CONTRATTO DI NOMINA A RESPONSABILE DEL TRATTAMENTO
E CONFERIMENTO DELLE RELATIVE ISTRUZIONI

Tra

Provincia autonoma di Trento, con sede in Trento, C.A.P. 38122, piazza Dante n. 15, codice fiscale e partita I.V.A. n. 00337460224, rappresentata da:

- dott.ssa Cristina Ioriatti, nata a Ravenna il 14/03/1964, la quale interviene ed agisce in rappresentanza della stessa nella sua qualità di Dirigente del Servizio formazione professionale, formazione terziaria e funzioni di sistema;

e

Enaip Trentino, con sede legale in Trento, Via Madruzzo, n. 41, codice fiscale e partita IVA 00869370221, rappresentato da:

- sig. Arrigo Dalfovo;

di seguito, congiuntamente, le "Parti".

Premesso che:

- tra la **Provincia autonoma di Trento** e **Enaip Trentino** intercorre un rapporto contrattuale, in forza del contratto di servizio per l'affidamento dei servizi di istruzione e formazione professionale previsti dagli strumenti di programmazione settoriale, ai sensi dell'art. 36 commi 1 e 2 della l.p. 7.08.2006, n. 5 e dell'art. 30 del d.p.p. 1.10.2008, n. 42- 149/leg;
- tale rapporto contrattuale implica, necessariamente, il trattamento, da parte di **Enaip Trentino**, di dati personali di cui la **Provincia autonoma di Trento** è Titolare del trattamento;
- il Regolamento UE 2016/679 (di seguito, il Regolamento) "*si applica al trattamento dei dati personali effettuato nell'ambito delle attività (…) di un Responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*";
- ai sensi dell'art. 28, paragrafo 1, del Regolamento, "*Qualora un trattamento debba essere effettuato per conto del Titolare, quest'ultimo ricorre unicamente a Responsabili del trattamento che presentino garanzie sufficienti per mettere in atto*

misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato";

- ai sensi dell'art. 29 del Regolamento, "*Il Responsabile del trattamento, o chiunque agisca sotto la sua autorità, che abbia accesso a dati personali non può trattare tali dati se non è istruito in tal senso dal Titolare…*";
- ai sensi dell'art. 28, paragrafo 3, del Regolamento, inoltre, "*I trattamenti da parte di un Responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico, che vincoli il Responsabile del trattamento al Titolare 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*";
- ai sensi dell'art. 28, paragrafo 4, del Regolamento, "*Quando un Responsabile del trattamento ricorre a un altro Responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del Titolare del trattamento, su tale altro Responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il Titolare del trattamento e il Responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro Responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il Responsabile iniziale conserva nei confronti del Titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro Responsabile*";
- ai sensi dell'art. 31 del Regolamento, "*…il Responsabile del trattamento... coopera…, su richiesta, con l'Autorità di controllo…*";
- ai sensi dell'art. 82, paragrafo 2, del Regolamento, il *"Responsabile del trattamento risponde per il danno causato dal trattamento se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai Responsabili del trattamento o ha agito in modo difforme, o contrario, rispetto alle istruzioni impartite dal Titolare del trattamento*";
- a seguito delle garanzie offerte, dal Codice comportamentale del personale dipendente, dal Codice Etico dei docenti di ENAIP Trentino, nonché dal Registro delle attività di Trattamento adottato ai sensi del GDPR (General Data Protection

Regulation) il Regolamento Europeo per la protezione dei dati personali 2016/679 e considerando la non segnalazione di violazioni al sistema informatico e alla violazione\compromissione dei dati personali e\o sensibili conservati all'interno dei sistemi informatici negli ultimi cinque anni, in forza di quanto previsto al considerando n. 81 del Regolamento, tale soggetto è stato ritenuto idoneo ad assumere la qualifica di Responsabile del trattamento.

Tutto ciò premesso e considerato,
che costituisce parte integrante e sostanziale del presente atto,
si conviene quanto segue.

Art. 1 – Ai sensi e per gli effetti dell'art. 28 del Regolamento e, più precisamente, allo scopo di garantire il rispetto dei relativi paragrafi 3 e 4, con il presente contratto (di seguito, il "Contratto") la **Provincia autonoma di Trento**, in qualità di "*Titolare del trattamento*" (di seguito, il "Titolare"), nomina **Enaip Trentino** "*Responsabile del trattamento*" (di seguito, il "Responsabile"). Il Responsabile, pertanto, si impegna al rigoroso rispetto – con la diligenza di cui all'art. 1176, comma 2, del Codice Civile – della predetta normativa europea, della connessa disciplina nazionale, nonché delle prescrizioni dell'Autorità di controllo. Ferma ogni ulteriore responsabilità nei confronti del Titolare, resta inteso che ogni forma di determinazione delle finalità e/o dei mezzi del trattamento da parte del Responsabile comporta l'assunzione, da parte dello stesso, della qualifica di Titolare del trattamento, con ogni ulteriore conseguenza.

Art. 2 – Le presenti clausole lasciano impregiudicati gli obblighi cui è soggetto il Titolare a norma del Regolamento. Si precisa che le presenti clausole non garantiscono, di per sé, il rispetto degli obblighi connessi ai trasferimenti internazionali conformemente al Capo V del Regolamento.
Le presenti clausole vanno lette e interpretate alla luce delle disposizioni del Regolamento.
Le presenti clausole non devono essere interpretate in un senso che non sia conforme ai diritti e agli obblighi previsti dal Regolamento, o che pregiudichi i diritti o le libertà fondamentali degli interessati. In caso di contraddizione tra le presenti clausole e le disposizioni di accordi correlati, vigenti tra le Parti al momento della sottoscrizione del Contratto, o conclusi successivamente, prevalgono le presenti clausole.

Il Responsabile è consapevole ed accetta che i propri dati possano essere pubblicati sul sito istituzionale e/o sulla bacheca del Titolare, per finalità di trasparenza (artt. 13, 14 e 15 del Regolamento) nei confronti degli interessati, o comunque resi noti agli stessi.

Art. 3 – Il Responsabile si impegna a trattare i dati personali soltanto sulla base delle istruzioni documentate (anche successivamente rilasciate, nel corso del rapporto) da parte del Titolare, anche in caso di trasferimento di dati personali verso un Paese Terzo o un'organizzazione internazionale, salvo che lo richieda il diritto europeo o nazionale cui è soggetto il Responsabile; in tal caso, lo stesso Responsabile informerà il Titolare di tale obbligo giuridico prima del relativo trattamento, salvo che la normativa in questione vieti tale informazione per rilevanti motivi di interesse pubblico.
Qualora i dati personali fossero trasferiti verso Paesi Terzi ovvero organizzazioni internazionali, fatti salvi i casi eccezionali e di rilevante interesse pubblico di cui all'art. 49 del Regolamento applicabili alla presente fattispecie contrattuale, ciò potrà avvenire esclusivamente ai sensi dell'art. 45 del Regolamento. Sono vietati, pertanto, i trasferimenti basati sugli ulteriori strumenti previsti dal Capo V del Regolamento.
Il Responsabile informerà immediatamente il Titolare qualora, a suo parere, un'istruzione violasse il Regolamento o altre disposizioni, europee o nazionali, relative alla protezione dei dati.
I dati personali trattati dal Responsabile concernono sia i dati c.d. "comuni" che quelli annoverabili nelle particolari categorie di dati di cui all'art. 9 del Regolamento (dati c.d. "sensibili"), nonché quelli di cui all'art. 10 (dati c.d. "giudiziari"); le categorie di interessati coinvolti nel trattamento riguardano esclusivamente alunni e genitori degli alunni o chi esercita la potestà genitoriale.
In relazione al rapporto contrattuale di cui in premessa e fermo restando quanto presente nell'art. 26 del Contratto di Servizio il Responsabile potrà trattare i dati esclusivamente per finalità connesse all'esercizio di un compito di interesse pubblico relativo al servizio di istruzione e formazione professionale e potrà effettuare, con o senza strumenti automatizzati soltanto le seguenti operazioni di trattamento: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso. La durata del trattamento coincide con il termine del Contratto.

Art. 4 – In ogni fase e per ogni operazione del trattamento, il Responsabile dovrà garantire il rispetto dei principi europei (ad esempio, di *privacy by design e by default*) e nazionali in

ambito di protezione dei dati personali e, in particolare, quelli di cui agli artt. 5 e 25 del Regolamento, anche nel rispetto della *privacy policy* del Titolare che il Responsabile dichiara di conoscere. Il Responsabile dovrà:

a) garantire che le persone che trattano i dati personali siano state specificamente autorizzate, adeguatamente istruite/formate e si siano impegnate alla riservatezza, o abbiano un adeguato obbligo legale di riservatezza e possano accedere ai dati personali soltanto nella misura strettamente necessaria all'attuazione, gestione e controllo del contratto;

b) oltre ad assistere il Titolare nell'adempimento degli obblighi di cui all'art. 32 del Regolamento, adottare tutte le misure richieste ai sensi del medesimo articolo dirette a garantire la sicurezza dei dati personali. Ciò include la protezione da ogni violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati (violazione dei dati personali). Nel valutare l'adeguato livello di sicurezza, le Parti tengono debitamente conto dello stato dell'arte, dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per gli interessati.

Ciò premesso, il Responsabile dichiara di mettere in atto almeno le seguenti misure tecniche ed organizzative:

MISURE DI SICUREZZA GENERALI.

In orario di apertura l'accesso agli uffici della Sede è sorvegliato dal personale di Segreteria, il quale provvede alla sorveglianza della porta di accesso. Le chiavi delle porte di accesso agli uffici sono in possesso del personale. Al di fuori delle aree di accesso consentite al pubblico eventuali visitatori e/o prestatori d'opera sono accompagnati e controllati dal personale in servizio. Alla chiusura degli uffici le porte d'ingresso sono chiuse a chiave e viene attivato il sistema antintrusione inserendo l'allarme.

Per le misure relative al trattamento di dati giudiziari, sanitari (sia per l'utenza che per i dipendenti) si fa riferimento a quanto previsto nel citato Registro dei Trattamenti. Vale comunque la penna di precisare che al personale è data comunicazione scritta, che rende note le procedure a cui tutto il personale, che gestisce a vario titolo dati dell'ente, deve ottemperare e che sono programmati ed effettuati interventi formativi dedicati al Titolare, ai responsabili e alle persone autorizzate al trattamento per renderli consapevoli dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative

attività, delle responsabilità che ne derivano, delle modalità per aggiornarsi sulle adeguate misure di sicurezza adottate dall'ente.

MISURE DI SICUREZZA GENERALI RELATIVAMENTE AI DATI SU SUPPORTO INFORMATICO.

Premesso che la gestione e conservazioni dei dati personali e\o sensibili in gestione da parte di ENAIP Trentino, viene gestita in parte presso la struttura interna (on premises) e parte all'esterno (cloud), nel rispetto delle direttive menzionate all'interno del Regolamento generale sulla protezione dei dati, e di seguito illustrate:

Conservazione e trattamento dei dati presso la struttura interna (on premises)

Infrastruttura hardware:

L'archetipo di riferimento per descrivere infrastruttura hardware presente presso la sede provinciale di ENAIP Trentino è definito "client server", in cui sono presenti dei sistemi di gestione centralizzata, denominati "server di rete" e dei sistemi di utilizzo personale, denominati "client" (Personal Computer).

Lo spazio fisico dove sono conservati le architetture hardware "server di rete" e "client", sono "protetti" da vari sistema di sicurezza che riguardano l'accesso allo spazio fisico, mediante sistema di chiusura meccanica e\o elettronica, sistemi di sicurezza antiintrusione mediante videosorveglianza H24 e sistema di rilevamento volumetrico (tecnologia IR), e sistemi antincendio.

L'architettura hardware relativa al sistema di conservazione dei dati "server di rete" è caratterizzata da una tecnologia di conservazione delle informazioni basata sulla ridondanza e duplicazione degli stessi, mediante un sistema di conservazione esterna (NAS dir rete), sul quale vengono conservate le informazioni (back-up) con cadenza giornaliera, mentre dal punto di vista hardware, il sottosistema per la conservazione delle informazioni basato su dischi elettro-meccanici, è stato progettato con un sistema di tolleranza ai guasti hardware, mediante la tecnologia RAID di livello 10 (mirroring e striping), che prevede il mantenimento operativo anche alla presenza di un disco guasto. Inoltre il sistema è protetto da un duplice sistema di alimentazione elettrica, mediante la presenza di un doppio alimentatore, con diversificata sorgente di alimentazione, una direttamente dall'impianto elettrico, l'altra mediante fornitura proveniente da un sistema di "protezione" UPS (gruppo di continuità), che ne garantisce la continuità operativa in caso di interruzione dell'alimentazione elettrica da parte del gestore.

Per quanto concerne l'architettura hardware dei dispositivi "client", essi sono sottoposti a backup con cadenza settimanale, dell'intero contenuto conservato, direttamente all'interno di un server NAS dedicato.

Infrastruttura software:

Sistemi operativo (S.O.):

Il S.O. utilizzato per le gestione del server di rete, si basa sulla versione dedicata ai server, prodotta da Microsoft e denominata Windows Server 201x, esso viene aggiornato con le ultime versioni\aggiornamenti che sono rilasciati mensilmente dal produttore del software Microsoft in base all'aggiunta di nuove funzionalità e\o aggiornamenti relativi alla correzione di eventuali "criticità", in materia di sicurezza.

Il S.O. utilizzato per l'utilizzo delle P.D.L. client, anch'esso sviluppato dalla software house Microsoft, e declinato nella versione Windows 10 Professional e Windows 11 Professional, anche in questo contesto il S.O., viene costantemente aggiornato (mensilmente) dagli aggiornamenti che la software house Microsoft rilascia in merito alla implementazione di nuove funzionalità e\o aggiornamenti relativi alla correzione di eventuali "criticità", in materia di sicurezza.

Software applicativi orizzontali:

Le applicazioni software come ad esempio la suite Microsoft Office 201x, sono costantemente aggiornate, in base ai piani di rilascio delle nuove funzionalità e\o aggiornamenti relativi alla correzione di eventuali "criticità", in materia di sicurezza.

Software applicativi verticali:

Le applicazioni software utilizzate per la gestione specifica dei processi aziendali, come ad esempio la gestione magazzino, la gestione del personale, ecc.…, sono aggiornate con cadenza annuale, in base alla disponibilità delle nuove versioni, rilasciate dalle varie software house, allo scopo migliorare le funzionalità dell'applicazione e\o apportare eventuali correzioni per correggere eventuali "criticità", in materia di sicurezza.

Software di sicurezza:

Ogni server di rete e ogni P.D.L., è protetta da un software dedicato al controllo e alla prevenzione da software malevolo (antivirus), nello specifico la versione 14.3.x di Symantec EndPoint Protecion. Il software di protezione, si occupa di analizzare in tempo reale tutto il traffico in entrata e in uscita da ogni singola P.D.L. (firewall) e al tempo stesso, si preoccupa di analizzare tutti i file (app, documenti, fotografie, video, ecc.…), presenti all'interno di ogni spazio dedicato alla conservazione dei dati, allo scopo di verificare e se il caso correggere e segnale eventuali presenze di software malevolo.

Nel caso in cui il sistema di controllo sulla sicurezza, riscontrasse una qualsiasi anomalia e\o difformità del software utilizzato su ogni P.D.L., viene generato un "avviso" relativo alla criticità segnalata, mediante l'invio di un messaggio di posta elettronica all'amministratore del sistema I.T.

Oltre all'invio di avvisi estemporanei relativi alla sicurezza, il sistema di controllo sulla sicurezza, invia quotidianamente e settimanalmente (riepilogo), un report attraverso la posta elettronica, riportante il nome dell'account utente che ha effettuato il login su ogni P.D.L., la data e l'ora, il grado di aggiornamento delle impronte digitale dell'antivirus e la eventuale segnalazioni di software malevolo identificato e\o modifiche al S.O. avvenute.

Autenticazione alla rete informatica:

L'accesso ad ogni P.D.L. presente all'interno della rete locale, viene "garantito" mediante l'inserimento di credenziali univoche e assegnate ad ogni utente autorizzato all'utilizzo delle P.D.L.. Le credenziali identificano in modo univoco l'utilizzatore e sono nella forma (nome.cognome), oltre al proprio account, viene richiesta la digitazione di una password riservata e personale, da modificare obbligatoriamente al primo accesso.

La password è conforme alle specifiche indicate nel G.DPR, e nello specifico sono soggette alle seguenti regole:

- Lunghezza password: 12 caratteri o superiore
- Complessità password: obbligatorio l'utilizzo di almeno uno dei seguenti caratteri maiuscolo, minuscolo, e carattere speciale (@, $, %, !, …..)
- Ripetibilità password: Non corrispondente alle ultime 12 password utilizzate
- Durata minima password: 1 giorno
- Durata massima password: 365 giorni
- Numero tentativi di accesso (non riusciti) prima della chiusura account in automatico: 5 tentativi

Ogni account utente è associato ad un gruppo omogeneo per tipologia di utilizzo \ accesso e trattamento delle informazioni, ad ogni gruppo omogeneo sono associate specifiche "regole" di accesso alle informazioni condivise all'interno del server, come ad esempio sola lettura, modifica, cancellazione, creazione, copia, ecc….

Ogni anno viene verificata la "titolarità" dell'account utente, all'accesso alla rete informatica e al ruolo di appartenenza nei gruppi di lavoro e di conseguenza alle regole di accesso alle informazioni condivise.

Il protocollo di accesso \ comunicazione fra la P.D.L. e il server di rete, si basa sulla versione 2 del protocollo SMB.

Tutti gli accessi alla rete informatica, sono registrati e disponibili attraverso la visione di specifici "log", conservati all'interno del server di rete, per una durata non superiore ai 180 giorni.

Procedura di dismissione dei dispositivi contenenti informazioni\dati personali e\o sensibili:

Durante la fase di dismissione dei dispositivi hardware per vetustà \ obsolescenza tecnologica o guasto hardware, vengono implementate le seguenti procedure:

Nel caso di dispositivo hardware guasto, il componente deteriorato viene sottoposto ad azione meccanica, mediante la perforazione da parte a parte del dispositivo, con l'ausilio di un trapano elettrico.

Nel caso di dispositivo funzionante, lo stesso viene sottoposto ai seguenti standard di sanificazione:

- Zero veloce Sovrascrivi
- Sovrascrittura casuale
- Standard DOD 5220.28 STD

Conservazione e trattamento dei dati presso la struttura esterna (cloud)

ENAIP Trentino utilizza come piattaforma informatica per la gestione della posta elettronica, per la condivisione e conservazione dati e per le riunioni e conversazioni, Microsoft 365, dedicata per l'utilizzo educativo.

La conservazione fisica dei dati si trova presso il data center di Microsoft a Dublino e in copia presso il data center di Amsterdam.

L'accesso alla piattaforma Microsoft 365, avviene mediante l'inserimento di proprie credenziali univoche e personali nella forma nome.cognome@enaip.tn.it, oltre all'inserimento del proprio account, viene richiesto la digitazione di una password personale e privata, corrispondente alle seguenti regole:

- Lunghezza password: 12 caratteri o superiore
- Complessità password: obbligatorio l'utilizzo di almeno uno dei seguenti caratteri maiuscolo, minuscolo, e carattere speciale (@, $, %, !, …..)
- Ripetibilità password: Non corrispondente alle ultime 12 password utilizzate
- Durata minima password: 1 giorno
- Durata massima password: 365 giorni
- Numero tentativi di accesso (non riusciti) prima della chiusura account in automatico: 5 tentativi

Ogni anno, vengono controllati i singoli account utente per verificare la titolarità o meno dell'accesso alla piattaforma.
Nel caso di eliminazione \ perdita del diritto di accesso di ogni account utente, i dati dello stesso vengono eliminati dalla piattaforma entro 90 giorni.
La piattaforma Microsoft 365 rispetta un'ampia gamma di normative e standard globali, regionali e di settore, come il General Data Protection Regulation (GDPR), l'Health Insurance Portability and Accountability Act (HIPAA) ed il Federal Risk and Authorization Management Program (FedRAMP).
Inoltre la piattaforma Microsoft 365, utilizza le seguenti procedure per la protezione dei dati:
Microsoft Defender XDR: per tutto ciò che riguarda sicurezza dei device Windows, Posta Elettronica e Identità.
Microsoft Pureview (Compliance): per tutto ciò che riguarda la classificazione dei dati, la crittografia ed i controlli di accesso, grazie ai quali possiamo salvaguardare le informazioni sensibili da accessi non autorizzati, da divulgazione o uso improprio.
Nel caso di un tentativo di accesso non autorizzato alla piattaforma, oppure alla verifica di comportamenti anomali rilevati dal sistema, quale ad esempio l'invio massivo di mail, la condivisione eccessiva di documenti, ecc…, attivano in modo proattivo un servizio di allerta, mediante l'invio di posta elettronica, in merito all'attività sospetta e al blocco preventivo dell'account utente, individuato come responsabile dell'attività anomala.
In caso di trattamento con strumenti automatizzati, il Responsabile garantisce di aver adottato misure di sicurezza analoghe e non inferiori al livello minimo di cui alla circolare Agid n. 2/2017 (Misure minime di sicurezza ICT per le pubbliche amministrazioni) e successive modifiche e integrazioni;
c) assistere il Titolare 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 (Capo III del Regolamento), nonché informare tempestivamente il Titolare dei reclami eventualmente presentati dagli interessati, oltre che di qualsiasi altra richiesta dagli stessi pervenuta, attenendosi alle istruzioni del Titolare ed astenendosi dal rispondere direttamente alla richiesta stessa, a meno che sia stato autorizzato in tal senso dal Titolare;
d) rispondere prontamente ed adeguatamente alle richieste di informazioni del Titolare relative al trattamento dei dati e mettere a sua disposizione tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente Contratto o che

derivano dal Regolamento, consentendo e contribuendo alle attività di revisione, comprese le ispezioni (da intendersi anche quelle nei locali, o nelle strutture fisiche del Responsabile), realizzate dal Titolare, dal suo *Data Protection Officer*, o da un altro soggetto a ciò deputato, effettuate con adeguato preavviso e ad intervalli ragionevoli, o qualora vi fossero indicazioni di inosservanza. Nel decidere in merito a un riesame o a un'attività di revisione, il Titolare può tenere conto delle pertinenti certificazioni in possesso del Responsabile.

Su richiesta, le Parti mettono a disposizione della/e Autorità di controllo competente/i le informazioni di cui alla presente clausola, compresi i risultati di eventuali attività di revisione;

e) assistere il Titolare nel garantire il rispetto degli obblighi di cui agli articoli 35 e 36 del Regolamento tenendo conto della natura del trattamento e delle informazioni a disposizione, nonché garantire che i dati personali siano esatti e aggiornati, informando senza indugio il Titolare qualora venga a conoscenza del fatto che i dati personali che sta trattando sono inesatti od obsoleti.

In particolare, relativamente alla predisposizione della valutazione di impatto, nel caso in cui il Responsabile fornisse al Titolare gli strumenti/applicativi informatici e/o gestisse gli stessi strumenti/applicativi informatici del Titolare, lo stesso sarà tenuto a predisporre ed aggiornare l'analisi dei rischi (probabilità di violazione della sicurezza) degli strumenti/applicativi informatici, comunicandola al Titolare, adottando i criteri di valutazione forniti da quest'ultimo;

f) in caso di violazione dei dati personali (*data breach*), cooperare con il Titolare e assisterlo nell'adempimento degli obblighi di cui agli artt. 33 e 34 del Regolamento, tenendo conto della natura del trattamento e delle informazioni a disposizione.

In caso di violazione dei dati trattati dal Titolare, assistere quest'ultimo nell'adempimento dell'eventuale notifica all'Autorità di controllo e nell'eventuale comunicazione agli interessati, ottenendo le seguenti informazioni: 1) la natura dei dati personali compresi, 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; 2) le probabili conseguenze della violazione dei dati personali; 3) le misure adottate o di cui si propone l'adozione da parte del Titolare per porre rimedio alla violazione dei dati personali, se del caso anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la comunicazione

iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
In caso di violazione dei dati personali trattati dallo stesso Responsabile, informare il Titolare (cioè alla Struttura provinciale di merito, inviando il rapporto di *data breach* anche alla Struttura provinciale competente in materia di protezione dei dati personali) non appena venuto a conoscenza dell'evento, adempiendo a quanto previsto dalla specifica *policy* provinciale in tema di *data breach* che il Responsabile dichiara di conoscere. Tale informazione contiene almeno: 1) una descrizione della natura della violazione (compresi, ove possibile, le categorie e il numero approssimativo di interessati e di registrazioni dei dati in questione); 2) i recapiti di un punto di contatto presso il quale possono essere ottenute maggiori informazioni sulla violazione dei dati personali; 3) le probabili conseguenze della violazione dei dati personali e le misure adottate o di cui si propone l'adozione per porre rimedio alla violazione, anche per attenuarne i possibili effetti negativi. Qualora, e nella misura in cui, non sia possibile fornire tutte le informazioni contemporaneamente, la comunicazione iniziale contiene le informazioni disponibili in quel momento, e le altre informazioni sono fornite successivamente, non appena disponibili, senza ingiustificato ritardo.
Sempre con riferimento ai casi di *data breach* (di cui agli artt. 33 e 34 del Regolamento), qualora gli strumenti/applicativi informatici del Titolare fossero forniti o gestiti dal Responsabile, quest'ultimo è sin d'ora delegato dal Titolare, accettando tale delega senza costi aggiuntivi, ad effettuare la relativa notifica all'Autorità di controllo e comunicazione ai relativi interessati qualora la violazione riguardasse gli strumenti/applicativi informatici stessi; tali adempimenti dovranno essere effettuati previa valutazione, con la Struttura provinciale direttamente coinvolta e a cui compete la decisione, degli elementi della violazione e delle necessarie conseguenti azioni da intraprendere;
g) nei casi prescritti dall'art. 37 del Regolamento, oltre che nelle fattispecie in cui tale adempimento sia raccomandato nelle specifiche Linee Guida del Gruppo di Lavoro Art 29/EDPB, provvedere alla nomina del *Data Protection Officer* (di seguito, "DPO"), nel rispetto dei criteri di selezione stabiliti dallo stesso Regolamento, dalle relative Linee Guida del Gruppo di Lavoro Art 29/EDPB, nonché dalle indicazioni fornite dall'Autorità di controllo, garantendo il rispetto delle prescrizioni di cui all'art. 38, anche allo scopo di consentire al medesimo DPO l'effettivo adempimento dei compiti di cui all'art. 39 del Regolamento;

h) provvedere alla designazione per iscritto del/degli Amministratore/i di Sistema secondo i criteri di individuazione e selezione previste dall'Autorità di controllo con provvedimento dd. 27/11/2008 e s.m.i., conservando l'elenco degli stessi Amministratori, verificandone annualmente l'operato ed adottando sistemi idonei alla registrazione dei relativi accessi logici (da conservare con caratteristiche di inalterabilità e integrità per almeno per 6 mesi). Qualora l'attività degli stessi Amministratori di Sistema riguardasse, anche indirettamente, servizi o sistemi che trattano, o che permettono il trattamento, di informazioni di carattere personale dei dipendenti del Titolare, comunicare a quest'ultimo l'identità degli Amministratori di Sistema (provvedendo a dare idonea informativa, *ex* art. 13 del Regolamento, agli stessi Amministratori);

i) provvedere alla predisposizione del Registro delle attività del trattamento nei termini di cui all'art. 30.2 del Regolamento, mettendolo tempestivamente a disposizione del Titolare, o dell'Autorità di controllo, in caso di relativa richiesta;

j) effettuare la segregazione (fisica e logica) dei dati personali (ovvero mantenerli separati rispetto a quelli di cui è Titolare, o Responsabile per altri soggetti) ed informare tempestivamente il Titolare di ogni variazione oggettiva della propria compagine societaria o qualità soggettive tale da compromettere il corretto espletamento dei compiti assegnati, nonché perdita (anche parziale) dei requisiti e delle garanzie offerte;

k) comunicare, al Titolare, i nominativi di riferimento per l'esecuzione del Contratto, nonché il nominativo dell'eventuale DPO;

l) alla scadenza del rapporto contrattuale di cui in premessa (ivi compresi i casi di risoluzione o recesso), o al più al termine dell'esecuzione delle relative attività/prestazioni e, quindi, delle conseguenti operazioni di trattamento, fatta salva una diversa determinazione del Titolare (concernente, ad esempio, la restituzione dei dati), provvedere alla cancellazione (ivi compresa ogni eventuale copia esistente) dei dati personali in oggetto (certificando al Titolare di aver ottemperato in tal senso), a meno che il diritto europeo o nazionale ne preveda la conservazione ed esclusa ogni altra forma di conservazione anche per finalità compatibili. In caso di trattamento con modalità automatizzate, il Responsabile garantisce che, su richiesta del Titolare e senza costi aggiuntivi, prima di effettuare la cancellazione predetta potrà effettuare la trasmissione sicura dei dati personali ad altro soggetto, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, beninteso qualora il destinatario sia attrezzato a riceverli. Sino a quando i dati non sono cancellati (o restituiti), il Responsabile continua ad assicurare il rispetto del presente Contratto.

Art. 5 Il Responsabile non può subcontrattare a un sub-Responsabile i trattamenti da effettuare per conto del Titolare conformemente al presente Contratto senza la previa autorizzazione specifica scritta dello stesso Titolare. Il Responsabile presenta la richiesta di autorizzazione specifica almeno trenta giorni prima di ricorrere al sub-Responsabile in questione, unitamente alle informazioni necessarie per consentire al Titolare di decidere in merito all'autorizzazione. L'elenco dei sub-Responsabili autorizzati dal Titolare sono allegati al Contratto. Le Parti tengono aggiornato tale allegato.
In ogni caso, qualora il Responsabile ricorresse ad un sub-Responsabile per l'esecuzione di specifiche attività di trattamento per conto del Titolare, dovrà sottoscrivere, con tale sub-Responsabile, un contratto analogo al presente Contratto – stipulato in forma scritta, anche in formato elettronico – imponendo a quest'ultimo, nella sostanza, gli stessi obblighi in materia di protezione dei dati contenuti nel presente Contratto (e in ogni altro atto giuridico o *addendum* intervenuto tra le Parti) e prevedendo, in particolare, garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento, nonché della connessa disciplina nazionale. Su richiesta del Titolare, il Responsabile gli fornisce copia del contratto stipulato con il sub-Responsabile e di ogni successiva modifica. Nella misura necessaria a proteggere segreti aziendali o altre informazioni riservate, compresi i dati personali, il Responsabile può espungere informazioni dal contratto prima di trasmetterne una copia.
Il Responsabile si assicura che il sub-Responsabile rispetti gli obblighi a cui lo stesso Responsabile è soggetto a norma del Contratto e del Regolamento.
Il Responsabile comunica al Titolare qualunque inadempimento, da parte del sub-Responsabile, degli obblighi contrattuali. Laddove il sub-Responsabile ometta di adempiere ai propri obblighi contrattuali, il Responsabile sarà ritenuto integralmente responsabile nei confronti del Titolare.
Il Responsabile concorda con il sub-Responsabile una clausola del terzo beneficiario secondo la quale, qualora il Responsabile sia scomparso di fatto, abbia giuridicamente cessato di esistere o sia divenuto insolvente, il Titolare ha diritto di risolvere il contratto con il sub-Responsabile e di imporre a quest'ultimo di cancellare o restituire i dati personali.

Art. 6 – In caso di azione di risarcimento civile, o responsabilità amministrativa, promossa nei confronti del Titolare per i danni provocati, o le violazioni commesse dal Responsabile a seguito di inadempienze normative o contrattuali, il Responsabile stesso manleva integralmente il Titolare, ogni eccezione rimossa. Analogamente, il Responsabile manleva

integralmente il Titolare, ogni eccezione rimossa, in caso di applicazione di sanzioni da parte dell'Autorità di controllo per inadempienze normative o contrattuali commesse dallo stesso Responsabile.

Art. 7 – Il Contratto avrà termine il 31/08/2026, in forza del collegamento con il Contratto di Servizio di cui in premessa, la risoluzione o il recesso dello stesso contratto produrrà medesimo effetto sul presente Contratto. Nel caso in cui la Provincia si avvalesse dell'opzione di proroga, prevista al comma 5 dell'art. 3 del Contratto di Servizio, il Contratto avrà termine il 31/08/2028.

Art. 8 – Fatte salve le disposizioni del Regolamento, qualora il Responsabile violi gli obblighi che gli incombono ai sensi del Contratto, il Titolare del trattamento può dare istruzione al Responsabile di sospendere il trattamento dei dati personali fino a quando quest'ultimo non rispetti le presenti clausole, o non sia risolto il Contratto stesso. Il Responsabile informa immediatamente il Titolare del trattamento qualora, per qualunque motivo, non sia in grado di rispettare le presenti clausole.

Il Titolare ha diritto di risolvere il Contratto, per quanto riguarda il trattamento dei dati personali conformemente alle presenti clausole, qualora si verifichi anche solo una delle seguenti situazioni: (a) il trattamento dei dati personali da parte del Responsabile sia stato sospeso dal Titolare ai sensi del comma precedente e il rispetto delle presenti clausole non sia ripristinato entro un termine ragionevole e in ogni caso entro un mese dalla sospensione; (b) il Responsabile violi in modo sostanziale, o persistente, le presenti clausole, o gli obblighi che gli incombono a norma del Regolamento, o della connessa disciplina nazionale, o delle prescrizioni dell'Autorità di controllo; (c) il Responsabile non rispetti una decisione vincolante di un organo giurisdizionale competente, o della/e Autorità di controllo competente/i per quanto riguarda i suoi obblighi in conformità del Contratto, o del Regolamento, o della connessa disciplina nazionale.

Il Responsabile ha diritto di risolvere il Contratto, per quanto riguarda il trattamento dei dati personali a norma delle presenti clausole, qualora, dopo aver informato il Titolare che le sue istruzioni violano i requisiti giuridici applicabili, in conformità al precedente Art. 3, il Titolare insista sul rispetto delle istruzioni.

Dopo la risoluzione del Contratto il Responsabile, dovrà agire nel rispetto di quanto previsto al precedente Art. 4, lett. l).

Art. 9 – Per ogni controversia riguardante il presente Contratto è competente il Foro di Trento.

Provincia autonoma di Trento Cristina Ioriatti

Enaip Trentino Arrigo Dalfovo

Il Responsabile, ai sensi e per gli effetti dell'art. 1341 c.c., accetta e sottoscrive espressamente le seguenti clausole:

Art. 1 – diligenza professionale

Art. 5 – restrizione alla libertà contrattuale nei rapporti coi terzi

Art. 6 – limitazione di responsabilità (manleva)

Art. 8 – Facoltà di risoluzione

Art. 9 – Foro competente

Enaip Trentino Arrigo Dalfovo