il consenso e i presupposti per un consenso fornito liberamente.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Esiste una procedura per documentare l'espressione di consenso ottenute dai soggetti interessati?	X			Procedura di gestione del consenso specifico
Esistono delle procedure per la revoca del consenso al trattamento dei dati e la cancellazione dello stesso?	X			Procedura di gestione del consenso specifico

6.1.6 *Articolo 8: Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione*

Il consenso così come specificato all'articolo Art. 6 (1) a) sul trattamento dei dati in relazione ai servizi della società dell'informazione deve essere dato o essere autorizzato dal titolare della potestà genitoriale se il minore ha meno di 16 anni o, se previsto dalla legislazione nazionale, fino ad un'età inferiore ai 13 anni.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Esistono procedure appropriate per verificare, se necessario, l'età degli utenti?	X			Procedura di gestione del consenso specifico
Esistono misure tecniche adeguate per assicurare che il consenso sia dato o autorizzato dal titolare della potestà genitoriale nel caso in cui il minore non abbia l'età richiesta per dare il consenso se necessario?	X			Procedura di gestione del consenso specifico

6.1.7 *Articolo 9: Trattamento di categorie particolari di dati personali*

Il trattamento di categorie particolari di dati personali (origini etniche o razziali, credo politico, religioso o filosofico, appartenenza a sindacati, dati genetici, biometrici o sanitari, dati relativi all'orientamento sessuale della persona) sono solitamente proibiti a meno che non siano applicabili le eccezioni esplicitamente elencate in questo articolo.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Esistono trattamenti di categorie particolari di dati personali e, in caso di consenso, questo è conforme ai requisiti del Regolamento?	X			Registro dei trattamenti Procedura di gestione del consenso specifico
Esistono misure tecniche ed organizzative che proteggono questi dati in modo specifico e sicuro?	X			Valutazione dei rischi

6.1.8 *Articolo 10: Trattamento dei dati personali relativi a condanne penali e reati*

Il trattamento di categorie particolari di dati personali (origini etniche o razziali, credo politico, religioso o filosofico, appartenenza a sindacati, dati genetici, biometrici o sanitari, dati relativi all'orientamento sessuale della persona) sono solitamente proibiti a meno che non siano applicabili le eccezioni esplicitamente elencate in questo articolo.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Nel caso in cui la presentazione del casellario giudiziale faccia parte del processo di assunzione della propria impresa, è autorizzato dalla legislazione dell'Unione o di uno Stato Membro?	X			Registro dei trattamenti: descrive le attività di trattamento
Esistono misure tecniche ed organizzative che proteggono questi dati in modo specifico e sicuro?	X			Valutazione dei rischi: elenca le misure di sicurezza applicate.

6.1.9 *Articolo 11: Trattamento che non richiede l'identificazione*

Il titolare del trattamento non è obbligato a conservare le informazioni per identificare l'interessato al solo scopo di essere conforme al Regolamento. Se il titolare non è in grado di identificare l'interessato, deve se possibile informarne lo stesso.

6.2 Le informative

6.2.1 *Articolo 12: Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato*

L'articolo 12 contiene requisiti dettagliati relativi agli obblighi del titolare di fornire comunicazione e informazioni chiare e trasparenti all'interessato e alle modalità per l'esercizio dei diritti dell'interessato.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	

Esistono delle procedure per verificare che le comunicazioni verso gli interessati siano semplici, chiare e comprensibili?	X			Procedura di gestione delle informative.

6.2.2 *Articolo 13: Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato*

Gli articoli elencano i tipi di informazioni che devono essere fornite all'interessato quando tali dati sono raccolti direttamente dall'interessato.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete controllato le procedure esistenti e il contenuto delle informazioni fornite all'interessato, in particolare per quanto riguarda forma delle comunicazioni e tempi di conservazione?	X			Procedura di gestione delle informative.
Avete verificato l'attuale informativa utilizzata in modo da assicurarvi che contenga tutte le informazioni così come richiesto dal Regolamento?	X			Procedura di gestione delle informative.

6.2.3 *Articolo 14: Informazioni da fornire qualora i dati personali non siano raccolti presso l'interessato*

Gli articoli elencano i tipi di informazioni che devono essere fornite all'interessato quando tali dati sono non raccolti direttamente dall'interessato.

6.3 I diritti

6.3.1 *Articolo 15: Diritto di accesso dell'interessato*

L'articolo stabilisce il diritto dell'interessato di ottenere l'accesso ai dati personali che sono trattati dal titolare e definisce i contenuti delle informazioni (ad esempio scopo, categorie, destinatari, conservazione, reclami alle autorità di controllo, diritto di richiedere la rettifica o la cancellazione dei dati, l'origine dei dati raccolti, l'esistenza di un processo decisionale automatizzato compresa la profilazione, informazione sulla corretta salvaguardia dei dati quando questi vengono trasferiti a paesi terzi).

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete una procedura per la gestione delle richieste degli interessati di ottenere l'accesso ai loro dati e tale procedura è conforme al Regolamento?	X			Procedura di gestione dell'accesso e manutenzione dei dati dell'interessato

6.3.2 *Articolo 16: Diritto di rettifica*

L'articolo stabilisce il diritto dell'interessato di ottenere la rettifica di suoi dati personali inesatti o incompleti.

Questionario	*Conformità*	*Procedure di gestione*

	SI	NO	NA	
Avete una procedura in merito alle richieste degli interessati relative al diritto di rettifica dei dati?	X			Procedura di gestione dell'accesso e manutenzione dei dati dell'interessato

6.3.3 Articolo 17: Diritto alla cancellazione ('diritto all'oblio')

I titolari devono cancellare i dati personali dell'interessato "senza indebito ritardo" su richiesta dell'interessato se i dati non sono più necessari, se l'interessato nega il trattamento, se il trattamento non è effettuato ai sensi di legge o per altro motivo di cui al presente articolo.

Questionario	Conformità			Procedure di gestione
	SI	NO	NA	
Avete una procedura in merito alle richieste degli interessati relative al diritto di cancellazione dei dati?	X			Procedura di gestione dell'accesso e manutenzione dei dati dell'interessato

6.3.4 Articolo 18: Diritto di limitazione di trattamento

L'interessato ha il diritto di richiedere al titolare la limitazione del trattamento.

Questionario	Conformità			Procedure di gestione
	SI	NO	NA	
Avete implementato tecnicamente la possibilità di limitazione dell'utilizzo dei dati?	X			Procedura di gestione dell'accesso e manutenzione dei dati dell'interessato

6.3.5 Articolo 20: Diritto alla portabilità dei dati

Su richiesta il titolare del trattamento trasmette all'interessato i dati che il soggetto interessato ha fornito a lui o ad un altro titolare del trattamento in un formato di uso comune e leggibile da un dispositivo automatico.

Questionario	Conformità			Procedure di gestione
	SI	NO	NA	
Avete una procedura per rispondere alle richieste degli interessati di ricevere i dati in formato strutturato, di uso comune e leggibile da dispositivo automatico e di trasmetterli ad un altro titolare del trattamento?	X			Procedura di risposta agli interessati
Avete una procedura per informare l'interessato, al massimo entro un mese, sulle ragioni per le quali non è stata presa in carico la sua richiesta se ci sono delle ragioni per non aver preso in carico la richiesta dell'interessato?	X			Procedura di risposta agli interessati

6.3.6 Articolo 21: Diritto di opposizione

Gli interessati hanno il diritto di opporsi al trattamento dei dati se si basa su ragioni di interesse pubblico o legittimi interessi del titolare, con il risultato che l'elaborazione deve interrompersi a meno

che gli interessi del titolare siano superiori a quelli del soggetto interessato. Il soggetto interessato può anche opporsi al trattamento dei dati per scopi di marketing diretto.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Siete in grado di verificare gli interessi legittimi del titolare in caso di opposizione di un interessato?	**X**			Procedure di gestione della revoca del consenso
Le persone sono informate chiaramente e separatamente per ogni punto della prima comunicazione sul loro diritto di opporsi (ad esempio, avvisi e criteri)?	**X**			Procedure di gestione della revoca del consenso
Esiste una procedura che assicura che il trattamento dei dati può essere immediatamente interrotto nel momento in cui l'interessato si oppone al trattamento per finalità di marketing diretto e di marketing diretto basato sulla profilazione?	**X**			Procedure di gestione della revoca del consenso
Esiste una procedura che consenta all'interessato di opporsi tramite processi automatici sulla base di specifiche tecniche?	**X**			Procedure di gestione della revoca del consenso

6.3.7 Articolo 22: Processo decisionale automatizzato relative alle persone fisiche, compresa la profilazione

Gli interessati hanno il diritto di non essere soggetti a decisioni basate esclusivamente ad un trattamento automatizzato, inclusa la profilazione, che produca effetti giuridici o li influenzi in modo significativo. Alcune eccezioni si applicano, ad esempio, a decisioni basate sulla profilazione se necessarie per stipulare un contratto con l'interessato.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
È escluso che un minore possa essere coinvolto da una decisione automatizzata?			**X**	Nessuna in particolare. L'attività non è condotta.
Se vengono trattate categorie particolari di dati esiste una base giuridica (consenso esplicito dell'interessato al trattamento di tali dati personali per uno o più scopi specifici – ad eccezione di quando l'Unione o la legislazione degli Stati membri prevede che il divieto del trattamento di tali dati non possa essere revocato dall'interessato)?			**X**	Nessuna in particolare
Esistono misure idonee a tutelare i diritti dell'interessato che includano: Informazioni specifiche sul processo decisionale automatico all'interessato?			**X**	Nessuna in particolare

Esistono misure idonee a tutelare i diritti dell'interessato che includano: Il diritto dell'interessato di opporsi alla decisione, di esprimere il suo punto di vista e di ottenere un intervento umano da parte del titolare?		X	Nessuna in particolare
Esistono misure idonee a tutelare i diritti dell'interessato che includano: Adeguate misure tecniche ed organizzative per proteggere i dati personali e per assicurare che il rischio di errore venga ridotto al minimo?		X	Nessuna in particolare

6.4 Obblighi generali

6.4.1 Articolo 24: Responsabilità del titolare del trattamento

Il titolare del trattamento deve implementare adeguate misure tecniche ed organizzative, inclusa nella maggior parte dei casi una procedura di protezione dei dati, per assicurare ed essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento. Per dimostrare la conformità agli obblighi del titolare possono essere utilizzati l'applicazione di codici di condotta o meccanismi di certificazione.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Effettuate una valutazione dei rischi per tutti i progetti e sistemi più importanti?	X			Valutazione dei rischi
Esiste una procedura che assicura la sicurezza del trattamento dei dati (incluse misure tecniche ed organizzative) prima che vengano avviate attività di trattamento con terze parti?	X			Valutazione dei rischi. Politica di gestione dei dati
È presente documentazione sufficiente a dimostrare la conformità al Regolamento?	X			Valutazione dei rischi
Siete in possesso di certificazioni?	X			Certificazione del sistema qualità ISO 9001:2015.

6.4.2 Articolo 25: Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita

L'articolo 25 implementa i principi della protezione dei dati "by design" e "by default". Il principio della protezione dei dati a partire dalla progettazione ("by design") richiede al titolare del trattamento, al momento della determinazione dei metodi di trattamento e del tempo del trattamento stesso durante il ciclo di vita di un servizio, un prodotto o ogni altra attività di trattamento, di assicurare l'implementazione di adeguate misure tecniche ed organizzative (ad esempio la pseudonimizzazione) in conformità ai principi della protezione dei dati. La protezione dei dati per impostazione predefinita

("by default") obbliga il titolare del trattamento a implementare misure tecniche ed organizzative che garantiscano che siano trattati solamente i dati necessari allo scopo.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Le attività di trattamento avviati o quelli in essere hanno sufficiente documentazione atta a garantire i principi della protezione dei dati "by design"?	**X**			Valutazione dei rischi Procedura di controllo interno (Audit)
Esistono dati gestiti nelle attività di trattamento che risultano non utilizzati (dati raccolti in eccesso)?	**X**			Valutazione dei rischi Procedura di controllo interno (Audit)

6.4.3 Articolo 26: Contitolari del trattamento

L'articolo fornisce la definizione di contitolari del trattamento e le condizioni rilevanti per tali attività congiunte.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Se la vostra azienda in qualità di titolare del trattamento collabora con un altro titolare del trattamento in relazione alle stesse attività di trattamento dei dati, esiste un accordo coerente con l'articolo 26 del Regolamento?	**X**			Procedura di gestione dei responsabili esterni
Esistono dati gestiti nelle attività di trattamento che risultano non utilizzati (dati raccolti in eccesso)?	**X**			Valutazione dei rischi Procedura di controllo interno (Audit)

6.4.4 Articolo 27: Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione

L'articolo definisce l'obbligo, nel caso il Titolare abbia sede fuori dall'Unione, di definire un suo rappresentante all'interno dell'Unione.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Se la vostra azienda ha sede fuori dall'Unione, avete identificato e incaricato il rappresentante con sede nell'Unione?			**X**	L'organizzazione ha sede solo in Italia

6.4.5 Articolo 28: Responsabile del trattamento

L'articolo 28 indica i requisiti nel caso in cui il trattamento debba essere effettuato per conto di un titolare. Inoltre l'articolo contiene indicazioni specifiche se il responsabile del trattamento vuole nominare un altro responsabile.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	

Avete definito un elenco di tutti i responsabili presenti e avete identificato le attività da questi compiute?	X			Procedura di gestione dei responsabili esterni
Avete controllato l'attuale contratto tra le parti per il trattamento dei dati e la sua conformità al Regolamento?	X			Procedura di gestione dei responsabili esterni
Il trattamento dei dati per conto del titolare è disciplinato da un contratto scritto, Art. 28 (9) (accordo per il trattamento dei dati)?	X			Procedura di gestione dei responsabili esterni
E' stato verificato che il responsabile fornisca sufficienti garanzie di attuare misure tecniche ed organizzative adeguate (ad esempio certificazioni)?	X			Procedura di gestione dei responsabili esterni
Avete verificato la conformità con le misure tecniche e organizzative concordate per la prima volta da contratto non appena il contratto è stato firmato ed anche prima dell'inizio del trattamento?	X			Procedura di gestione dei responsabili esterni Procedura di controllo interno (Audit)
Le responsabilità delle parti e le questioni di responsabilità legale sono chiaramente definite nel contratto?	X			Procedura di gestione dei responsabili esterni

6.4.6 *Articolo 29: Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento*

L'articolo 29 definisce l'obbligo del responsabile o degli addetti di conformarsi alle disposizioni del titolare se richiesto da un provvedimento dell'Unione o dalla legislazione di uno stato membro.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete definito una procedura per fornire istruzioni ai responsabili o addetti che agiscono per conto del Titolare.	X			Procedura di gestione dei responsabili esterni Procedura di formazione

6.4.7 *Articolo 30: Registri delle attività di trattamento*

Sia il titolare che il responsabile hanno l'obbligo di conservare delle registrazioni. Il Titolare registra le attività di trattamento che, su richiesta, devono essere rese disponibili alle autorità di controllo. Il Responsabile registra le categorie di trattamento. I requisiti riguardanti i contenuti delle registrazioni sono differenti.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete un elenco delle attività di trattamento svolte?	X			Registro dei trattamenti
Registrate i trattamenti in appositi elenchi che contengano tutte le linee informazioni necessarie previste dall'articolo 30?	X			Registro dei trattamenti

6.5 Sicurezza dei dati personali

6.5.1 Articolo 32: Sicurezza del trattamento

Titolari e responsabili, devono implementare misure tecniche e organizzative per assicurare un livello di sicurezza appropriato al rischio.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
La valutazione dei rischi è effettuata secondo quanto previsto dall'attuale Regolamento?	X			Valutazione dei rischi
Effettuate i controlli di valutazione privacy a campione, allo scopo di controllare se la documentazione e la categorizzazione all'interno della valutazione privacy è effettuata in maniera corretta?	X			Procedura di controllo interno (Audit)
Se la vostra azienda svolge il ruolo di responsabile anche per altre imprese: siete in grado di rispettare i requisiti del Regolamento e dimostrare la conformità?	X			Valutazione dei rischi

6.5.2 Articolo 33: Notifica di una violazione dei dati personali all'autorità di controllo - Articolo 34: Comunicazione di una violazione dei dati personali all'interessato

In caso di violazione dei dati personali, l'autorità di controllo competente deve essere immediatamente informata. Il Titolare deve anche comunicare la violazione dei dati personali all'interessato se la violazione provoca alto rischio per i diritti e le libertà dell'interessato.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
E' presente una procedura di gestione degli incidenti?	X			Procedura di gestione incidenti
La vostra azienda tiene traccia di ogni violazione dei dati personali in conformità ai requisiti del Regolamento?	X			Procedura di gestione incidenti
La vostra azienda ha implementato una procedura di comunicazione delle violazioni dei dati personali?	X			Procedura di gestione incidenti Procedura di comunicazione agli interessati

6.5.3 Articolo 35: Valutazione d'impatto sulla protezione dei dati - Articolo 36: Consultazione preventiva

L'Articolo 35 impone ai titolari l'obbligo di effettuare una valutazione dei rischi sulla protezione dei dati in determinate situazioni di trattamento e ne definisce i requisiti. La valutazione dei rischi è un processo necessario ad identificare e ridurre al minimo i rischi di non conformità. L'articolo 36 obbliga il titolare a consultare le autorità di controllo prima di un trattamento se la valutazione dei rischi individua un alto livello di rischio non mitigato.

Questionario	*Conformità*	*Procedure di gestione*

	SI	NO	NA	
La valutazione dei rischi è effettuata secondo quanto previsto dalla versione applicabile del Regolamento?	X			Valutazione dei rischi
C'è un collegamento tra i processi di sviluppo del prodotto e la valutazione dei rischi, che assicura che ogni nuovo sistema o prodotto tiene conto della valutazione dei rischi?	X			Procedura di controllo interno (Audit)

6.5.4 Articolo 37: Designazione del responsabile della protezione dei dati

L'articolo stabilisce i casi in cui il titolare o il responsabile del trattamento deve individuare un Responsabile per la Protezione dei Dati (Data Protection Officier) e indica le differenti possibilità per ogni nomina.

Questionario	*Conformità*			*Procedure di gestione*
	SI	NO	NA	
È stato individuato un referente interno per tutte le questioni legate alla privacy?	X			Procedura di gestione delle informative Disciplinare interno, sezione organizzazione.
L'azienda ha nominato un Responsabile per la Protezione dei Dati?			X	Non è stato definito come necessario il ruolo di DPO.
I contatti del referente privacy sono stati pubblicati e i contatti del Responsabile per la Protezione dei Dati sono stati comunicati all'autorità di controllo?			X	Non è stato definito come necessario il ruolo di DPO.
Il Responsabile per la Protezione dei Dati soddisfa i requisiti di competenza stabiliti dal Regolamento?			X	Non è stato definito come necessario il ruolo di DPO.

6.5.5 Articolo 38: Posizione del responsabile della protezione dei dati

L'articolo stabilisce i diritti del Data Protection Officer e la sua posizione all'interno dell'organizzazione del titolare e del responsabile.

Questionario	*Conformità*			*Procedure di gestione*
	SI	NO	NA	
Il Responsabile per la Protezione dei Dati ha adeguate risorse umane e finanziarie per implementare i requisiti di protezione dei dati?			X	Non è stato definito come necessario il ruolo di DPO.
C'è un contatto diretto (report diretti) tra il Responsabile per la Protezione dei Dati e la direzione?			X	Non è stato definito come necessario il ruolo di DPO.
Esistono adeguate procedure per assicurare che il Responsabile per la Protezione dei Dati sia coinvolto in modo coerente e per tempo in tutte le questioni relative alla protezione			X	Non è stato definito come necessario il ruolo di DPO.

dei dati personali (esempio valutazione dei rischi privacy)?				
Le modalità di contatto del Responsabile per la Protezione dei Dati sono chiare e trasparenti?			X	Non è stato definito come necessario il ruolo di DPO.
Il Data Protection Officer svolge altre funzioni oltre a quelle di DPO? Se sì, tali attività risultano in conflitto di interesse?			X	Non è stato definito come necessario il ruolo di DPO.

6.5.6 Articolo 39: Compiti del responsabile della protezione dei dati

L'articolo stabilisce le attività e i doveri del Data Protection Officer.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete un programma di formazione?	X			Procedura di formaizone
Avete implementato un programma di controllo (audit) per la conformità al Regolamento?	X			Procedura di controllo interno (Audit)
Svolgete audit periodici per monitorare la conformità al Regolamento, altri requisiti legali o interni per la protezione dei dati in azienda?	X			Procedura di controllo interno (Audit)
Registrate gli audit periodici e la direzione è informata dei risultati delle verifiche?	X			Procedura di controllo interno (Audit)

6.6 Codici di condotta e certificazioni

6.6.1 Articolo 42: Certificazione - Articolo 43: Organismi di certificazione

L'articolo 42 stabilisce il quadro di riferimento per la certificazione della protezione dei dati. Titolare e responsabile possono dimostrare su questa base la conformità al Regolamento attraverso meccanismi di certificazione riconosciuti, sigilli di protezione dei dati e marchi.

L'articolo 43 descrive i requisiti da seguire per gli organismi di certificazione. Il nuovo concetto di certificare le operazioni di trattamento dei dati (vedere la certificazione generale IV.42; 43.6) può supportare la realizzazione di un quadro affidabile e verificabile per le operazioni di trattamento dei dati. Il quadro sarà sviluppato dalle autorità di vigilanza e dalla Commissione europea.

6.6.2 Articolo 44: Principio generale per il trasferimento - Articolo 45: Trasferimento sulla base di una decisione di adeguatezza - Articolo 46: Trasferimento soggetto a garanzie adeguate

Gli articoli dal 44 al 49 del Regolamento stabiliscono le condizioni per il trasferimento internazionale dei dati a paesi terzi. I paesi terzi (al di fuori dell'Unione europea e dell'area economica europea) devono garantire un adeguato livello di protezione dei dati. Il Regolamento contiene diverse possibilità per come stabilire e raggiungere un adeguato livello di protezione dei dati:

1. ***Decisione di adeguatezza della Commissione***: la commissione europea può decidere che un paese terzo, un territorio, un settore e organizzazioni internazionali assicurino un adeguato livello di protezione Articolo 45.

2. ***Adeguate misure di protezione***: i dati possono essere trasferiti ad un paese terzo se esistono adeguate misure di protezione, ad esempio regole aziendali vincolanti, clausole standard per la protezione dei dati e meccanismi di certificazione riconosciuti. Articolo 46.

3. Un trasferimento dei dati richiesto da una sentenza del giudice o da una decisione di un'autorità amministrativa è permesso solamente se basato su un accordo internazionale. Articolo 48.

Deroghe: in assenza di una decisione di adeguatezza e di adeguate misure di protezione, il trasferimento dei dati ad un paese terzo è possibile se vengono soddisfatte determinate condizioni, ad esempio l'interessato ha dato consenso esplicito al trasferimento.

Questionario	***Conformità***			***Procedure di gestione***
	SI	*NO*	*NA*	
Trasferite dati personali a paesi terzi, o permettete l'accesso ai dati a questi paesi?			**X**	Non sono effettuati trasferimenti di dati all'estero verso paesi terzi
Se sì, avete verificato la presenza di una decisione di adeguatezza?			**X**	Non sono effettuati trasferimenti di dati all'estero verso paesi terzi
Se non esistono decisioni del genere vi siete accertati che esistano misure di protezione equivalenti (ad esempio regole aziendali vincolanti, disposizioni europee)?			**X**	Non sono effettuati trasferimenti di dati all'estero verso paesi terzi

6.6.3 Articolo 47: Norme vincolanti di impresa

L'Articolo 47 contiene una lista dettagliata dei requisiti per le norme vincolanti di impresa. Secondo quanto stabilito dall'articolo 46 (5) le autorizzazioni dell'autorità di controllo sulla base dell'articolo 26 (2) della Direttiva 95/46/EC devono rimanere valide a meno che non siano modificati, sostituiti o abrogati da tale autorità di controllo. Le modifiche sostanziali alle norme vincolanti di impresa devono essere concordate con l'autorità di controllo.

Questionario	***Conformità***			***Procedure di gestione***
	SI	*NO*	*NA*	
La vostra organizzazione della privacy locale è pienamente conforme alla parte 4 "Organizzazione della privacy dei dati" delle norme vincolanti di impresa?			**X**	Non sono effettuati trasferimenti di dati all'estero verso paesi terzi
La vostra azienda ha implementato una procedura per segnalare all'autorità di controllo ogni requisito legale nel proprio paese che potrebbe avere effetti negativi sulle garanzie fornite dalle norme vincolanti di impresa, Art. 47 (2) m), §33 Norme vincolanti di impresa?			**X**	Non sono effettuati trasferimenti di dati all'estero verso paesi terzi

6.7 Provvedimenti specifici del garante

6.7.1 Provvedimento in materia di videosorveglianza

Nel caso in cui sia presente un sistema di videosorveglianza installato presso gli spazi dell'organizzazione deve essere preso in considerazione il provvedimento dell' aprile 2010 che definisce le regole di gestione del sistema di trattamento di dati personali.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Sono presenti cartelli informativi presso gli spazi sottoposti a videosorveglianza?	X			Procedura di gestione del sistema di videosorveglianza
Sono definite regole di utilizzo dello strumento videosorveglianza da parte degli addetti specifici mediante procedure, anche tecniche, di utilizzo degli strumenti di trattamento.	X			Procedura di gestione del sistema di videosorveglianza
Sono definite, mediante atto scritto, le motivazioni per cui è presente il sistema di videosorveglianza.	X			Procedura di gestione del sistema di videosorveglianza
Sono presenti documentazioni tecniche che definiscano le caratteristiche del sistema e la collocazione dei punti di ripresa e di registrazione?	X			Procedura di gestione del sistema di videosorveglianza
E' stata valutata la necessità di presentare richiesta di autorizzazione scritta alle autorità competenti per l'installazione dell'impianto di videosorveglianza?	X			Procedura di gestione del sistema di videosorveglianza

6.7.2 Provvedimento in materia di amministratore di sistema

Nel caso in cui siano presenti soggetti specifici (interni o esterni) dedicati alla gestione e manutenzione dei sistemi informatici, essi vanno gestiti così come prescritto dal provvedimento in materia di amministratore di sistema del novembre 2008.

Questionario	*Conformità*			*Procedure di gestione*
	SI	*NO*	*NA*	
Avete identificato tutti gli ambiti presenti dei sistemi informativi ed i relativi soggetti gestori?	X			Procedura di gestione dei responsabili esterni
Avete definito uno strumento di monitoraggio dei log degli accessi dei soggetti definiti amministratori di sistema.	X			Procedura di gestione dei responsabili esterni
Avete valutato la competenza dei soggetti definiti amministratori di sistema.	X			Procedura di gestione dei responsabili esterni

7 Struttura di gestione

7.1 Titolari e responsabili del trattamento

In questo capitolo sono elencate le che hanno un ruolo nel sistema di gestione.

Titolare del trattamento	
Società:	Azienda Speciale per la Formazione della Provincia di Sondrio
Indirizzo:	Via Carlo Besta, 3, Sondrio
Partita IVA:	00867240145
Legale rappresentante*:	Evaristo Pini

Referente privacy – area procedure e documenti	
Società:	Azienda Speciale per la Formazione della Provincia di Sondrio
Indirizzo:	Via Carlo Besta, 3, Sondrio
Nome Cognome:	Luca Valenti

Referente privacy – area IT	
Società:	Azienda Speciale per la Formazione della Provincia di Sondrio
Indirizzo:	Via Carlo Besta, 3, Sondrio
Nome Cognome:	Alessandro Zoaldi

Responsabile della Protezione dei dati	
Società:	Non identificato
Indirizzo:	
Nome Cognome:	

Luoghi di custodia dei dati	
Società:	Azienda Speciale per la Formazione della Provincia di Sondrio
Indirizzo:	Via Carlo Besta, 3, Sondrio
Indirizzo:	Via Zubiani, 37, Sondalo

8 Conservazione

Il presente documento, sarà conservato a cura del titolare del trattamento, presso la sede di Azienda Speciale per la Formazione della Provincia di Sondrio.

9 Approvazione del documento

Titolare del trattamento,

Il legale rappresentante	Firma
Evaristo Pini	

Sondrio,

Data
Sondrio 13/12/2018